รายงานฉบับสมบูรณ์

(Final Report)

กฎหมายความปลอดภัยทางไซเบอร์กับการกำกับดูแลเศรษฐกิจดิจิทัลของประเทศจีน:ถอดบทเรียนสำหรับเศรษฐกิจดิจิทัลในยุคไทยแลนด์ 4.0

China's Cybersecurity Law and the Regulation of China's Digital Economy: Lessons for the Digital Economy in Thailand 4.0 Era

โดย

ดร.อาร์ม ตั้งนิรันดร

ภายใต้แผนงานยุทธศาสตร์เป้าหมาย (Spearhead) ด้านสังคม แผนงานคนไทย 4.0

สนับสนุนโดย

สำนักงานการวิจัยแห่งชาติ (วช.)

กรกฎาคม 2563

เลขที่สัญญา 2562/2-06

รายงานฉบับสมบูรณ์

(Final Report)

กฎหมายความปลอดภัยทางไซเบอร์กับการกำกับดูแลเศรษฐกิจดิจิทัลของประเทศจีน:ถอดบทเรียน สำหรับเศรษฐกิจดิจิทัลในยุคไทยแลนด์ 4.0

โดย

ดร.อาร์ม ตั้งนิรันดร คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

ภายใต้แผนงานยุทธศาสตร์เป้าหมาย (Spearhead) ด้านสังคม แผนงานคนไทย 4.0

สนับสนุนโดย

สำนักงานการวิจัยแห่งชาติ (วช.)

กิตติกรรมประกาศ

ผู้วิจัยขอกราบขอบพระคุณแผนงานบูรณาการยุทธศาสตร์เป้าหมาย (Spearhead) ด้านสังคมคนไทย 4.0 สนับสนุนโดยสำนักงานการวิจัยแห่งชาติ (วช.) ประจำปีงบประมาณ 2562 ที่กรุณาให้ทุนสนับสนุนโครงการวิจัย งานวิจัยชิ้นนี้จะไม่สามารถสำเร็จได้ หากไม่ได้รับความเห็นและข้อเสนอแนะที่เป็นประโยชน์จาก ศ.ดร.มิ่งสรรพ์ ขาวสอาด ศ.ดร.กาญจนา กาญจนสุต รศ.ดร.กอบกุล รายะนาคร ดร.สมเกียรติ ตั้งกิจวาณิชย์ โดยเฉพาะอย่างยิ่ง ศ.ดร.กาญจนา กาญจนสุต ได้กรุณาให้โอกาสผู้วิจัยร่วมเดินทางไปประชุม World Internet Conference ร่วมกับท่านที่เมืออู่เจิน สาธารณรัฐประชาชนจีน จนได้เก็บข้อมูลและสร้างเครือข่ายทางวิชาการที่เป็นประโยชน์อย่างยิ่งในการวิจัยเกี่ยวกับกฎหมายความปลอดภัยทางไซเบอร์ของประเทศจีน จนสำเร็จเป็นผลงานวิจัยเล่มนี้

บทสรุปผู้บริหาร

เศรษฐกิจดิจิทัลของจีนมีการพัฒนาอย่างรวดเร็ว จนจีนนับเป็นผู้นำด้านเศรษฐกิจดิจิทัลในระดับโลก โดยกฎหมายความปลอดภัยทางไซเบอร์ของจีน (Cybersecurity Law 2017) เป็นกฎหมายหลักที่เป็นรากฐานของการกำกับดูแลความปลอดภัยของข้อมูลและความปลอดภัยทางไซเบอร์ในยุคเศรษฐกิจดิจิทัล กฎหมายดังกล่าวได้ผ่านการพิจารณาจากสภาประชาชนแห่งชาติในวันที่ 7 พฤศจิกายน ค.ศ. 2016 และเริ่มมีผลบังคับใช้ตั้งแต่วันที่ 1 มิถุนายน ค.ศ. 2017 เป็นต้นมา

จากการศึกษาพบว่า กฎหมายความปลอดภัยทางไซเบอร์ของจีนสะท้อนให้เห็นถึงความพยายามของรัฐบาลจีนในการอ้างอำนาจอธิปไตยบนโลกอินเทอร์เน็ต ประเทศจีนมีความต้องการจัดการดูแลไซเบอร์เสปซด้วยตัวเอง ด้วยการมอบอำนาจให้รัฐบาลในการระบุและควบคุมพฤติกรรมต่างๆ บนโลกออนไลน์ที่ไม่เหมาะสม การทำความเข้าใจในกฎหมายความปลอดภัยทางไซเบอร์ของจีนควรพิจารณาผ่านมุมมองพิเศษของประเทศจีนที่มีต่อความปลอดภัยทางไซเบอร์ ซึ่งมีความหมายกว้างขวางกว่าของชาติตะวันตก ในประเทศจีนความปลอดภัยทางไซเบอร์จะเกิดขึ้นได้ก็ด้วยการควบคุมเนื้อหาบนอินเทอร์เน็ต เพื่อรักษาไว้ซึ่งความเสถียรภาพทางการเมืองและสังคม นอกจากนี้ การปฏิบัติต่อข้อมูลส่วนบุคคลในกฎหมายฉบับนี้สะท้อนให้เห็นถึงมุมมองของประเทศจีนในด้านสิทธิมนุษยชน สิทธิมนุษยชนได้รับการรับรองตามกฎหมาย ทว่าก็สามารถถูกละเมิดโดยอำนาจรัฐได้

ภายใต้การบังคับใช้ของกฎหมายความมั่นคงปลอดภัยไซเบอร์นี้ ผู้ให้บริการทางโครงข่ายซึ่งประกอบกิจการอันเกี่ยวข้องกับระบบโครงสร้างพื้นฐานสำคัญจะถูกบังคับให้มีส่วนร่วมในการปกป้องความมั่นคงปลอดภัยไซเบอร์ด้วย ประเทศจีนเชื่อมั่นในระบบบังคับและจะทดลองมาตรการต่างๆ เพื่อนำไปสู่การให้ความคุ้มครองระบบโครงสร้างพื้นฐานที่มีประสิทธิภาพและยั่งยืน สำหรับประเด็นเรื่องการเก็บรวบรวมข้อมูลในท้องที่นั้น ก็จัดว่าเป็นอีกภาระหนึ่งที่ยุ่งยากสำหรับผู้ให้บริการเครือข่ายที่เกี่ยวข้องกับระบบโครงสร้างพื้นฐานสำคัญ และไม่มีความแน่ชัดว่ามาตรการดังกล่าวจะช่วยเสริมสร้างความแข็งแกร่งให้กับความปลอดภัยไซเบอร์ในระยะยาวได้จริง ทั้งนี้ มาตรการการเก็บรวบรวมข้อมูลในท้องที่อาจทำให้ผู้ประกอบธุรกิจได้รับความเสี่ยงจากการถูกสอดแนมโดยรัฐบาลท้องที่ และถึงแม้ว่ากฎหมายจะมีบทบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลเกิดขึ้นมาแล้วก็ตาม แต่กฎหมายความปลอดภัยทางไซเบอร์ก็ยังให้อำนาจรัฐบาลในการเข้าถึงข้อมูลเหล่านั้น อันนำไปสู่การรั่วไหลของข้อมูลอยู่นั่นเอง

เมื่อเปรียบเทียบแล้ว โมเดลกฎหมายจีนเริ่มมีอิทธิพลต่อการบัญญัติกฎหมายของประเทศไทยในการกำกับดูแลเศรษฐกิจดิจิทัลในยุคไทยแลนด์ 4.0 ถึงแม้ว่าในทางรูปแบบและเนื้อหาของกฎหมายส่วนใหญ่ จะมีความพยายามยึดตามโมเดลของสหภาพยุโรปและสหรัฐอเมริกา แต่ก็มีการสอดแทรกเนื้อหาหรือลักษณะเด่นของโมเดลจีนด้วย ในประเทศตะวันตกเอง ก็เริ่มมีกระแสการเดินตามโมเดลจีนบ้างเช่นกัน เนื่องจากความกังวลเรื่องภัยคุกคามต่อความมั่นคง การแข่งขันทางเทคโนโลยีระหว่างมหาอำนาจ และความปลอดภัยทางไซ

เบอร์ ดังนั้น เส้นการแบ่งแยกที่ชัดเจนระหว่างสำนัก Cyber Paternalism ตามแนวจีน กับสำนัก Cyber Commons ตามแนวตะวันตก อาจไม่สามารถแบ่งได้ชัดเจนดังเช่นในอดีต โดยจะมีความซับซ้อนมากขึ้นตามแต่ละประเด็นกฎหมาย รวมทั้งจะมีแนวโน้มเป็นเรื่องของระดับการที่รัฐเข้ามากำกับดูแลไซเบอร์สเปซมากกว่าเรื่องว่ารัฐจะเข้ามากำกับหรือไม่

บทเรียนด้านกฎหมายที่สำคัญ คือ ในการวางแนวทางการกำกับดูแลเศรษฐกิจดิจิทัลในยุคไทยแลนด์ 4.0 จะต้องก้าวข้ามกรอบคิดว่าจะเลือกแบบสำนัก Cyber Paternalism ตามแนวจีน หรือสำนัก Cyber Commons ตามแนวตะวันตก แต่จะต้องพิจารณาถึงการสร้างสมดุลระหว่าง 2 แนวคิด ผ่านการออกแบบกลไกที่เหมาะสม และการออกแบบเกณฑ์หรือมาตรฐานที่จำกัดการใช้ดุลยพินิจของรัฐเกินสมควร

บทเรียนด้านภูมิรัฐศาสตร์การเมืองและเทคโนโลยีระหว่างประเทศที่สำคัญ คือ คนไทย 4.0 กำลังเผชิญกับโลกภูมิรัฐศาสตร์การเมืองและเทคโนโลยีระหว่างประเทศที่มีความซับซ้อน และแตกต่างจากโลกเดิมที่มีความเห็นร่วมกัน (Consensus) เกี่ยวกับไซเบอร์สเปซที่ค่อนข้างชัดเจน สำหรับคนไทย 4.0 ซึ่งต่อไปในทุกมิติของชีวิตย่อมมีความเกี่ยวข้องกับเทคโนโลยีอินเตอร์เน็ตอย่างหลีกเลี่ยงไม่ได้ ควรตระหนักว่าการเชื่อมโยงกับไซเบอร์สเปซมีมิติด้านความมั่นคงของรัฐเสมอ คนไทย 4.0 อาจหลีกเลี่ยงไม่ได้ที่จะกลายเป็นส่วนหนึ่งของแพลตฟอร์มสหรัฐฯ หรือจีนในแต่ละประเด็นและแต่ละเทคโนโลยี ประเด็นสำคัญจึงอยู่ที่การกำกับดูแลที่สมดุลทั้งคุณค่าในเรื่องความมั่นคงของรัฐและคุณค่าเสรีนิยม เพื่อประกันความปลอดภัยทางไซเบอร์และความมั่นคงของชาติ

Executive Summary

With its rapid digital development, China becomes a leader in the area of digital economy. Chinese Cybersecurity Law 2017, the core law which underlies data security supervision and cybersecurity in the digital economy, was promulgated by the National People's Congress on 7 November 2016 and came into effect on 1 June 2017.

This research finds that China's cybersecurity law reflects the Chinese government's efforts to assert sovereignty on the Internet. China aims to manage cyberspace by giving the government the power to identify and control inappropriate behaviors in social network. To understand China's cybersecurity law, we must consider China's unique perspective towards cybersecurity. The Chinese concept of cybersecurity has a wider scope compared to that of Western version. In China, cybersecurity is achieved by regulating content on the Internet in order to maintain political and social stability. In addition, the treatment of personal information in this law reflects China's view on human rights.

Under China's cybersecurity law, network service providers operating activities related to critical infrastructure will be forced to take part in safeguarding cybersecurity. The issue of collecting local information is considered another difficult duty for these network service providers. It is unclear whether the measure will actually strengthen long-term cybersecurity. Local data collection measures could put entrepreneur at risk of being spied by local governments. Despite the law seeking to protect personal information, the government still has the power to access them with the aim of protecting national security.

Although the form and content of relevant Thai laws were based on EU and US models, there are insertions of content or features of Chinese models. Some Western countries have also begun to follow some Chinese models due to concerns over security threats, the technological competition between the superpowers, and cybersecurity. Therefore, the line between the Cyber Paternalism model of China and the Cyber Commons model of the Western world may not be clearly divided as in the past. Government intervention in cyberspace becomes a matter of degree.

A key lesson for Thailand is not to choose between the Chinese Cyber Paternalism model or the Western Cyber Commons model, but to strike a balance between the two

concepts through the appropriate mechanism and the design of the criteria or standards that limit the use of unreasonable judgments of the state.

From geopolitical perspective, this study sheds light on the shift from the clear consensus regarding the governance of cyberspace to two diverging models. Thai people in the era of 4.0 should bear in mind that the connection to cyberspace always have a security dimension. They may inevitably become part of the US platform or China's in different issues and technologies. The key point is to find the right balance between state security and liberal values to insure cybersecurity while safeguarding freedom.

บทคัดย่อ

งานวิจัยทำการวิเคราะห์บทบัญญัติสำคัญของกฎหมายความปลอดภัยทางไซเบอร์ของจีน ศึกษาเปรียบเทียบกับโมเดลกฎหมายของสหภาพยุโรปและสหรัฐอเมริกา รวมทั้งศึกษาเปรียบเทียบกับกฎหมายไทย จากการศึกษาพบว่า กฎหมายความปลอดภัยทางไซเบอร์ของจีนสะท้อนความพยายามของรัฐบาลจีนในการอ้างอำนาจอธิปไตยบนโลกอินเทอร์เน็ต โมเดลกฎหมายจีนเริ่มมีอิทธิพลต่อการบัญญัติกฎหมายของประเทศไทยในการกำกับดูแลเศรษฐกิจดิจิทัลในยุคไทยแลนด์ 4.0 ถึงแม้ว่าในทางรูปแบบและเนื้อหาของกฎหมายส่วนใหญ่ จะมีความพยายามยึดตามโมเดลของสหภาพยุโรปและสหรัฐอเมริกา แต่ก็มีการสอดแทรกเนื้อหาหรือลักษณะเด่นของโมเดลจีนด้วย แม้กระทั่งในประเทศตะวันตกเอง ก็เริ่มมีกระแสการเดินตามโมเดลจีน เนื่องจากความกังวลเรื่องภัยคุกคามต่อความมั่นคง การแข่งขันทางเทคโนโลยีระหว่างมหาอำนาจ และความปลอดภัยทางไซเบอร์

Abstract

This research analyses important provisions of China's cybersecurity law and conducts comparative studies with the European and U.S. cybersecurity regulatory models, as well as relevant Thai laws. The research finds that China's law reflects the country's assertion of its internet sovereignty. The Chinese cybersecurity regulatory model becomes influential on Thai laws regulating digital economy in Thailand 4.0 era. Despite the form and content of relevant Thai laws attempting to follow the European and US models, some provisions also reflect the Chinese model. Even the Western model itself also starts to converge with the Chinese model on cyber sovereignty because of increasing national security concerns, technological competition between superpowers, and cybersecurity risks.

สารบัญ

บทที่ 1

ภูมิหลังและแนวคิดพื้นฐานเกี่ยวกับความปลอดภัยทางไซเบอร์

ไซเบอร์สเปซ เป็นการสมมติถึงพื้นที่ที่มองไม่เห็น จับต้องไม่ได้ พื้นที่ดังกล่าวเป็นพื้นที่ในโลกดิจิทัล เชื่อมโยงถึงกันโดยอินเทอร์เน็ต ซึ่งหมายถึงระบบหรือเครือข่ายคอมพิวเตอร์ขนาดใหญ่ที่เชื่อมโยงเครือข่ายคอมพิวเตอร์ย่อยๆ ทั่วโลกเข้าไว้ด้วยกัน เพื่อแลกเปลี่ยนข้อมูลสื่อสารระหว่างกัน อาจกล่าวได้ว่า ทุกๆ กิจกรรมที่ทำโดยผ่านอินเทอร์เน็ตนั้นเกิดขึ้นบนไซเบอร์สเปซ เปรียบเทียบได้กับการอ่านหนังสือ หนังสือคือสื่อกลางที่ผู้เขียนส่งผ่านข้อมูลให้ผู้อ่าน เช่นเดียวกัน อินเทอร์เน็ตก็คือสื่อกลางที่ใช้เชื่อมต่อข้อมูลระหว่างกัน ส่วนการอ่านแล้วทำให้จินตนาเกิดเรื่องราวขึ้นในสมอง โลกในจินตนาการและความนึกคิดของผู้อ่าน ก็เปรียบเทียบได้กับพื้นที่ที่เรียกว่าไซเบอร์สเปซนั่นเอง

คำว่าไซเบอร์สเปซ ถูกสร้างขึ้นครั้งแรกโดย William Gibson นักเขียนชาวอเมริกันในปี ค.ศ. 1982 ในนวนิยายของเขาที่มีชื่อว่า ‘Burning Chrome’ ซึ่งหมายถึงโลกเสมือนจริงที่ถูกสร้างขึ้นโดยคอมพิวเตอร์ และได้เป็นที่รู้จักกันแพร่หลายมากขึ้นในปี ค.ศ. 1984 ผ่านนวนิยายอีกเล่มหนึ่งของเขาที่ชื่อว่า Neuromancer โดยคำว่า ‘cyber’ มีรากศัพท์มาจากภาษากรีกว่า ‘kybernetes’ ซึ่งหมายถึงกัปตัน หรือผู้ปกครอง ในขณะเดียวกัน คำว่า cyber ก็เกี่ยวข้องกับคำว่า ‘cyborg’ ซึ่งเป็นคำอธิบายถึงมนุษย์ครึ่งหุ่นยนต์ที่ผ่านกระบวนการดัดแปลงด้วยเทคโนโลยีชั้นสูง ในการเล่าเรื่องของ William Gibson ไซเบอร์สเปซคือพื้นที่โลกเสมือนเล็ก ๆ ในสังคมเมืองที่ถูกสร้างขึ้นเพื่อรับมือกับปัญหาอาชญากรรม การถูกกีดกันจากสังคม และความยากจน อย่างไรก็ดี ในภายหลังที่รู้จักกันแพร่หลาย ศัพท์นี้ถูกใช้กันอย่างแพร่หลายในวงการคอมพิวเตอร์ ไม่ได้หมายความเพียงพื้นที่ในนิยายของผู้สร้างอีกต่อไป แต่หมายถึงพื้นที่จริง ๆ บนโลกอินเทอร์เน็ต[1]

สถาบันมาตรฐานและเทคโนโลยีแห่งสหรัฐอเมริกา (NIST) ได้ให้นิยามของคำว่า ความปลอดภัยทางไซเบอร์ ไว้ว่า“ความสามารถในการป้องกันหรือปกป้องไซเบอร์เสปซจากการโจมตีทางไซเบอร์”[2] ในขณะที่หน่วยงานความมั่นคงปลอดภัยไซเบอร์และโครงสร้างพื้นฐานแห่งสหรัฐอเมริกาได้ให้นิยามไว้ว่า “ความสามารถในการป้องกันระบบ เครื่องมือ และข้อมูลจากการเข้าถึงที่ไม่ได้รับอนุญาต หรือจากอาชญกร และหมายถึงวิธีการในการรักษาความลับ ความสมบูรณ์ และความสามารถในการใช้งานของข้อมูลเหล่านั้น”[3]

---

[1]Fourkas, Vassilys. 2004. "WhatIs‘Cyberspace’?". Researchgate. https://www.researchgate.net/publication/328928631_What_is_'cyberspace'.

[2] "Cybersecurity - Glossary | CSRC". 2020. Csrc.Nist.Gov. https://csrc.nist.gov/glossary/term/cybersecurity.

[3] "Security Tip (ST04-001) What Is Cybersecurity?". 2009. Department Of Homeland Security. https://www.us-cert.gov/ncas/tips/ST04-001.

1.1 ภยันตรายจากไซเบอร์สเปซ

ในปัจจุบัน ภยันตรายจากไซเบอร์สเปซมีด้วยกันหลายรูปแบบ ซึ่งสามารถแยกเป็นกลุ่มโดยพิจารณาจากเป้าหมายของการโจมตี และประเภทของความรุนแรงที่เกิดจากการโจมตีนั้น ดังต่อไปนี้[4]

1.1.1 กรณีที่เป้าหมายของการโจมตีเป็นบุคคล

ในกรณีที่บุคคลตกเป็นเป้าหมายของการโจมตี วัตถุประสงค์มักเป็นการโจรกรรมเพื่อให้ได้มาซึ่งทรัพย์สิน โดยผู้โจมตีอาจจะใช้วิธีในเชิงรุกโดยการหลอกลวงเหยื่อเพื่อให้ได้ข้อมูลส่วนบุคคล (ยกตัวอย่างเช่น หมายเลขบัญชีธนาคาร หมายเลขประกันสังคม หรือ รหัสผ่านของบัญชีต่างๆ) หรืออาจจะใช้วิธีในเชิงรับ เช่น ปล่อยไวรัสเข้าไปในคอมพิวเตอร์ของเหยื่อเพื่อให้ได้ข้อมูลของเหยื่อ หากผู้โจมตีสามารถหลอกลวงระบบได้ว่าเขาคือบุคคลที่เป็นเจ้าของข้อมูลนั้น เขาสามารถทำอะไรก็ได้ในนามของเจ้าของข้อมูลนั้น เช่น การเปิดบัญชีบัตรเครดิตใหม่ หรือใช้คอมพิวเตอร์ของผู้ถูกโจมตีเพื่อใช้ในการขยายผลอื่นๆ ต่อไป นอกจากนี้ อาจเกิดกรณีที่ร้ายแรงกว่านั้น อาทิ การโจมตีเพื่อมุ่งทำลายตัวบุคคลโดยเฉพาะ ยกตัวอย่างเช่น ด้วยการใช้วิธีต่างๆ ที่กล่าวมา ผู้โจมตีสามารถนำข้อมูลส่วนบุคคลของเหยื่อมาเปิดเผยต่อสาธารณชน ทำให้เกิดความเสียหายต่อชื่อเสียงของผู้ถูกโจมตี

มีกรณีศึกษาที่โด่งดังคือการแบล็คเมล์นักแสดงสาวรายหนึ่ง ในปี ค.ศ. 2019 เบลล่า ธอร์น (Bella Thorne) นักแสดงหญิงชื่อดังชาวอเมริกา ได้ถูกแฮ็คเกอร์ข่มขู่ผ่านทวิตเตอร์ส่วนตัวว่าจะปล่อยภาพอนาจารของเธอสู่สาธารณะ หากเธอไม่ยอมส่งเงินให้ โดยแฮ๊คเกอร์ได้ภาพเหล่านั้นมาจากการเจาะระบบโทรศัพท์ อย่างไรก็ดี เบลล่า ธอร์น ได้แก้ปัญหาด้วยการโพสต์ภาพที่ถูกแบล็คเมย์เหล่านั้นสู่สาธารณะด้วยตนเอง เพื่อไม่ให้แฮ็คเกอร์สามารถหาประโยชน์จากภาพเหล่านั้นได้อีกต่อไป[5]

1.1.2 กรณีที่เป้าหมายของการโจมตีเป็นองค์กรธุรกิจ

ในกรณีที่องค์กรธุรกิจตกเป็นเป้าหมายของการโจมตี วัตถุประสงค์นั้นเป็นการโจรกรรมเช่นกัน โดยเป้าหมายของการโจรกรรมนั้นอาจเป็นได้ทั้งข้อมูลของทรัพย์สินทางปัญญา ข้อมูลของผู้บริโภค และบทสนทนาส่วนบุคคล ซึ่งเป็นประโยชน์ต่อตัวของผู้โจมตีเองหรือเป็นโทษกับผู้ถูกโจมตีก็ได้

---

[4] Jacob Quinn. 2017. "A Peek Over The Great Firewall: A Breakdown Of China'S New Cybersecurity Law". SMU Science & Technology Law Review 2 (20): 408-411.

[5] Calfee, Bailey. 2020. "Bella Thorne Posted Her Own Nudes After Blackmail Threats". Nylon. https://www.nylon.com/bella-thorne-nudes-hacker-blackmail.

กรณีศึกษาแรก คือการโจรกรรมข้อมูลความลับทางการค้าของบริษัทผลิตเหล็กรายใหญ่ที่สุดของโลก ThyssenKrupp โดยจากการตรวจสอบความปลอดภัยของระบบป้องกันประจำปี จึงได้พบว่าระบบป้องกันของบริษัทถูกเจาะโดยแฮ็คเกอร์ ส่งผลให้มีข้อมูลโครงการต่าง ๆ จำนวนมากของบริษัทถูกขโมยไป[6]

กรณีศึกษาที่สอง สำนักงานที่ปรึกษากฎหมาย Grubman Shire Meiselas & Sacks ซึ่งลูกค้าส่วนมากเป็นศิลปิน และดาราชื่อดังได้ถูกแฮ็ค ส่งผลให้ข้อมูลส่วนตัวของลูกค้า เช่นอีเมลและเบอร์โทรศัพท์ส่วนตัวถูกโจรกรรมไป ทั้งนี้แฮ็คเกอร์ได้เรียกค่าไถ่ 2.3 ล้านดอลล่าสหรัฐจากสำนักงานที่ปรึกษากฎหมายดังกล่าว นอกจากนี้ แฮ็คเกอร์ยังอ้างว่าตนมีข้อมูลหลักฐานการฟอกเงินของประธานาธิบดี โดนัลด์ ทรัมป์อีกด้วย[7]

นอกจากตัวอย่างของการโจรกรรมข้อมูลเพื่อผลประโยชน์ของตนเองแล้ว ในบางกรณี หากปรากฏว่าธุรกิจนั้นเป็นธุรกิจประเภทให้บริการ การทำให้บริการของธุรกิจนั้นหยุดชะงักลงก็อาจเป็นหนึ่งในวิธีการโจมตีก็ได้ เช่น การทำคำร้องขอในเว็บไซด์หลายๆ เว็บไซด์ (จากคอมพิวเตอร์ที่มีซอฟแวร์อันตราย) ทำให้เซิฟเวอร์ของผู้บริการที่รับคำร้องขอจากเว็บไซด์เหล่านั้นพร้อมกันทำงานไม่ไหว (หรือที่เรียกกันว่า ยิงเว็บ) การโจมตีดังกล่าวเป็นตัวอย่างของการทำให้เซิฟเวอร์ของบริษัท Dyn เป็นอัมพาต และเป็นเหตุให้เว็บไซด์ต่าง ๆ ของเช่น Facebook และ Twitter ต้องหยุดชะงักลง[8]

1.1.3 กรณีที่เป้าหมายของการโจมตีเป็นรัฐบาล

ในกรณีที่รัฐบาลตกเป็นเป้าหมายของการโจมตี มักเป็นไปเพื่อให้ได้ข้อมูลข่าวสาร หรือการเผยแพร่ข้อมูลอันเป็นเท็จ หรือแม้กระทั่งการรบกวนระบบการทำงานของเซิฟเวอร์ โดยผู้โจมตีอาจเป็นได้ทั้งประชาชนทั่วไปที่ไม่พอใจในรัฐบาล องค์กรที่ต้องการประกาศถึงการมีอยู่ของตน หรือแม้แต่รัฐบาลอื่น

สำหรับการโจมตีระบบโดยรัฐบาลประเทศอื่นนั้นมีตัวอย่างเช่น การกระทำของสำนักงานความมั่นคงแห่งชาติของสหรัฐอเมริกา ซึ่งอาศัยช่องโหว่ในระบบรักษาความปลอดภัยของข้อมูลในการแอบสังเกตการณ์กิจกรรมของประชาชนและรัฐบาลต่างประเทศ[9] ในบางครั้ง งานระบบสาธารณูปโภคก็อาจเป็นเป้าหมายของ

---

[6] Auchard, Eric, and Tom Käckenhoff. 2016. "Thyssenkrupp Secrets Stolen In 'Massive' Cyber Attack". U.S. Reuters. https://www.reuters.com/article/us-thyssenkrupp-cyber/thyssenkrupp-secrets-stolen-in-massive-cyber-attack-idUSKBN13X0VW.

[7] Battaglio, Stephen. 2020. "Celebrity Law Firm Won't Pay Ransom to Hackers Claiming to Have 'Dirty Laundry' On Trump". Los Angeles Times. https://www.latimes.com/entertainment-arts/business/story/2020-05-18/hackers-demand-42-million-to-keep-from-leaking-law-firms-stolen-data-on-president-trump.

[8] Woolf, Nicky. 2016. "Ddos Attack That Disrupted Internet Was Largest of Its Kind in History, Experts Say". The Guardian. https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet.

[9] Funk, Matthew. 2015. "Tragedy Of The Commons: Snowden'S Reformation And The Balkanization Of The Internet". Syracuse Journal Of Science And Technology Law 31: 49-52.

การโจมตีได้เช่นกัน ตัวอย่างเช่นการโจมตีระบบเพื่อขัดขวางการจ่ายกระแสไฟฟ้าไปสู่ประชาชน[10] หากการโจมตีเหล่านั้นถูกกระทำโดยต่างชาติ และได้สนธิกำลังร่วมกันกับกองทัพ ย่อมจะเกิดความเสียหายหนักขึ้นไปอีก

เป้าหมายของการโจมตีที่สำคัญคือ การโจมตีโครงสร้างพื้นฐานอินเทอร์เน็ต อินเตอร์เน็ตเป็นระบบเครือข่ายคอมพิวเตอร์ขนาดใหญ่ ดังนั้น จึงจำเป็นต้องมีโครงสร้างพื้นฐานด้านระบบเครือข่ายเพื่อรองรับการสื่อสารระหว่างคอมพิวเตอร์ อันได้แก่ ระบบเครือข่ายย่อย ซึ่งอาจเป็นเครือข่ายส่วนบุคคลหรือขององค์กรที่ต้องการเชื่อมต่อกับอินเตอร์เน็ต เช่น LAN, MAN หรือ WAN ระบบโครงข่ายการสื่อสาร เช่น โครงข่ายโทรศัพท์โครงข่าย Fiber Optics หรือ ระบบดาวเทียมเป็นต้น ตลอดจนเร้าเตอร์ (Router) ซึ่งเป็นอุปกรณ์สำหรับจัดการเส้นทางจราจรของข้อมูลที่ส่งผ่านอินเตอร์เน็ต หาก Routing and Domain Name System โดนโจมตี จะส่งผลกระทบต่อระบบทั้งหมด

สิ่งที่อันตรายที่สุดที่รัฐบาลต้องเผชิญกับการโจมตีเหล่านั้นคือการหยุดชะงักลงของบริการโครงสร้างพื้นฐานที่สำคัญ โดยหากบริการโครงสร้างพื้นฐานเหล่านั้นถูกโจมตี ประเทศชาติจะเกิดความวุ่นวายได้ มีข้อควรสังเกตว่า สิ่งใดจะเป็นโครงสร้างพื้นฐานในแต่ละประเทศ ก็สุดแล้วแต่ประเทศนั้น ๆ จะเป็นผู้กำหนด[11] เช่น กรณีการโจมตี Dyn แม้ว่าผู้ถูกโจมตีจะเป็นบริษัทเอกชน แต่สหรัฐอเมริกามองว่านั่นคือการโจมตีโครงสร้างพื้นฐาน เพราะการโจมตีทำให้เกิดความวุ่นวาย จากการที่บุคคลไม่สามารถเข้าใช้เว็บไซต์ในเซิฟเวอร์ของบริษัทได้[12] หรือในกรณีที่รัฐบาลประเทสออสเตรเลียออกมาประณามว่ากองทัพจีนอยู่เบื้องหลังการเจาะระบบป้องกันของหน่วยงานรัฐเพื่อโจรกรรมเอกสารทางการทูต[13]

---

[10] Polityuk, Pavel, Oleg Vukmanovic, and Stephen Jewkes. 2017. "Ukraine's Power Outage Was A Cyber Attack: Ukrenergo". U.S. Routers. https://www.reuters.com/article/us-ukraine-cyber-attack-energy/ukraines-power-outage-was-a-cyber-attack-ukrenergo-idUSKBN1521BA.

[11] Shackelford, Scott, and Amanda Craig. 2014. "Beyond The New “Digital Divide”: Analyzing The Evolving Role Of National Governments In Internet Governance And Enhancing Cyber-Security". Stanford Journal Of International Law 50: 119, 144.

[12] Woolf, Nicky. 2016. "Ddos Attack That Disrupted Internet Was Largest of Its Kind in History, Experts Say". The Guardian. https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet.

[13] Australian Associated Press, "Chinese Cyber-Attack Launched On WA Government". 2020. 9NEWS. https://www.9news.com.au/national/chinese-cyberattack-blamed-for-hack-on-wa-government/f1de86d4-67a6-498e-a95d-3624727a6856#close.

1.2 ลักษณะของการโจมตี

การกระทำอันเป็นภัยคุมคามทางไซเบอร์ (Cyber threat) ยังอาจแบ่งตามลักษณะของการโจมตี ได้เป็น

1.2.1 Web-based Attacks & System-based Attacks

Web-based Attacks คือ การโจมตีที่เกิดขึ้นบนเว็บไซต์หรือการใช้แอปพลิเคชั่น เพื่อเข้าถึงหรือเอาข้อมูลสำคัญของผู้ใช้งาน ล็อกอิน รหัสผ่าน เลขประจำตัวประชาชน เลขบัตรเครดิต

System-based Attacks คือ การโจมตีเพื่อควบคุมตัวเครื่องคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ โดยส่วนมากอาจก่อให้เกิดผลร้ายกับฮาร์ดแวร์ด้วย ส่งผลให้ระบบล่ม หรือทำให้ผู้ใช้งานสูญเสียความสามารถในการควบคุมคอมพิวเตอร์

1.2.2 Active Attacks and Passive Attacks

Active Attacks เป็นการโจมตีที่พยายามควบคุม ขัดขวาง รบกวนการใช้งานของผู้ใช้โดยตรง แตกต่างจาก Passive Attacks ที่จะเป็นการเรียนรู้ข้อมูลและนำข้อมูลที่ได้มาใช้ประโยชน์ โดยไม่รบกวนการใช้งานของผู้ใช้อินเทอร์เน็ต

1.2.3 Inside Attacks and Outside Attacks

แบ่งแยกโดยใช้จุดกำเนิดในการโจมตีเป็นหลัก โดย Inside Attacks เป็นการโจมตีที่เริ่มขึ้นภายใต้การรักษาความปลอดภัยของระบบคอมพิวเตอร์ย่อยๆ เช่น มีผู้ปล่อยไวรัสในคอมพิวเตอร์ของบริษัท ส่วน Outside Attacks เป็นการเริ่มการโจมตีจากภายนอกโดยไม่ได้รับอนุญาต เช่น แฮกเกอร์ทั่วไป บริษัทคู่แข่ง จนถึงผู้ก่อการร้ายไซเบอร์

1.3 ความตึงเครียดด้านความปลอดภัยทางไซเบอร์ระหว่างสหรัฐอเมริกาและจีน

สหรัฐอเมริกาได้ระบุว่าจีนเป็นมหาอำนาจด้านดิจิทัลที่เป็นภัยคุกคามที่สำคัญที่สุดต่อความมั่นคงแห่งชาติของสหรัฐอเมริกา[14] ส่วนจีนเองก็ออกมาระบุว่าตนเองก็เป็นเหยื่อของการโจมตีทางไซเบอร์เช่นเดียวกัน โดยเฉพาะจากสหรัฐอเมริกา[15] ทั้งสหรัฐอเมริกาและจีนต่างโจมตีอีกฝ่ายว่ามีการดำเนินการโจมตีทางไซเบอร์ประเทศตน สะท้อนให้เห็นความตึงเครียดระหว่างมหาอำนาจทางเทคโนโลยีทั้งสองฝ่าย และสะท้อนว่าภัยอันตรายในไซเบอร์สเปซมีมิติเกี่ยวข้องกับด้านความมั่นคงทั้งในทางการเมืองและเศรษฐกิจ

[14] Blinderman, Eric, and Myra Din. 2017. "Hidden By Sovereign Shadows: Improving The Domestic Framework For Deterring State-Sponsored Cybercrime". SSRN Electronic Journal 50: 889, 896-897. doi:10.2139/ssrn.3365244.

[15] Selby, John. 2017. "Data Localization Laws: Trade Barriers Or Legitimate Responses To Cybersecurity Risks, Or Both?". International Journal Of Law And Information Technology 25 (3): 213, 231. doi:10.1093/ijlit/eax010.

ในส่วนของการโจมตีโดยสหรัฐอเมริกามักมีเป้าหมายทางการเมืองเป็นสำคัญ หลังจากเอ็ดเวิร์ด สโนว์เดนเปิดโปงโครงการลับผิดกฎหมายโดยกระบวนการบนไซเบอร์เสปซ[16] การเปิดเผยเรื่องราวดังกล่าวของเอ็ดเวิร์ด สโนว์เดนทำให้สหรัฐอเมริกาถูกวิพากษ์วิจารณ์อย่างกว้างขวางในประชาคมโลก ก่อนการเปิดเผยนั้น ประเทศจีนได้เคยประเมินไว้ก่อนแล้วว่าสหรัฐอเมริกาเป็นผู้อยู่เบื้องหลังจากแฮ็คเครือข่ายของประเทศจีน โดยสำนักงานความมั่นคงแห่งชาติของสหรัฐอเมริกาได้ทำการเจาะระบบเพื่อล้วงข้อมูลสำคัญทางการเมืองและความลับทางการทหารของประเทศจีน[17]

ในทางตรงกันข้าม การโจมตีโดยจีนมักมีเป้าหมายทางเศรษฐกิจเป็นหลัก เดอะวอลล์สตรีทจัวนัลได้รายงานว่าจีน “มักทำการโจมตีทางไซเบอร์ด้วยบุคลากรจำนวนมากทั้งที่มาจากกองทัพและนอกกองทัพ โดยมีรัฐบาลเป็นผู้ชี้เป้าหมาย”[18] โดยจะเห็นได้ว่าการแฮ็คแต่ละครั้งของจีนล้วนเป็นไปเพื่อผลประโยชน์ในทางเศรษฐกิจ องค์กรธุรกิจหลายแห่งของสหรัฐอเมริกาที่เป็นเหยื่อในการแฮ็คนั้นรวมไปถึง Apple, Facebook, Google, Twitter และ the Washington Post[19] แรงกดดันต่อจีนในประเด็นเหล่านี้นำไปสู่การที่ในปี ค.ศ. 2015 ประธานาธิบดี สี จิ้นผิงของจีนได้ลงนามในข้อตกลงด้านไซเบอร์กับสหรัฐอเมริกา โดยข้อตกลงดังกล่าวได้ห้ามทั้งสาธารณรัฐประชาชนจีนและสหรัฐอเมริกาในการสนับสนุนการโจรกรรมทางข้อมูลเพื่อผลประโยชน์ทางเศรษฐกิจ

มีผู้ตั้งข้อสังเกตว่า สหรัฐอเมริกาได้แบ่งแยกการแฮ็คข้อมูลออกเป็น 2 ประเภท คือ การแฮ็คที่ดีและการแฮ็คที่ไม่ดี โดยการแฮ็คเพื่อผลประโยชน์ทางการเมืองจัดอยู่ในการแฮ็คประเภทแรก ส่วนการแฮ็คที่ไม่ดีคือการที่ประเทศจีนแฮ็คข้อมูลของบริษัทต่างชาติ เพื่อขโมยข้อมูลอันมีทรัพย์สินทางปัญญาสำหรับนำมาช่วยบริษัทเอกชนในประเทศจีนหรือรัฐวิสาหกิจของจีน[20]

ส่วนมุมมองของจีนนั้น จีนไม่เคยมองว่าตนเองเป็นผู้ล่า แต่กลับมองว่าตนเองเป็นเพียงเหยื่อที่ถูกโจมตีทางไซเบอร์ โดยมักจะประณามจากโจมตีทางไซเบอร์จากสหรัฐอเมริกา ยิ่งไปกว่านั้น ในการพัฒนาอาวุธทางไซเบอร์ เพื่อดำเนินการการแฮ็คของประเทศจีนนั้น ประเทศจีนมักจะกำกับไว้ว่าการพัฒนาขีดความสามารถใน

---

[16] Ewen MacAskill. 2013. "NSA Files Decoded: Edward Snowden's Surveillance Revelations Explained". The Guardian.https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded.

[17] Balke, Liudmyla. 2018. "China’S New Cybersecurity Law And U.S.-China Cybersecurity Issues". Santa Clara Law Review 58 (1): 141.

[18] Valentino-DeVries, Jennifer, and Danny Yadron. 2015. "Cataloging The World’S Cyberforces". The Wall Street Journal. https://www.wsj.com/articles/cataloging-the-worlds-cyberforces-1444610710.

[19] Moore, Stephen. 2014. "Cyber Attacks And The Beginnings Of An International Cyber Treaty". North California Journal Of International Law And Commercial Regulation 39 (1): 223, 253.

[20] Balke, Liudmyla. 2018. "China’S New Cybersecurity Law And U.S.-China Cybersecurity Issues". Santa Clara Law Review 58 (1): 141.

ด้านดังกล่าว มีสาเหตุมาจาก “ความกดดันซึ่งก่อโดยอำนาจทางเทคโนโลยีของสหรัฐอเมริกา”[21] จีนจึงได้ยกระดับเรื่องความปลอดภัยทางไซเบอร์ขึ้นเป็นวาระแห่งชาติด้านความมั่นคง เพื่อตอบสนองต่อภัยคุกคามจากสหรัฐอเมริกา

1.4 สำนักคิดที่เกี่ยวกับการกำกับดูแลไซเบอร์สเปซ

คำถามสำคัญคือรัฐควรจะเข้ามามีบทบาทอย่างไรในการกำกับดูแลไซเบอร์สเปซ รัฐควรแทรกแซงธุรกิจของเอกชนหรือไม่ เพื่อให้แน่ใจว่าข้อมูลที่เอกชนรวบรวมจากประชาชนได้รับการคุ้มครองที่เหมาะสม หรือรัฐควรป้องกันไม่ให้มีการเข้าถึงบางส่วนของอินเตอร์เน็ต เพื่อป้องกันไม่ให้ประชาชนเข้าไปตกอยู่ในภาวะเสี่ยงที่ข้อมูลส่วนตัวจะถูกลักลอบ ปัจจุบัน ในประเด็นเหล่านี้ มีสองสำนักคิดที่แตกต่างกันอย่างสุดขั้ว[22]

1.4.1 สำนัก Cyber Paternalism

ขั้วปรัชญาของสำนักคิดแรกชื่อว่า “Cyber Paternalism” หรือเรียกว่า “Data Nationalism” หรือ “Internet Sovereignty”[23] เป็นแนวคิดที่ว่าด้วยการขยายอำนาจของรัฐเข้าไปในไซเบอร์สเปซ และควบคุมการเคลื่อนไหวของข้อมูลซึ่งบันทึกไว้ในหน่วยของประเทศทั้งขาเข้าและขาออก[24]

ภายใต้แนวคิดนี้ เขตอำนาจบังคับใช้กฎหมายย่อมครอบคลุมไปถึงสื่อต่างๆ ในโลกความเป็นจริง และเพื่อให้การขยายขอบเขตอำนาจบังคับใช้กฎหมายเป็นไปอย่างมีประสิทธิภาพมากที่สุด ข้อมูลต่างๆ ที่เก็บรวบรวมได้ภายในประเทศควรถูกบังคับให้นำมาเก็บไว้ในแหล่งเก็บข้อมูลของประเทศด้วย โดยขั้นตอนดังกล่าวเรียกว่า data localization[25]

นอกจากนี้แล้ว แนวคิดนี้ยังสนับสนุนการอ้างเขตอำนาจบังคับใช้กฎหมายเหนือประชากรส่วนใหญ่บนโลกอินเตอร์เน็ต โดยไม่สนใจว่าข้อมูลเหล่านั้นเก็บไว้ที่ใด หากโดเมนนั้นได้เข้ามาในเขตอำนาจแล้ว ก็ย่อมตกอยู่ใต้การกำกับควบคุมนั้นด้วย[26]

---

[21] Lee, Jyh-An. 2014. "The Red Storm In Uncharted Waters: China And International Cyber Security". University Of Missouri-Kansas City Law Review 8 (4): 951, 953.

[22] Shackelford, Scott J. 2013. "Toward Cyber Peace: Managing Cyber Attacks Through Polycentric Governance". SSRN Electronic Journal 62 (5): 1281-1282.

[23] Shackelford, Scott J. "Toward Cyber Peace: Managing Cyber Attacks Through Polycentric Governance": 1283.

[24] Chander, Anupam. 2015. "Data Nationalism". Emory Law Journal 64 (3): 680.

[25] Chander, Anupam. "Data Nationalism": 680-681.

[26] Johnson, David R., and David G. Post. 1996. "Law And Borders - The Rise Of Law In Cyberspace". Stanford Law Review 48: 1367, 1394.

หลักฐานของการรับเอาแนวคิดของสำนักคิดนี้ไปใช้ อาจพิจารณาได้จากการพยายามผลักดันกฎหมาย Stop Online Piracy Act และ PROTECT IP Act ของสหรัฐอเมริกาในปี ค.ศ. 2011 ที่ถูกเสนอขึ้นโดยมีวัตถุประสงค์เพื่อใช้ต่อต้านเว็บไซต์ต่าง ๆ ที่ละเมิดกฎหมายลิขสิทธิ์ และสินค้าที่ละเมิดกฎหมายเหล่านั้น ด้วยการบังคับให้เจ้าของเว็บไซต์หรือผู้ให้บริการต้องทำการยืนยันตัวตนเสมอ นอกจากนี้ ทั้งผู้ให้บริการอินเทอร์เน็ต ผู้ให้บริการการชำระเงิน และผู้ให้บริการเครื่องมือค้นหาทางอินเทอร์เน็ตต้องทำการบล็อคเนื้อหาเว็บไซต์และไม่ให้ความร่วมมือแก่เว็บไซต์ใด ๆ ก็ตามที่ละเมิดกฎหมายลิขสิทธิ์[27] ทว่า ในการเสนอร่างกฎหมายนี้กลับมีผู้เห็นค้านจำนวนมาก รวมไปถึงผู้ให้บริการอินเทอร์เน็ต และผู้ให้บริการเครื่องมือค้นหาทางอินเทอร์เน็ตก็ต่างออกมาประท้วงด้วย ซึ่งต่างมองว่ากฎหมายนี้เป็นการเซ็นเซอร์เนื้อหา ปิดกั้นเสรีภาพ โดย Wikipedia ได้ประท้วงโดยการหยุดให้บริการเว็บไซต์ตนเองหนึ่งวันและแสดงข้อความว่า “ลองจินตนาการถึงโลกที่ปราศจากความรู้ฟรี ๆ ดูสิ” ("*Imagine a world without free knowledge.*") และบริษัท Google ได้ทำการล่ารายชื่อได้กว่า 7 ล้านรายชื่อเพื่อประท้วงการออกกฎหมายฉบับนี้[28] ทร่ามกลางแรงกดดันมากมายกฎหมายทั้งสองฉบับนี้ จึงไม่ผ่านกระบวนการพิจารณาในท้ายที่สุด

สำหรับทางฝั่งประเทศจีน แนวคิดของสำนักคิดนี้ถูกสะท้อนผ่าน Golden Shield Project ตั้งแต่ปี ค.ศ. 1990 และได้เปิดตัวสู่สาธารณชนในปี ค.ศ. 2000 ณ กรุงปักกิ่ง โดยวัตถุประสงค์ของโครการนี้คือเพื่อ “ปรับใช้ระบบสารสนเทศและเทคโนโลยีชั้นสูงเพื่อเพิ่มศักยภาพให้แก่การทำงานของเจ้าหน้าที่ตำรวจในการต่อต้านอาชญากรรม” ซึ่งเป็นผลให้การเข้าถึงเว็บไซต์ใด ๆ ก็ตามที่ถูกบล็อกในประเทศจีนไม่สามารถทำได้ และรัฐเองก็สามารถสอดแนมได้ว่าประชาชนของตนมีประวัติเข้าชมเว็บไซต์ใดอยู่ รวมไปถึงว่าประชาชนมีข้อมูลไหนเก็บไว้อย่างไร อย่างไรก็ดี เนื่องจากการใช้อินเทอร์เน็ตที่แพร่หลายอย่างรวดเร็วในประเทศ โครงการนี้จึงประสบปัญหาในการจัดการดูแลให้ครอบคลุมได้ ทำให้รัฐต้องจ้างทั้งหน่วยงานภายในประเทศและภายนอกประเทศมาช่วยศึกษาวิจัยและแก้ปัญหานี้ โดยหน่วยงานภายในประเทศได้แก่มหาวิทยาลัยชิงหัว ในขณะที่หน่วยงานภายนอกประเทศได้แก่ บริษัทเทคโนโลยีการสื่อสารและอุปกรณ์สารสนเทศสัญชาติแคนนาดา Nortel Networks[29]

---

[27] Law Library of Congress. "H.R.3261 - 112Th Congress (2011-2012): Stop Online Piracy Act". 2012. CONGRESS.GOV. https://www.congress.gov/bill/112th-congress/house-bill/3261.

[28] Engleman, Eric. 2011. "SOPA Bill Petition Collects 7 Million Signatures, According To Google". Washington Post. https://web.archive.org/web/20120120082947/http://www.washingtonpost.com/business/google-says-7 - million-signed-petition-against-anti-piracy-bills/2012/01/19/gIQAJ2MiBQ_story.html?tid=pm_business_pop.

[29] "The Great Firewall Of China: Background". 2011. Torfox A Stanford Project. https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreedomOfInformationChina/the-great-firewall-of-china-background/index.html.

จากการกระทำทั้งทางฝั่งของสหรัฐอเมริกาและจีนจะเห็นได้ว่ารัฐเองต่างมีความต้องการที่จะขยายขอบเขตอำนาจของตนเข้าไปในพื้นที่ไซเบอร์สเปซทั้งสิ้น ไม่ว่าจะด้วยเหตุผลด้านลิขสิทธิ์ เหตุผลด้านความมั่นคงปลอดภัย ซึ่งแท้จริงแล้ว อาจซ่อนนัยยะทางการเมืองไว้ การกระทำเหล่านี้ชี้ให้เห็นว่ารัฐเล็งเห็นปัญหาว่าในไซเบอร์สเปซ รัฐอาจเป็นได้เพียงแค่ผู้ใช้รายหนึ่ง เปรียบได้ดังบุคคลธรรมดาคนหนึ่งที่อาศัยอยู่ในสภาวะอนาธิปไตย อำนาจในการบัญญัติกฎหมาย บังคับใช้กฎหมายซึ่งจำกัดอยู่ในขอบเขตอธิปไตยของประเทศไม่สามารถใช้ได้ในไซเบอร์สเปซที่ไร้พรมแดน ด้วยเหตุนี้ รัฐจึงมีการออกกฎหมายมากมายเพื่อก้าวล้ำเข้ามาในไซเบอร์สเปซ เพื่อให้กฎหมายของตนสามารถบังคับใช้ได้ต่อไป อนึ่ง เมื่อสังเกตปฏิกิริยาของประชาชนที่มีต่อ Cyber Paternalism ทั้งในฝั่งของสหรัฐอเมริกาและประเทศจีนแล้ว จะสะท้อนให้เห็นว่า ในประเทศประชาธิปไตยที่ประชาชนยึดมั่นในเสรีภาพและสิทธิความเป็นส่วนตัวของตนเอง หากประชาชนเห็นว่าเนื้อหาของกฎหมายเองเป็นการละเมิดสิทธิที่ชัดเจน ประชาชนย่อมมีเสรีภาพในการชุมนุมเพื่อไม่ให้ร่างกฎหมายนั้นผ่านไป ผลจึงทำให้การที่รัฐออกกฎหมายล่วงล้ำเข้ามาในไซเบอร์สเปซทำได้ยาก ในขณะที่ในประเทศที่ประชาชนหรือรัฐมองว่าความปลอดภัยส่วนรวมหรือความมั่นคงของรัฐสำคัญกว่าสิทธิส่วนบุคคล การออกกฎหมายเข้าไปควบคุมไซเบอร์จะทำได้ง่ายและมีเนื้อหาที่สุดโต่งมาก สำหรับประเทศจีนเอง แนวคิดเรื่องสิทธิมนุษยชนหรือเสรีภาพต่าง ๆ เป็นเพียงสิทธิ ๆ หนึ่งที่รัฐมอบให้เท่านั้น ไม่ใช่สิทธิตามธรรมชาติที่ประชาชนมีอยู่โดยชอบธรรมมาแล้วแต่ต้นเพื่อใช้อ้างยันแก่รัฐที่เป็นผู้กดขี่ของตน ดังเช่นชาติประชาธิปไตยในฝั่งตะวันตกด้วยแนวคิดที่แตกต่างออกไปนี้ จึงทำให้รัฐจีนมองว่าสิทธิดังกล่าว รัฐสามารถช่วงชิงคืนหรือจำกัดมันได้เสมอ ดังนั้น กฎหมายที่อนุญาตให้รัฐสอดแนมประชาชนจึงเป็นสิ่งที่ประชาชนจีนไม่ได้รู้สึกกระทบกระเทือนตนเองมากเท่าใดนัก

อนึ่ง มีข้อสังเกตว่า แท้จริงแล้ว สหรัฐอเมริกาควรเป็นประเทศที่ประชาชนเห็นด้วยกับการออกกฎหมายล่วงล้ำเข้าสู่ไซเบอร์สเปซมากที่สุด เนื่องจากสหรัฐอเมริกาเคยมีบทเรียนจากเหตุวินาศกรรม 11 กันยายน ปี ค.ศ. 2001 ดังนั้น สถานการณ์นี้อาจสร้างความได้เปรียบแก่รัฐในการออกกฎหมายเพื่อสอดแนมประชาชนเพื่อเหตุผลในด้านการป้องกันการก่อการร้าย ทว่า เสียงประชาชนส่วนใหญ่ก็ยังไม่เห็นด้วยกับการอนุญาตให้รัฐสอดแนมประชาชนทางอินเทอร์เน็ตด้วยเหตุผลใด ๆ โดยอาจเป็นเพราะประชาชนเห็นว่าสิทธิส่วนตัวของตนเองมีความสำคัญไม่แพ้ความมั่นคงของรัฐ ปัจจุบัน จึงมีข่าวลือเพียงว่าหน่วยงานของรัฐได้สอดแนมประชาชนตนเองอย่างลับ ๆ แทน โดยที่ไม่มีกฎหมายใดมารองรับ แต่สำหรับประเทศจีนเอง ซึ่งไม่เคยผ่านเหตุการณ์รุนแรงใด ๆ กลับเป็นที่แปลกประหลาดว่าเหตุใดประชาชนกลับไม่คัดค้านที่จะให้รัฐออกกฎหมายมาบังคับแก่ตนเอง กรณีนี้มีคำตอบเดียวคือ ประชาชนเห็นว่าหน่วยทางสังคมที่เล็กที่สุดไม่ใช่ตนเอง แต่เป็นครอบครัว แนวคิดนี้เป็นปรัชญาพื้นฐานของสังคมจีนมาแต่ดั้งเดิม ดังนั้น จึงไม่มีเหตุผลใดที่จะตั้งคำถามกับการที่รัฐออกกฎหมายมาเพื่อรองรับความปลอดภัยของตนรอบตัว ในขณะเดียวกัน ในแนวคิดของชาวจีน สิทธิมนุษยชน หรือเสรีภาพต่าง ๆ จะเกิดขึ้นไม่ได้เลยหากรัฐไม่มอบให้ ดังนั้น ความมั่นคงของรัฐจึงสำคัญกว่าสิทธิหรือเสรีภาพใด ๆ ทั้งมวล ปัจจุบัน จึงเห็นได้ว่า ประเทศจีนมีกฎหมายจำนวนมากที่ถูกบัญญัติและลุกคืบเข้าไปในไซเบอร์สเปซ เพื่อเป็นการสถาปนาอำนาจอธิปไตยของตนในภาวะที่ไร้รัฐแห่งนั้น

1.4.2 สำนัก Cyber Commons

ขั้วปรัชญาของสำนักคิดขั้วตรงข้ามมีชื่อว่า “Cyber Commons” กลับมีความเชื่อว่าขอบเขตอำนาจบังคับใช้กฎหมายแยกกันต่างหากกับไซเบอร์สเปซ ขอบเขตอำนาจบังคับใช้กฎหมายจะใช้บังคับได้มากน้อยเพียงใด ย่อมขึ้นกับว่าใครเป็นผู้บริหารจัดการโดเมนของเว็บไซต์นั้นๆ มิใช่ขึ้นอยู่กับว่าแหล่งข้อมูลนั้นจะถูกเก็บไว้ ณ ที่ใด[30] มาตรการรักษาความปลอดภัยของโดเมนควรถูกควบคุมอยู่แล้วโดยมาตรฐานอุตสาหกรรม ซึ่งเป็นระดับความระมัดระวังตามกฎหมายที่ใช้ในการอ้างถึงเมื่อเกิดกรณีพิพาทระหว่างบริษัทผู้ให้บริการกับคู่กรณี[31] มาตรฐานเช่นว่านี้คือผลของการร่วมมือกันระหว่างภาครัฐและเอกชน องค์กรธุรกิจ นักกฎหมาย และนักวิชาการเพื่อสร้างความมั่นคงให้กับโลกไซเบอร์[32] ซึ่งบุคคลเหล่านี้ต่างก็เป็นผู้มีส่วนได้เสียกับการปกครองบนโลกอินเตอร์เน็ต

หากพิจารณาในด้านคำศัพท์ จะพบว่า Commons หมายถึง ที่ดินหรือทรัพยากรที่เป็นของชุมชนและมีลักษณะเป็นทรัพย์สินร่วมกัน มิใช่ของผู้ใดผู้หนึ่ง กล่าวคือเป็นทรัพย์สินสาธารณะ การมองว่าไซเบอร์สเปซเป็นทรัพย์สินสาธารณะ เช่นเดียวกันกับ น้ำ อากาศ หรือพื้นที่ในอวกาศ เท่ากับเป็นการปฏิเสธไม่ให้ผู้ใช้งานหน่วยหนึ่งหน่วยใดมีอำนาจเหนือกว่ากันในการใช้ทรัพยากรนั้น

เมื่อกล่าวถึงคำว่า Commons แล้ว สิ่งที่ต้องพูดตามมาเสมอก็คือบทความ โศกนาฏกรรมของทรัพย์สินร่วม หรือ ‘The Tragedy of the Commons’ ของ Garrett Hardin โดยมีใจความสำคัญว่า เมื่อทรัพยากรใดกลายเป็นของส่วนรวมแล้ว ปัจเจกชนแต่ละรายจะพยายามใช้ทรัพยากรนั้นเพื่อก่อให้เกิดประโยชน์กับตนอย่างสูงสุด เมื่อเป็นเช่นนั้นแล้ว ทรัพย์สินร่วมนั้นก็จะเสียหายและไม่สามารถก่อให้เกิดประโยชน์แก่ปัจเจกชนรายใดได้อีก ตัวอย่างเช่น หมู่บ้านแห่งหนึ่งมีป่าที่อุดมสมบูรณ์เป็นทรัพย์สินร่วมกัน ในวัน ๆ หนึ่งจะมีชาวบ้านเข้าป่าไปหาผลไม้ ตัดไม้มาสร้างบ้านของตน เผาป่าเพื่อสร้างพื้นที่เพาะปลูก ทว่า มิได้มีใครสนใจที่จะดูแลรักษาป่านั้นเลย เมื่อวันเวลาผ่านไป ชาวบ้านจะไม่สามารถหาประโยชน์จากพื้นที่ป่าที่เสื่อมโทรมแห่งนั้นได้อีก เหตุการนี้แสดงให้เห็นว่าการมีอยู่ของทรัพย์สินร่วมทำให้ผู้ใช้งานขาดซึ่งความรู้สึกรับผิดชอบ ตรงกันข้ามกับทรัพย์สินที่กรรมสิทธิ์อยู่ในความครอบครองของเอกชน ซึ่งเอกชนพร้อมที่จะดูแลรักษาเป็นอย่างดี

---

[30] Johnson, David R., and David G. Post. 1996. "Law And Borders - The Rise Of Law In Cyberspace": 1378, 1380.

[31] Shackelford, Scott J., Andrew A. Proia, Brenton Martell and Amanda N. Craig. 2014. “Toward a Global Cybersecurity Standard of Care? Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices.”: 305, 311.

[32] Eichensehr, Kristen. 2015. "The Cyber-Law Of Nations". *Georgetown Law Journal*, 317, 346.

หากพิจารณาเรื่องโศกนาฏกรรมของทรัพย์สินร่วมผ่านเหตุการณ์บนไซเบอร์สเปซแล้ว จะเห็นได้ว่าไม่ต่างกันเท่าใดนัก ไซเบอร์สเปซเปรียบเสมือนป่าที่อุดมสมบูรณ์ เป็นไปด้วยข้อมูลต่าง ๆ ที่สำคัญ หากปล่อยให้ปัจเจกชนดูแลกันเองโดยปราศจากผู้มีอำนาจเหนือกว่าเข้ามาควบคุม ก็อาจเกิดการโจรกรรมข้อมูล การละเมิดข้อมูลต่าง ๆ ทำให้สุดท้ายแล้ว ไซเบอร์สเปซกลายเป็นพื้นที่อันตรายที่ไม่มีใครกล้าเข้าไป ส่งผลไซเบอร์สเปซที่เคยแบ่งปันข้อมูลกันได้อย่างไร้พรมแดน แพร่หลาย และเสรีก็จะใช้ประโยชน์ไม่ได้อีก ดุจดั่งป่าที่เสื่อมโทรมนั่นเอง

นอกจากนี้ แนวคิดเรื่อง Cyber Commons ก็คือการยืนหยัดในเรื่องภาวะอนาธิปไตยของไซเบอร์สเปซ และเชื่อว่าทุกคนบนไซเบอร์สเปซจะร่วมมือกันเพื่อควบคุมกันเองเพื่อก่อให้เกิดความสงบสุข ดังสังคมยูโทเปียที่สังคมขับเคลื่อนได้เองด้วยความช่วยเหลือเกื้อกูลกัน มิใช่เพราะรัฐบังคับบัญชา ทว่า ในความเป็นจริงแล้ว มนุษย์ทุกคนล้วนมีความต้องการของตนเองและมักเห็นแก่ประโยชน์ส่วนตน หากเอกชนจะก่อกำแพงล้อมรั้วบ้านเพื่อป้องกันโจร ก็คงจะล้อมรั้วแต่เพียงรอบบ้านของตัวเองเท่านั้น เช่นเดียวกับที่เอกชนอาจหวงแหนข้อมูลของตนเอง แต่หากมีข้อมูลผู้อื่นมาเก็บไว้ในมือก็อาจจะไม่ได้ดูแลให้ดีได้เท่าข้อมูลของตัวเอง เพราะเห็นว่าความสำคัญไม่เท่ากัน นอกจากนี้ หากเอกชนรู้ว่าตนเองมีโอกาสขโมยโดยที่ไม่มีใครจับได้ เอกชนก็คงเลือกที่จะขโมยอยู่นั่นเอง ซึ่งไซเบอร์สเปซเป็นสิ่งที่เอื้อให้เกิดโอกาสนั้นเป็นอย่างยิ่ง ประการแรก การขโมยข้อมูลก็คือการทำสำเนาข้อมูลนั้นแล้วจากไป ผลคือผู้ที่ขโมยอาจไม่คิดว่าสิ่งที่ตนทำอยู่นั้นเป็นความผิด เนื่องจากข้อมูลก็ยังคงอยู่กับตัวเจ้าของอยู่ และในประการถัดมา การจับขโมยบนไซเบอร์สเปซไม่ใช่เรื่องง่าย ยิ่งแฮ็คเกอร์ใช้เทคนิคชั้นสูงมากเท่าใด โอกาสตามตัวยิ่งน้อยลง สภาวะที่ “ไม่สามารถจับมือใครดมได้” ได้ยั่วยวนให้ผู้ใช้งานทั้งหลายทำร้ายผู้อื่นบนสภาวะไร้รัฐ ณ ไซเบอร์สเปซแห่งนี้ อย่างไรก็ดี ถึงแม้ว่าภาวะอนาธิปไตยของไซเบอร์สเปซที่แฝงมากับ แนวคิดเรื่อง Cyber Commons ทำให้ไซเบอร์สเปซกลายเป็นพื้นที่อันตราย แต่หากเทียบกับความปลอดภัยที่ได้มาจากการแทรกแซงของรัฐแล้ว อาจมีผู้คนเห็นว่าการยอมถูกละเมิดโดยเอกชนด้วยกันอาจจะเป็นตัวเลือกที่ดีกว่า

ในบทนี้ได้กล่าวถึงภยันตรายในโลกไซเบอร์ รวมทั้งลักษณะของการโจมตีในโลกไซเบอร์ ซึ่งเป็นสาเหตุให้มีความจำเป็นที่จะต้องมีการออกกฎเกณฑ์ในการกำกับดูแลไซเบอร์สเปซและความปลอดภัยทางไซเบอร์ ยิ่งในกรณีของประเทศจีนและสหรัฐอเมริกา ซึ่งต่างก็เป็นมหาอำนาจในโลกไซเบอร์ ทั้งสองฝ่ายต่างถูกกล่าวหาว่าเป็นประเทศที่อยู่เบื้องหลังการโจมตีทางไซเบอร์ของอีกประเทศ ในขณะเดียวกัน ทั้งสองประเทศก็มองว่าตนตกเป็นเป้าหมายของการถูกโจมตีทางไซเบอร์ ข้อสังเกตที่น่าสนใจคือ สหรัฐอเมริกาและจีนมีลักษณะการโจมตีทางไซเบอร์ที่แตกต่างกัน โดยการโจมตีของสหรัฐอเมริกามักมีเป้าหมายทางการเมืองเป็นหลัก ขณะที่การโจมตีของจีนมีเป้าหมายทางเศรษฐกิจเป็นหลัก ดังนั้น จะเห็นได้ว่าความปลอดภัยทางไซเบอร์มีความเชื่อมโยงกับความมั่นคงทางการเมืองและเศรษฐกิจอย่างหลีกเลี่ยงไม่ได้

ด้วยเหตุนี้จึงเกิดคำถามว่า รัฐควรจะเข้ามามีบทบาทมากน้อยเพียงใดในการกำกับดูแลไซเบอร์สเปซ ปัจจุบันมีสองสำนักคิดที่แตกต่างกันอย่างสุดขั้ว ได้แก่ สำนัก Cyber Paternalism และสำนัก Cyber Commons ซึ่งเป็นพื้นฐานในการทำความเข้าใจแนวความคิดเกี่ยวกับการกำกับดูแลทางไซเบอร์ของประเทศต่างๆ ในบทถัดไป จะกล่าวถึงแนวคิดเกี่ยวกับการกำกับดูแลทางไซเบอร์ของประเทศจีน ซึ่งเป็นตัวแทนความคิดของสำนัก Cyber Paternalism ที่โดดเด่นในโลกปัจจุบัน

บทที่ 2

แนวคิดของประเทศจีนในเรื่องความปลอดภัยทางไซเบอร์

เมื่อพิจารณามุมมองและแนวคิดพื้นฐานของสหรัฐอเมริกาและสหภาพยุโรป เปรียบเทียบกับประเทศจีนต่อคำว่า “ความปลอดภัยทางไซเบอร์” (Cybersecurity) พบว่ามีความแตกต่างกันในระดับความคิดพื้นฐาน กล่าวคือ สหรัฐอเมริกาและสหภาพยุโรปมีความคิดสอดคล้องกับสำนักคิด Cyber Commons โดยมองว่าอินเตอร์เน็ตคือช่องทางเปิด ควรส่งเสริมให้สามารถเข้าถึงได้อย่างเสรี นโยบายต่างๆ เกี่ยวกับความปลอดภัยทางไซเบอร์ควรเกิดจากการพัฒนาร่วมกันระหว่างภาครัฐและเอกชน ด้วยแนวความคิดว่าเครือข่ายนั้นเป็น “สินทรัพย์ร่วมกัน” และการเป็นสินทรัพย์ร่วมกันเป็นพื้นฐานให้เกิดการสร้างมาตรฐานในการดูแลรักษาความปลอดภัยไซเบอร์ ในขณะที่รัฐบาลจีนกลับเป็นตัวแทนของแนวคิด Cyber Paternalism ที่โดดเด่น โดยรัฐบาลจีนได้เชื่อมาอย่างยาวนานแล้วว่าอินเตอร์เน็ตต้องถูกควบคุม และเนื่องจากว่าประเทศจีนต้องการที่จะเป็นอิสระจากอิทธิพลของประเทศอื่น ด้วยเหตุนี้ประเทศจีนจึงสนับสนุนแนวคิดว่าด้วยอธิปไตยไซเบอร์ ประเทศจีนมองว่าความปลอดภัยทางไซเบอร์คือความมั่นคงของชาติ และกฎหมายความปลอดภัยทางไซเบอร์ก็คือสิ่งที่บ่งบอกว่าประเทศจีนมีความพยายามในการยกระดับความมั่นคงของชาติตนทั้งในด้านการเมืองและเศรษฐกิจ

ในการทำความเข้าใจกฎหมายความปลอดภัยทางไซเบอร์ของจีน จึงมีความจำเป็นที่จะต้องทำความเข้าใจแนวคิดที่เกี่ยวข้องของประเทศจีนในเรื่องความปลอดภัยทางไซเบอร์ อันได้แก่ ความปลอดภัยทางไซเบอร์ในมุมมองของจีน ความสัมพันธ์ระหว่างความปลอดภัยทางไซเบอร์กับระบบสังคมนิยมอันมีเอกลักษณ์แบบจีน แนวความคิดว่าด้วยความเป็นอิสระทางเทคโนโลยีของจีน แนวความคิดว่าด้วยอธิปไตยไซเบอร์ และแนวความคิดเกี่ยวกับสิทธิมนุษยชนของประเทศจีน

2.1 ความปลอดภัยทางไซเบอร์ในมุมมองของจีน

กฎหมายความปลอดภัยทางไซเบอร์ของจีนมีขอบเขตที่กว้างขวางกว่านิยามความปลอดภัยทางไซเบอร์ที่เข้าใจกันในตะวันตก ในขณะที่ชาติตะวันตกให้ความระมัดระวังอันตรายจากโลกไซเบอร์ที่มีต่อเทคโนโลยี ประเทศจีนกลับให้ความระมัดระวังอันตรายจากโลกไซเบอร์ที่มีต่อความคิดและอุดมการณ์ทางการเมือง ยิ่งไปกว่านั้น ประเทศจีนยังมีการเซ็นเซอร์เนื้อหาและแนะนำวิธีการแสดงความเห็นบนอินเทอร์เน็ตที่เหมาะสม กิจกรรมออนไลน์หรือข้อมูลข่าวสารใดๆ ก็ตามที่ทำลายเสถียรภาพทางสังคมและการเมืองจะถูกมองว่าเป็นภัยต่อความปลอดภัยทางไซเบอร์ในมุมมองของจีน กรอบแนวคิดของคำว่าความมั่นคงปลอดภัยไซเบอร์ในมุมมองของประเทศจีนจึงมีความกว้างขวางมากกว่าประเทศอื่น

ในหนังสือปกขาว เผยแพร่โดยสำนักงานข้อมูลข่าวสารแห่งคณะมุขมนตรีจีน ปี ค.ศ. 2010 ได้กล่าวถึงนโยบายของรัฐบาลในการปกป้องความปลอดภัยทางไซเบอร์ไว้ และประกาศความมุ่งหมายที่จะกำจัดเนื้อหาที่

“ต่อต้านหลักการสำคัญในรัฐธรรมนูญ เป็นอันตรายต่อความมั่นคงของรัฐ เปิดเผยความลับของชาติ บ่อนทำลายชาติและความสามัคคี ทำลายเกียรติหรือผลประโยชน์ของประเทศ ส่งเสริมให้เกิดความเกลียดชังหรือเหยียดหยามศีลธรรมอันดีของสังคม ฝ่าฝืนนโยบายของชาติว่าด้วยการนับถือศาสนา โฆษณาเนื้อหาลัทธินอกรีต กระจายข่าวลือ สร้างความปั่นป่วนให้กับสังคม เผยแพร่สื่อลามกอนาจาร การพนัน ความรุนแรง การก่อการร้ายหรืออาชญากรรมอื่น การล้อเลียนเสียดสี ละเมิดสิทธิของผู้อื่น หรือเนื้อหาอื่นที่มีลักษณะต้องห้ามตามกฎหมายหรือระเบียบของฝ่ายบริหาร”[33]

ข้อความนี้สะท้อนให้เห็นถึงมุมมองของจีนที่มีต่อความปลอดภัยทางไซเบอร์อย่างชัดเจนว่าให้ความสำคัญกับเสถียรภาพทางสังคม อำนาจรัฐ และความสามัคคีของคนในชาติ

มุมมองที่เป็นเอกลักษณ์ของจีนนี้อาจพบได้จากการเสนอให้ร่างประมวลข้อปฏิบัติระหว่างประเทศในการจัดการความมั่นคงระหว่างประเทศ (the International Code of Conduct for Information Security) ซึ่งนำเสนอโดยประเทศจีน รัสเซีย ทาจิกิสถาน และอุซเบกิสถาน อันทำขึ้น ณ สมัชชาใหญ่แห่งสหประชาชาติ ในเดือนกันยายน ปี ค.ศ. 2011[34] เพื่อให้ข้อมูลข่าวสารบนโลกนี้ได้รับความปลอดภัย โดยประมวลนี้ร้องขอให้ประเทศต่างๆ ร่วมกันต่อสู้กับ “อาชญากรรมและการก่อการร้าย” ซึ่งรวมไปถึง “การป้องกันไม่ให้มีการเผยแพร่ข้อมูลที่ก่อให้เกิดการก่อการร้ายหรือข้อมูลที่เป็นของกลุ่มลัทธิหัวรุนแรง หรือข้อมูลที่บ่อนทำลายเสถียรภาพทางเศรษฐกิจ สังคม และการเมืองของประเทศอื่น รวมไปถึงข้อมูลใดที่บ่อนทำลายวัฒนธรรมหรือศีลธรรมของประเทศนั้น” อย่างไรก็ดี แม้ข้อเสนอให้จัดทำประมวลนี้จะไม่ได้รับความเห็นชอบจากสหรัฐอเมริกา[35] ข้อความต่าง ๆ ในประมวลนี้ก็สะท้อนให้เห็นถึงมุมมองของประเทศจีนที่มีต่อความปลอดภัยทางไซเบอร์ได้เป็นอย่างดีว่าประเทศจีนต้องการควบคุมและสนับสนุนเสถียรภาพทางการเมืองและสังคม

อีกสิ่งหนึ่งที่สะท้อนให้เห็นแนวคิดของประเทศจีนที่มีต่อความมั่นคงไซเบอร์อย่างชัดเจนคือมาตรการที่บังคับให้ผู้ให้บริการทางโครงข่ายมีหน้าที่ต้องเรียกเก็บชื่อจริงของผู้ใช้งานของตนไว้ เพื่อที่รัฐบาลเชื่อว่าการใช้อินเทอร์เน็ตอย่างมีอารยะจะเกิดขึ้นได้ ก็ด้วยการกำจัดข่าวลือ การใช้คำหยาบคาย และเนื้อหาที่เลวร้ายต่างๆ บนโลกอินเทอร์เน็ต นอกจากนี้ กฎหมายความปลอดภัยทางไซเบอร์ยังประกอบไปด้วยมาตการเพื่อคุ้มครอง

---

[33] Information Office of the State Council the People's Republic of China. 2010. "Govt. White Papers - The Internet In China". 2010. China.Org.Cn. http://www.china.org.cn/government/whitepaper/2010-06/08/content_
20208007.htm.

[34] McKune, Sarah. 2015. "Analysis Of International Code Of Conduct". The Citizen Lab. https://citizenlab.ca/2015/09/international-code-of-conduct/.

[35] เรื่องเดียวกัน.

ความปลอดภัยของเด็ก[36] ซึ่งพบได้ยากในกฎหมายความปลอดภัยทางไซเบอร์ของประเทศอื่น นอกจากนี้ พฤติกรรมต้องห้ามอันจัดว่าเป็นอันตรายต่อความปลอดภัยไซเบอร์ได้แก่

"การใช้โครงข่ายไปในทางที่ทำลายความมั่นคง ชื่อเสียง หรือผลประโยชน์ของชาติ รวมไปถึงการโค่นล้มอำนาจอธิปไตยของประเทศหรือเป็นภัยต่อคุณค่าทางสังคมนิยม การปลุกระดมให้เกิดการแบ่งแยกดินแดน หรือการสร้างความแตกแยกในชาติ การสนับสนุนกลุ่มก่อการร้ายหรือลัทธิหัวรุนแรง การปลุกระดมให้เกิดความเกลียดชังหรือการแบ่งแยกชาติพันธุ์ การเผยแพร่เนื้อหาที่มีความรุนแรง เนื้อหาลามกอนาจาร หรือการแพร่กระจายซึ่งข้อมูลที่ผิดพลาดอันส่งผลกระทบต่อระเบียบของสังคมหรือระบบเศรษฐกิจ การทำลายชื่อเสียงละเมิดสิทธิส่วนตัวและทรัพย์สินทางปัญญา หรือสิทธิอื่นตามกฎหมายต่างๆ"[37]

ตั้งแต่ที่กฎหมายนี้มีผลบังคับใช้ ทุกความสนใจต่างมุ่งไปยังมาตรการการควบคุมเนื้อหาต่าง ๆ และระเบียบเพิ่มเติมที่ออกมาควบคู่กัน เช่น ระเบียบฝ่ายบริหารว่าด้วยการจัดการเนื้อหาและการให้บริการบนอินเทอร์เน็ต ซึ่งแสดงให้เห็นถึงความพยายามของรัฐในการกวาดล้างเนื้อหาต่างๆ บนอินเทอร์เน็ตอันนำไปสู่การเรียกค่าปรับปริมาณมหาศาลจาก 3 บริษัทผู้ให้บริการอินเทอร์เน็ต อันได้แก่เท็นเซ็น ไป่ตู้ และซินล่าง เนื่องจาก 3 บริษัทนี้ล้มเหลวในการบริหารช่องทางการให้บริการของตัวเองตามกฎหมายนี้ โดยปรากฏว่ามีผู้ใช้บางราย "เผยแพร่เนื้อหาที่มีความรุนแรง ข่าวลือต่างๆ สื่อลามกอนาจาร และเนื้อหาที่บ่อนทำลายความมั่นคงของชาติ ความปลอดภัยของสาธารณะ และระเบียบของสังคม" [38]

นอกจากนี้ แมริออทอินเตอร์เนชั่นแนล (Marriott International) ซึ่งเป็นบริษัทที่ประกอบธุรกิจโรงแรมข้ามชาติก็ถูกลงโทษเนื่องจากล้มเหลวในการปฏิบัติตามระเบียบว่าด้วยการโฆษณาและกฎหมายความปลอดภัยทางไซเบอร์นี้ด้วยเช่นกัน โดยโทษที่บริษัทนี้ได้รับคือการถูกสำนักงานข่าวสารอินเทอร์เน็ตของเซี่ยงไฮ้ปิดเว็บไซต์เวอร์ชั่นภาษาจีนและระงับการใช้งานของแอปพลิเคชันบริษัทเป็นเวลาหนึ่งสัปดาห์[39] ทั้งที่จริงแล้วสิ่งที่บริษัทแมริออทอินเตอร์เนชั่นแนลกระทำไม่ได้เกี่ยวข้องกับความปลอดภัยทางไซเบอร์โดยตรงเลย หากเพียงแต่แสดงชื่อฮ่องกง มาเก๊า ไต้หวัน และทิเบต ในฐานะรายชื่อประเทศเพื่อให้ลูกค้าได้ทำการกรอกลงไปในแบบสำรวจ ทว่ารัฐบาลจีนกลับมองว่าการกระทำดังกล่าวคือการปลุกระดมให้มีการแบ่งแยกดินแดนซึ่งส่งผลกระทบต่อความเป็นเอกภาพและอำนาจอธิปไตยของจีน โดยสรุป การกระทำจำนวนมากถูกตีความอย่าง

---

[36] 《中华人民共和国网络安全法》第13 条 "国家支持研究开发有利于未成年人健康成长的网络产品和服务，依法惩治利用网络从事危害未成年人身心健康的活动，为未成年人提供安全、健康的网络环境。"

[37] 《中华人民共和国网络安全法》第 12 条

[38] Gao, Charlotte. 2017. "China Fines Its Top 3 Internet Giants for Violating Cybersecurity Law". The Diplomat. https://thediplomat.com/2017/09/china-fines-its-top-3-internet-giants-for-violating-cybersecurity-law/.

[39] Li, Pei. 2018. "Shanghai Temporarily Closes Marriott Website In China After Questionnaire Gaffe". U.S. Reuters. https://www.reuters.com/article/us-china-marriott/shanghai-temporarily-closes-marriott-website-in-china-after-questionnaire-gaffe-idUSKBN1F00UT.

กว้างขวางและครอบคุลมไว้ให้อยู่ในบังคับของกฎหมายความปลอดภัยทางไซเบอร์ของจีน ซึ่งมีขอบเขตกว้างขวางกว่ากฎหมายความปลอดภัยทางไซเบอร์ในประเทศอื่น

2.2 ความปลอดภัยทางไซเบอร์กับระบบสังคมนิยมอันมีเอกลักษณ์แบบจีน

เศรษฐกิจของสาธารณรัฐประชาชนจีนถูกควบคุมโดยรัฐอย่างเต็มรูปแบบภายใต้เศรษฐกิจระบบวางแผนตั้งแต่การก่อตั้งสาธารณรัฐประชาชนจีนในปี ค.ศ. 1948 ในช่วงปี ค.ศ. 1949-1978 ประเทศจีนไม่ทำการค้าขายกับต่างประเทศ เว้นแต่จะมีข้อยกเว้นเป็นกรณีพิเศษ โดยเป้าหมายของการพัฒนาเศรษฐกิจของจีนในสมัยนั้นคือการพัฒนาจากภายใน แต่เนื่องด้วยการดำเนินนโยบายทางเศรษฐกิจที่ผิดพลาด และความวุ่นวายทางการเมือง เศรษฐกิจของประเทศจีนจึงได้รับผลกระทบอย่างหนักในสมัยนั้น ต่อมาในปี ค.ศ. 1978 จีนได้ดำเนินนโยบายการเปิดและปฏิรูปเศรษฐกิจอย่างค่อยเป็นค่อยไป โดยหันมาใช้ระบบตลาด (Market Economy) อย่างไรก็ตาม รัฐวิสาหกิจยังคุมส่วนยอดของระบบเศรษฐกิจและมีบทบาทสำคัญในประเทศจีน เมื่อพิจารณาถึงเหตุการณ์ต่างๆ ในอดีตของจีน การที่ประเทศจีนสามารถกลายเป็นประเทศที่มีอัตราการเจริญเติบโตทางเศรษฐกิจสูงที่สุดในรอบ 3 ทศวรรษที่ผ่านมา นับเป็นสิ่งที่น่าชื่นชม

อย่างไรก็ตาม มีข้อสังเกตว่า พรรคคอมมิวนิสต์จีนให้ความสำคัญในเรื่องความมั่นคงเป็นเป้าหมายที่สำคัญที่สุดอันดับแรกเสมอ แม้แต่การมุ่งพัฒนาเศรษฐกิจก็มีเป้าหมายหลักเพื่อรักษาความมั่นคงและความชอบธรรมในการปกครองให้แก่พรรคคอมมิวนิสต์ เช่นเดียวกัน นโยบายของจีนที่มีต่อต่างชาติ รวมไปถึงการกระทำทางไซเบอร์ ก็ล้วนเป็นไปเพื่อเหตุผลทางการเมืองในการรักษาความมั่นคงของพรรคคอมมิวนิสต์เป็นหลัก[40] เป้าหมายระยะยาวของจีนทุกข้อ อันได้แก่ ความมีเสถียรภาพทางการเมือง ความสมบูรณ์ของดินแดน และความเจริญก้าวหน้าทางเศรษฐกิจ ล้วนต้องอาศัยการเตรียมพร้อมรับมือกับความขัดแย้งทางไซเบอร์ที่ดีพอ และทั้งหมดนี้จะสนับสนุนให้พรรคคอมมิวนิสต์อยู่ต่อไปได้อย่างมั่นคง ซึ่งกฎหมายและระเบียบต่างๆ ในประเทศจีนต่างก็มีลักษณะการตีความที่ยืดหยุ่น เพื่อสามารถนำมาใช้ให้สอดคล้องกับเป้าหมายทางการเมืองได้

นอกจากเป้าประสงค์หลักในเรื่องการรักษาความมั่นคงของพรรคคอมมิวนิสต์แล้ว รัฐบาลจีนยังมีวัตถุประสงค์อีกหลายๆ อย่าง ได้แก่ การรักษาความปลอดภัย กระตุ้นการผลิต การเพิ่มอุปสงค์ในประเทศ และช่วยเหลือธุรกิจด้านเทคโนโลยีภายในประเทศ

รัฐบาลจีนทุ่มเทอย่างมากในการศึกษาและพัฒนากฎหมายที่เกี่ยวกับอินเทอร์เน็ตมาใช้ในตลาด โดยมาตรการเกรทไฟร์วอลล์ของประเทศจีนถูกกล่าวขานเป็นอย่างมากว่าเป็นการแทรกแซงตลาดด้วยการปิดกั้นไม่ให้ผู้ให้บริการทางอินเทอร์เน็ตต่างชาติ เช่น เฟซบุ๊ก กูเกิล ยูทูป และบริษัทอื่นๆ เข้ามาในตลาดจีน นอกจากนี้ รัฐบาลจีนยังแสดงความปรารถนาอย่างชัดแจ้งที่จะแทรกแซงตลาดด้วยกฎหมายความปลอดภัย

[40] Chang, Amy. 2014. "Warring State: China'S Cybersecurity Strategy". Center For A New American Security. https://www.cnas.org/publications/reports/warring-state-chinas-cybersecurity-strategy.

ทางไซเบอร์ในหลายๆ หมวด ตัวอย่างเช่น มาตรการการเก็บรวบรวมข้อมูลในท้องที่มีข้อกำหนดที่บังคับให้ผู้ให้บริการระบบโครงสร้างพื้นฐานต้องบริการการจัดเก็บข้อมูลซึ่งมีที่ต้องอยู่ในประเทศเท่านั้น

การที่รัฐแทรกแซงตลาดยังอาจเห็นได้จากการมาตรการรับประกันความปลอดภัยและตรวจสอบอุปกรณ์ที่ใช้ในการให้บริการ โดยรัฐจะเป็นผู้กำหนดว่าสินค้าหรือบริการใดบ้างที่ได้รับอนุญาตให้ใช้ในกิจการของผู้ให้บริการระบบโครงสร้างพื้นฐานสำคัญได้ ซึ่งแสดงถึงความไม่เชื่อใจของรัฐที่มีต่อการดำเนินงานของเอกชน และมาตรการนี้เองก็ได้ขัดขวางไม่ให้ผู้ให้บริการระบบโครงสร้างพื้นฐานสามารถเลือกใช้สินค้าหรือบริการที่ตรงกับความต้องการของพวกเขาได้จริง

สำหรับมาตรการการรับประกันความปลอดภัยและการทดสอบ เป็นการปิดกั้นไม่ให้บริษัทต่างชาติเข้าถึงตลาดในประเทศจีน โดยประเทศจีนมองว่าเทคโนโลยีที่เกิดจากการพัฒนาภายในประเทศมีความน่าเชื่อถือมากกว่าเทคโนโลยีที่พัฒนาโดยต่างชาติ อีกทั้งประเทศจีนยังมองว่าการที่จีนพึ่งพาเทคโนโลยีต่างชาติจะเป็นตัวทำลายความปลอดภัยทางไซเบอร์ในระยะยาว ดังปรากฏในนโยบาย “แทนที่เทคโนโลยีต่างชาติ” โดยใช้ “สินค้าในชาติ” เป็นหลัก[41]

2.3 แนวความคิดว่าด้วยความเป็นอิสระทางเทคโนโลยีของจีน

ในระยะเวลาหลายปีที่ผ่านมา เนื่องด้วยความต้องการมีอิสระทางเทคโนโลยี ประเทศจีนได้สนับสนุนด้านความปลอดภัยทางอินเตอร์เน็ตและพัฒนาเทคโนโลยีสารสนเทศของตนเอง เมื่อปี ค.ศ. 2014 ประเทศจีนได้ทำการพัฒนาระบบปฏิบัติการของตนเองโดยมีพื้นฐานมาจากลีนุกซ์ ซึ่งในภายหลังได้ใช้อย่างแพร่หลายในคอมพิวเตอร์ของหน่วยงานรัฐบาลและระบบความปลอดภัยต่างๆ ยิ่งไปกว่านั้นประเทศจีนยังได้จำกัดการใช้งานของเทคโนโลยีต่างประเทศ เนื่องจากกลัวว่าการใช้ระบบดังกล่าวแฝงไว้ซึ่งโปรแกรมอันตรายอันมีผลกระทบต่อความมั่นคง[42]

การที่ประเทศจีนปกป้องตลาดภายในประเทศจากอิทธิพลภายนอก และการสนับสนุนนโยบายทางอุตสาหกรรมและนวัตกรรมย่อมเป็นการกระตุ้นการแข่งขันของบริษัทในพื้นที่ อย่างไรก็ดี สำหรับนวัตกรรมเทคโนโลยีขั้นสูงนั้น ประเทศจีนยังคงต้องอาศัยเทคโนโลยีจากต่างประเทศอยู่[43]

บริษัทโทรคมนาคมต่าง ๆ ซึ่งถูกบริหารโดยรัฐ (China Telecom, China Unicom, และ China Moblie) ครอบครองส่วนแบ่งตลาดส่วนใหญ่ในประเทศจีน[44] ทุกการตัดสินใจที่บริษัทเหล่านี้ทำล้วนต้องผ่าน

---

[41] Office of the United States Trade Representative. 2017. "2017 Special 301 Report". United States of America.

[42] Gierow, Hauke Johannes. 2015. "Cyber Security In China: Internet Security, Protectionism And Competitiveness: New Challenges To Western Businesses". China Moniter. https://www.merics.org/sites/default/files/2019-08/150407_MERICS%20China%20Monitor%2022_en.pdf.

[43] เรื่องเดียวกัน.

[44] เรื่องเดียวกัน.

การอนุญาตจากรัฐบาล การตัดสินใจเหล่านั้นรวมไปถึงการพิจารณาว่าเทคโนโลยีใดควรถูกพัฒนา[45] นอกจากนี้ บริษัทอื่น ๆ เช่น ZTE, Lenovo หรือ Datang ก็ยังถูกตั้งมาตรฐานการผลิตเทคโนโลยีโดยรัฐบาลจีนเช่นเดียวกัน[46] อย่างไรก็ดี ยังมีบริษัทไอทีในประเทศจีนอีกเป็นจำนวนมากที่ละเลยมาตรฐานด้านความปลอดภัยเกี่ยวกับตัวซอฟแวร์[47]

นอกจากนี้ บริษัทในจีนยังคงมีปัญหาเกี่ยวกับความน่าเชื่อถือในระบบเข้ารหัส มาตรฐานระบบการเข้ารหัสของจีนนั้นปกป้องข้อมูลได้เพียงบางส่วนเท่านั้น โดยผู้ผลิตของประเทศจีนถูกบังคับให้ใส่ “กุญแจผี” ไว้ในระบบของตนตามคำสั่งของคณะกรรมการการเข้ารหัสแห่งชาติ (National Encryption Leading Group) เพื่อให้รัฐบาลสามารถทำการเข้าถึงข้อมูลในส่วนที่สำคัญได้[48]

ตั้งแต่ปี ค.ศ. 2015 เป็นต้นมา คอมพิวเตอร์ร้อยละ 15 ของรัฐบาลจีนเริ่มเปลี่ยนจากระบบปฏิบัติการวินโดวน์มาเป็นระบบปฏิบัติการของประเทศจีนเอง[49] ทว่าปัญหาคือระบบดังกล่าวยังไม่มีความเสถียรมากนัก และเมื่อเปรียบเทียบระหว่างแอปพลิเคชันของประเทศจีนกับชาติตะวันตก แอปพลิเคชันของประเทศจีนมีข้อเสียเปรียบด้านระบบรักษาความปลอดภัยและมีไวรัสแอบแฝงอยู่

รัฐบาลจีนอธิบายเกี่ยวกับการจำกัดการใช้อินเตอร์เน็ตของตน ยกตัวอย่างเช่น การบล็อค google หรือ Facebook ว่าการกระทำดังกล่าวเป็นไปเพื่อความมั่นคงและเป็นการปกป้องประชาชนของเขาจากการก่อการร้าย[50] การจำกัดการใช้อินเตอร์เน็ตดังกล่าวของจีนมีต้นทุนการดำเนินการที่สูงมาก[51] ยกตัวอย่างเช่น ในเว็บบล็อคของจีนนั้นต้องมีการจ้างผู้คนมาเฝ้าดูเนื้อหาในเว็บไซด์ตลอดเวลาว่าควรลบหรือไม่ ด้วยเหตุนี้ การเซ็นเซอร์เนื้อหาจึงมิได้เพียงกระทบต่อเสรีภาพการแสดงออกแต่เพียงเท่านั้น หากแต่ยังกระทบถึงเศรษฐกิจทั้งประเทศ

---

[45] Ernst, Dieter, and Barry J. Naughton. 2008. "China's Emergent Political Economy Insights From The IT Industry". SSRN Electronic Journal, 39-59. doi:10.2139/ssrn.2742927.

[46] Gierow, Hauke Johannes. "Cyber Security In China: Internet Security, Protectionism And Competitiveness: New Challenges To Western Businesses".

[47] เรื่องเดียวกัน.

[48] Cloutier, Christopher T. 2012. "Casting A Wide Net: China’S Encryption Restrictions". Worldecr. https://research.umbc.edu/files/2014/10/11-11WorldECRCloutierCohen.pdf.

[49] Gierow, Hauke Johannes. "Cyber Security In China: Internet Security, Protectionism And Competitiveness: New Challenges To Western Businesses".

[50] Reuters. "China Takes Another Step Toward Controversial Cybersecurity Law". 2016. Fortune. https://fortune.com/2016/06/27/china-moves-toward-adopting-cybersecurity-law/.

[51] Ho, Alexander. 2014. "Why China Is A Nightmare for American Internet Companies". TIME. https://time.com/10178/why-china-is-a-nightmare-for-american-internet-companies/.

2.4 แนวความคิดว่าด้วยอธิปไตยไซเบอร์ (Cyber Sovereignty)

อธิปไตยไซเบอร์ (Cyber Sovereignty) บางครั้งเรียกว่า อธิปไตยอินเตอร์เน็ต (Internet Sovereignty)[52] หรืออธิปไตยเครือข่าย (Network Sovereignty)[53] อธิปไตยไซเบอร์คือหลักสำคัญในกฎหมายความปลอดภัยทางไซเบอร์และมาตรการอื่นๆ ที่เกี่ยวข้องกับอินเตอร์เน็ตของประเทศจีน และสะท้อนอย่างชัดเจนว่าจีนมีแนวคิดสอดคล้องกับสำนัก Cyber Paternalism

ในมาตรา 1 ของกฎหมายความปลอดภัยทางไซเบอร์กล่าวถึงเจตนารมณ์แห่งกฎหมายไว้อย่างชัดเจนว่า “เพื่อปกป้องความปลอดภัยทางไซเบอร์ เพื่อพิทักษ์ไว้ซึ่งอธิปไตยไซเบอร์ ความมั่นคงของชาติ และสาธารณประโยชน์ เพื่อปกป้องสิทธิประโยชน์ของประชาชน นิติบุคคล และองค์กรอื่นๆ และเพื่อสนับสนุนการพัฒนาทางเศรษฐกิจและสารสนเทศอย่างยั่งยืน”[54] จะเห็นได้ว่า กฎหมายฉบับนี้มองว่าภยันอันตรายที่มีต่อความปลอดภัยทางไซเบอร์คือภยันตรายต่ออธิปไตยและความมั่นคงของชาติ[55]

เป็นที่ยอมรับโดยทั่วไปว่าไซเบอร์สเปซนั้นเป็นโลกไร้พรมแดน ด้วยเหตุนี้จึงไม่ควรมีเรื่องของอธิปไตยมาเกี่ยวข้อง แต่จากมาตรา 1 ของกฎหมายดังกล่าวกลับแสดงให้เห็นเจตนารมณ์ของกฎหมายว่า “เพื่อพิทักษ์ไว้ซึ่งอธิปไตยไซเบอร์” ที่จริงแล้ว การอ้างถึงอำนาจอธิปไตยบนไซเบอร์สเปซนั้นมิได้ถูกยกขึ้นอ้างครั้งแรกในกฎหมายความปลอดภัยทางไซเบอร์ แต่เป็นรายงานสมุดปกขาว ออกโดยสำนักข่าวสารแห่งคณะรัฐมนตรีแห่งสาธารณรัฐประชาชนจีนเมื่อปี ค.ศ. 2010 ซึ่งมีหัวเรื่องว่า “อินเตอร์เน็ตในประเทศจีน” โดยกล่าวถึงเรื่องนี้เป็นครั้งแรกว่า

“...ในอาณาเขตของสาธารณรัฐประชาชนจีน อินเตอร์เน็ตก็อยู่ภายใต้การบังคับใช้กฎหมายของจีนด้วย อธิปไตยอินเตอร์เน็ตของสาธารณรัฐประชาชนจีนควรได้รับการเคารพและคุ้มครอง ประชาชนแห่งสาธารณรัฐประชาชนจีนและบุคคลต่างประเทศ นิติบุคคลและองค์กรอื่นๆ ซึ่งอยู่ในอาณาเขตของสาธารณรัฐประชาชนจีนย่อมมีสิทธิและเสรีภาพในการใช้อินเตอร์เน็ต ในขณะเดียวกัน พวกเขาต้องเคารพกฎหมายและระเบียบต่างๆ แห่งสาธารณรัฐประชาชนจีนและปกป้องความมั่นคงทางอินเตอร์เน็ต...[56]

---

[52] Jiang, Min. 2010. "Authoritarian Informationalism: China’S Approach to Internet Sovereignty". SAIS Review of International Affairs 30 (2): 71.

[53] Parasol, Max. 2018. "The Impact Of China's 2016 Cyber Security Law On Foreign Technology Firms, And On China's Big Data And Smart City Dreams". Computer Law & Security Review 34 (1): 67.

[54] 《中华人民共和国网络安全法》第 1 条

[55] Condron, Sean M. 2007. "Getting It Right: Protecting American Critical Infrastructure In Cyberspace". Harvard Journal Of Law & Technology 20 (2): 407.

[56] Information Office of the State Council the People's Republic of China. 2010. "Govt. White Papers - The Internet In China". 2010. China.Org.Cn. http://www.china.org.cn/government/whitepaper/2010-06/08/content
_20208007.htm.

กฎหมายความมั่นคงแห่งชาติ ซึ่งออกในปี ค.ศ. 2015 เน้นย้ำว่ารัฐต้อง “ธำรงไว้ซึ่งอธิปไตยไซเบอร์” ด้วยการ “เสริมสร้างการจัดการเครือข่าย [และ] ป้องกัน ยับยั้ง และลงโทษอาชญากรทางอินเตอร์เน็ต รวมไปถึงการโจมตีทางไซเบอร์ การแฮ็คเครือข่าย การโจรกรรมข้อมูล และการส่งผ่านข้อมูลที่มิชอบด้วยกฎหมายและเป็นอันตราย”[57]

การที่รัฐใดรัฐหนึ่งควรจะมีอำนาจอธิปไตยเหนือไซเบอร์สเปซหรือไม่นั้นเป็นเรื่องที่สามารถถกเถียงได้ อย่างไรก็ดี รัฐย่อมมีอำนาจเหนือเครือข่ายและระบบสารสนเทศซึ่งอยู่ในอาณาของของรัฐนั้นแน่นอน ด้วยเหตุนี้ รัฐบาลจึงสามารถนำแนวคิดเรื่องอธิปไตยไซเบอร์มาสู่การปฏิบัติจริงด้วยการยกระดับระบบสารสนเทศในรัฐตนได้ ประเทศจีนได้สร้างพรมแดนไซเบอร์เสปซขึ้นด้วยโครงสร้างเครือข่ายของตัวเอง ยกตัวอย่างเช่น "เกรตไฟร์วอลล์" (the Great Firewall) ซึ่งเป็นเครื่องมือในการปิดกั้นเนื้อหาออนไลน์จากต่างชาติ ประธานาธิบดี สีจิ้นผิงและรัฐบาลจีนต้องใช้คำว่า “อธิปไตยไซเบอร์” ในการสนับสนุนแนวคิดที่ว่ารัฐสามารถพัฒนาและควบคุมอินเตอร์เน็ตได้ตามที่พวกเขาต้องการ และอธิปไตยไซเบอร์ได้กลายเป็นปรัชญาพื้นฐานซึ่งก่อให้เกิดนโยบายทางอินเตอร์เน็ตต่างๆ ของประเทศจีน นักวิชาการชาวตะวันตกให้ความเห็นไว้ว่าการอ้างคำว่า “อธิปไตย” ของประเทศจีนนั้นเป็นไปเพื่อ “สร้างความชอบธรรมในการควบคุม” ไซเบอร์เสปซ[58]

2.5 แนวความคิดเรื่องสิทธิมนุษยชนของจีน

ความปลอดภัยทางไซเบอร์มีความเกี่ยวข้องกับสิทธิมนุษยชนในบางด้าน ด้วยเหตุนี้ จึงมีผู้เสนอว่าการกล่าวถึงผลกระทบต่อสิทธิมนุษยชนเป็นสิ่งที่ควรยกประเด็นขึ้นมาด้วยในการหารือเรื่องมั่นคงปลอดภัยไซเบอร์ระหว่างประเทศจีนและสหรัฐอเมริกา ถึงแม้ว่า ประเทศจีนมักมีภาพลักษณ์ในแง่ร้ายเกี่ยวกับการละเมิดสิทธิมนุษยชน อย่างไรก็ดี ประเทศจีนก็ได้มีการคุ้มครองสิทธิมนุษยชนไว้ในรัฐธรรมนูญตั้งแต่ปี ค.ศ. 1982 และในปี ค.ศ. 2004 รัฐธรรมนูญได้รับการยกร่างแก้ไขและบัญญัติอย่างเปิดเผยว่า “รัฐรับรองและให้การคุ้มครองสิทธิมนุษยชน”[59]

บนเวทีโลกนั้น เมื่อปี ค.ศ. 2012 ประเทศจีนกับสหรัฐอเมริกาได้ร่วมมือกันให้ความเห็นชอบต่อคณะมนตรีสิทธิมนุษยชนแห่งสหประชาชาติในการปกป้องเสรีภาพในการแสดงความคิดเห็นบนโลกอินเทอร์เน็ต อย่างไรก็ดี ความหมายของคำว่า “สิทธิมนุษยชน” ที่ประเทศจีนเข้าใจแตกต่างกับที่ชาติตะวันตก

ปรัชญาด้านสิทธิมนุษยชนของจีนนั้นได้สะท้อนผ่านความต้องการในการควบคุมอินเทอร์เน็ตซึ่งเน้นให้เห็นถึงหน้าที่ความรับผิดชอบของแต่ละบุคคลที่มาก่อนสิทธิของบุคคลนั้น ตัวอย่างเช่น แม้ในกฎหมายจะคุ้มครองสิทธิของข้อมูลส่วนบุคคล กฎหมายฉบับเดียวกันก็ยังเปิดช่องให้รัฐบาลหรือบุคคลที่สามเข้ามาล่วง

---

[57] 《中华人民共和国国家安全法》第 25 条

[58] Lindsay, Jon R. 2015. "The Impact Of China On Cybersecurity: Fiction And Friction". International Security 39 (3): 7, 13.

[59]《中华人民共和国宪法》第 13 条

ละเมิดต่อสิทธิส่วนนี้ได้ ประเทศจีนมองว่าสิทธิมนุษยชนคือสิ่งที่ได้มาเพราะรัฐเป็นผู้ให้ โดยรัฐมีอำนาจเหนือปัจเจกบุคคลเสมอ[60] จนสรุปได้ว่า สิทธิส่วนบุคคลไม่ได้หมายความรวมไปถึงสิทธิมนุษยชนด้วยในประเทศจีน

ด้วยเหตุผลที่รัฐเหนือว่าเอกชน ผู้ให้บริการทางโครงข่ายจึงมีหน้าที่ให้สิทธิความเป็นส่วนตัวแก่ผู้ใช้งาน แต่ในขณะเดียวกัน หากข้อมูลของผู้ใช้งานถูกละเมิดโดยรัฐ ผู้ใช้งานก็ไม่สามารถเรียกร้องขอการเยียวยาใดๆ ได้ ในทางเดียวกัน ถึงแม้ประเทศจีนจะรับรองเสรีภาพในการแสดงความคิดเห็น อย่างไรก็ดี การแสดงความเห็นต่อต้านรัฐบาลก็ยังคงเป็นสิ่งที่ถูกควบคุมอย่างเข้มงวด อันจะเห็นได้ว่าสิทธิมนุษยชนไม่สามารถถูกยกอ้างเพื่อใช้ทำลายเสถียรภาพของสังคมหรือระบบปกครองได้

ปรัชญาสิทธิมนุษยชนของจีนได้รับอิทธิพลมาจากโครงสร้างและกลไกการทำงานของรัฐบาลด้วยเช่นกัน ในชาติประชาธิปไตยในตะวันตก การคุ้มครองสิทธิมนุษยชนจะถูกรับประกันโดยระบบการถ่วงดุลอำนาจ แม้การสอดแนมจากรัฐจะเป็นสิ่งที่เห็นได้ทั่วไปในหลายรัฐ ทว่าการสอดแนมเช่นว่านั้นจะต้องพิจารณาประกอบกับหลักความได้สัดส่วน โดยพิจารณาว่าการทำนั้นเป็นไปเพื่อวัตถุประสงค์ใด ไม่ว่าจะเป็นการสอบสวนอาชญากรรม ประเด็นเกี่ยวเนื่องด้วยความมั่นคงของชาติ หรือเสรีภาพของประชาชน[61] ตัวอย่างเช่น ในสหรัฐอเมริกา กฎหมายข่าวกรองต่างชาติ (Foreign Intelligence Surveillance Act) ได้ห้ามไม่ให้รัฐใช้อุปกรณ์อิเลกทรอนิคในการสอดแนมในสหรัฐอเมริกาเพื่อให้ได้มาซึ่งข่าวกรองของต่างชาติ และหากรัฐบาลต้องทำการใดที่เกี่ยวข้องกับกิจกรรมข่าวกรองของต่างชาติ ผู้มีอำนาจต้องได้รับคำสั่งจากศาลอนุญาตเป็นรายกรณีไป[62] ในทางกลับกัน ประเทศจีนไม่ได้มีแนวคิดเกี่ยวกับระบบการถ่วงดุลอำนาจเลย ศาลไม่ได้คานอำนาจของเจ้าหน้าที่รัฐในการใช้อำนาจ ไม่ว่าเจ้าหน้าที่รัฐนั้นจะใช้อำนาจของตนไปในทางมิชอบหรือใช้อำนาจนั้นเพื่อละเมิดสิทธิมนุษยชน หากการกระทำเหล่านั้นมีจุดมุ่งหมายเพื่อปกป้องความมั่นคงของชาติ ด้วยเหตุนี้ กฎหมายความปลอดภัยทางไซเบอร์ของจีนจึงอนุญาตให้รัฐบาลทำการสอดแนมหรือควบคุมข้อมูลข่าวสารต่างๆ ได้โดยปราศจากข้อจำกัด

กรณีศึกษาตัวอย่างได้แก่ กรณีพิพาทระหว่างบริษัท แอปเปิ้ล กับ สำนักงานสอบสวนกลาง (Federal Bureau of Investigation หรือ FBI) ซึ่งแสดงให้เห็นถึงความแตกต่างในนิยามของคำว่าสิทธิมนุษยชนของประเทศจีนกับโลกตะวันตกได้อย่างชัดเจน โดยในปี ค.ศ. 2016 สำนักงานสอบสวนกลางได้ร้องขอให้บริษัทแอปเปิ้ลปลดล็อคโทรศัพท์มือถือยี่ห้อไอโฟนซึ่งเป็นของผู้ต้องหาที่ทำการกราดยิงสังหารหมู่ที่เมืองซาน เบอนาร์ดิโน่ รัฐแคลิฟอร์เนีย แต่บริษัทแอปเปิ้ลได้ปฏิเสธคำขอนั้น ในภายหลัง กระทรวงยุติธรรมจึงไปขอคำสั่งศาลเพื่อสั่งให้บริษัททำการปลดล็อคมือถือนี้ ทว่าบริษัทแอปเปิ้ลก็ได้โต้แย้งคำสั่งนั้น และเมื่อวันที่ 28 มีนาคม

[60] Daniel C. K. Chow. 2013. "How China Uses International Trade to Promote Its View of Human Rights." George Washington International Law Review 45. no. 4: 681-726.

[61] Justia U.S. Supreme Court. "United States V. United States Dist. Ct., 407 U.S. 297 (1972)". 1972. Justia Law. https://supreme.justia.com/cases/federal/us/407/297/.

[62] 50 U.S.C. § 1801(a)-(f) (2012).

ค.ศ. 2016 รัฐบาลได้ประกาศว่าสำนักงานสอบสวนกลางสามารถปลดล็อคไอโฟนเครื่องนั้นได้ด้วยความช่วยเหลือของบุคคลที่สามแล้ว อันเป็นการยุติข้อพิพาทระหว่างบริษัทแอปเปิ้ลกับรัฐบาล ทว่าในประเทศจีน กฎหมายความปลอดภัยทางไซเบอร์กลับให้อำนาจแก่เจ้าหน้าที่โดยตรงในการขอความช่วยเหลือในด้านการถอดรหัสจากบริษัทได้โดยตรง โดยไม่ต้องใช้คำสั่งศาลใด โดยสรุปก็คือ กฎหมายความปลอดภัยทางไซเบอร์ของจีนให้ความสำคัญกับความมั่นคงของรัฐบาลมากกว่าประเด็นด้านสิทธิมนุษยชน

กฎหมายความปลอดภัยทางไซเบอร์คือหัวใจหลักของกฎหมายและนโยบายต่างๆ ที่เกี่ยวข้องกับอินเทอร์เน็ต กฎหมายความปลอดภัยทางไซเบอร์ของจีนสะท้อนให้เห็นถึงความพยายามของรัฐบาลจีนในการอ้างอำนาจอธิปไตยบนโลกอินเทอร์เน็ต และแสดงให้เห็นว่าประเทศจีนได้ให้ความสนใจกับเรื่องความปลอดภัยทางไซเบอร์ยิ่งขึ้นกว่าแต่ก่อนเป็นอย่างมาก นอกจากนี้ กฎหมายนี้ยังแสดงให้เห็นว่าประเทศจีนมีความต้องการจัดการดูแลไซเบอร์เสปซด้วยตัวเอง ด้วยการมอบอำนาจให้รัฐบาลในการระบุและควบคุมพฤติกรรมต่างๆ บนโลกออนไลน์ที่ไม่เหมาะสม การทำความเข้าใจในกฎหมายความปลอดภัยทางไซเบอร์ของจีนควรพิจารณาผ่านมุมมองพิเศษของประเทศจีนที่มีต่อความปลอดภัยทางไซเบอร์ ซึ่งมีความหมายกว้างขวางกว่าของชาติตะวันตก ในประเทศจีน ความปลอดภัยทางไซเบอร์จะเกิดขึ้นได้ก็ด้วยการควบคุมเนื้อหาบนอินเทอร์เน็ต เพื่อรักษาไว้ซึ่งความเสถียรภาพทางการเมืองและสังคม นอกจากนี้ การปฏิบัติต่อข้อมูลส่วนบุคคลในกฎหมายฉบับนี้สะท้อนให้เห็นถึงมุมมองของประเทศจีนในด้านสิทธิมนุษยชน สิทธิมนุษยชนได้รับการรับรองตามกฎหมาย ทว่าก็สามารถถูกละเมิดโดยอำนาจรัฐได้

บทที่ 3

เนื้อหากฎหมายความปลอดภัยทางไซเบอร์ของประเทศจีน

กฎหมายความปลอดภัยทางไซเบอร์ของจีนได้ผ่านกระบวนการร่างกฎหมายและรับฟังความคิดเห็นอย่างยาวนาน สภาประชาชนแห่งชาติจีนได้เผยแพร่ร่างแรกของกฎหมายเพื่อรับฟังความคิดเห็นในเดือนกรกฎาคม ค.ศ. 2015 และร่างที่สองในเดือนมิถุนายน ค.ศ. 2016 มีรายงานว่า ในเดือนสิงหาคม ค.ศ. 2016 กลุ่มธุรกิจมากกว่า 40 แห่ง ได้ส่งข้อเสนอถึงนายกรัฐมนตรีหลี่เค่อเฉียงขอให้มีการพิจารณาแก้ไขร่างกฎหมายความปลอดภัยทางไซเบอร์ในหลายประเด็น[63] อย่างไรก็ดี กฎหมายความปลอดภัยทางไซเบอร์ ซึ่งได้ประกาศใช้จริงกลับไม่ได้มีการแก้ไขในประเด็นสำคัญต่างๆ ที่เป็นข้อกังวลของกลุ่มธุรกิจ กฎหมายความปลอดภัยทางไซเบอร์ของจีน ได้ผ่านการพิจารณาจากสภาประชาชนแห่งชาติในวันที่ 7 พฤศจิกายน ค.ศ. 2016 และเริ่มมีผลบังคับใช้ตั้งแต่วันที่ 1 มิถุนายน ค.ศ. 2017 เป็นต้นมา[64]

ในเดือนมิถุนายน ค.ศ. 2017 องค์กรอุตสาหกรรมคอมพิวเตอร์และสารสนเทศแห่งประเทศสหรัฐอเมริกา (The Computer and Communications Industry Organization) ซึ่งมาจากการรวมกลุ่มของผู้เล่นสำคัญในภาคอุตสาหกรรมคอมพิวเตอร์และสารสนเทศ เช่น Amazon Microsoft Mozilla Intel ได้เรียกร้องให้รัฐบาลของประธานาธิบดีทรัมป์กดดันให้จีนเลื่อนการบังคับใช้กฎหมาย แต่ความพยายามดังกล่าวไม่ประสบผลสำเร็จ เช่นเดียวกัน ในเดือนพฤษภาคม ค.ศ. 2017 ภาคีกลุ่มธุรกิจนานาชาติในประเทศจีนได้เรียกร้องให้รัฐบาลเลื่อนการบังคับใช้กฎหมายความปลอดภัยทางไซเบอร์ออกไปก่อน แต่หน่วยงานไซเบอร์สเปซแห่งประเทศจีน (Cyberspace Administration of China) ยอมเพียงให้เลื่อนการบังคับใช้กฎหมายลำดับรองที่เกี่ยวข้องกับการเคลื่อนที่ของข้อมูลข้ามพรมแดน (cross-border data flow) จนถึงสิ้นค.ศ. 2018 รายงานเหล่านี้สะท้อนให้เห็นข้อกังวลของกลุ่มธุรกิจ โดยเฉพาะกลุ่มธุรกิจเทคโนโลยีต่างชาติต่อกฎหมายความปลอดภัยทางไซเบอร์ของจีน[65]

ในบทนี้ จะวิเคราะห์ถึงความสัมพันธ์ระหว่างกฎหมายความปลอดภัยทางไซเบอร์กับกฎหมายอื่น การกำกับดูแลไซเบอร์สเปซก่อนการออกกฎหมายความปลอดภัยทางไซเบอร์ โครงสร้างเนื้อหากฎหมายความปลอดภัยทางไซเบอร์ รวมทั้งประเด็นกฎหมายที่สำคัญ

---

[63] Cheng, Ron. 2016. "China Passes Long-Awaited Cyber Security Law". FORBES. https://www.forbes.com/sites/roncheng/2016/11/09/china -passes-long-awaited-cyber-security-law/#5924ea3f24d2.

[64] เรื่องเดียวกัน.

[65] Greenfield, Heather. 2017. "CCIA Highlights to Trump Administration Trade Barriers in China's Cybersecurity Law". Computer and Communications Industry Association: CCIA. https://www.ccianet.org/2017/06/ccia-highlights-to-trump-administration-trade-barriers-in-chinas-cybersecurity-law/.

3.1 ความสัมพันธ์ระหว่างกฎหมายความปลอดภัยทางไซเบอร์ ค.ศ. 2017 กับกฎหมายอื่น

เนื่องด้วยการพัฒนาเทคโนโลยีดิจิตัลอย่างรวดเร็วในและการเชื่อมต่อระหว่างเครือข่ายในประเทศจีน เป็นส่วนสำคัญที่ทำให้ความปลอดภัยทางไซเบอร์กลายเป็นวาระระดับชาติ ดังที่ได้กล่าวข้างต้น กฎหมายความปลอดภัยทางไซเบอร์ถูกร่างขึ้นโดยอาศัยแนวคิด “อธิปไตยไซเบอร์” ซึ่งเป็นส่วนสำคัญในการกำหนดนโยบายและระเบียบของอินเตอร์เน็ตในประเทศจีน โดยมีวัตถุประสงค์เพื่อเป็นหลักสำคัญในการปกป้องความมั่นคงของจีน ด้วยเหตุนี้ กฎหมายฉบับดังกล่าวจึงไม่ได้อยู่โดดๆ หากควรทำความเข้าใจควบคู่กันกับกฎหมายด้านความมั่นคงฉบับอื่นๆ ด้วย เช่น กฎหมายความมั่นคงแห่งชาติ กฎหมายต่อต้านการก่อการร้าย เป็นต้น

ก่อนที่จะมีการร่างกฎหมายความปลอดภัยทางไซเบอร์ รัฐบาลจีนได้มีการออกมาตรการของฝ่ายบริหารและกฎต่างๆ ซึ่งเกี่ยวข้องกับความปลอดภัยทางไซเบอร์ ตัวอย่างเช่น ระเบียบว่าด้วยการปกป้องความมั่นคงเกี่ยวกับข้อมูลข่าวสารในระบบคอมพิวเตอร์ มาตรการป้องกันและรักษาไวรัสคอมพิวเตอร์ และลำดับขั้นมาตรการในการรักษาความปลอดภัยของข้อมูล นอกจากนี้ ประเทศจีนยังเสริมสร้างความปลอดภัยทางไซเบอร์โดยการร่วมมือกับสหรัฐอเมริกา โดยในเดือนเมษายน ค.ศ. 2017 ณ รัฐฟลอริดา ประธานาธิบดี โดนัลด์ ทรัมป์ และประธานาธิบดี สี จิ้นผิงได้หารือร่วมกันเกี่ยวกับความปลอดภัยทางไซเบอร์[66] โดยการเจรจาดังกล่าวยังมีอยู่อย่างต่อเนื่อง

เมื่อเปรียบเทียบกฎหมายความปลอดภัยทางไซเบอร์กับกฎหมายความมั่นคงแห่งชาติที่ออกมาก่อนหน้านี้ พบว่ากฎหมายทั้งสองฉบับต่างให้อำนาจรัฐในการควบคุมและกำกับดูแลการไหลเวียนของข้อมูลข่าวสารและเพิ่มมาตรการตรวจสอบเทคโนโลยีต่างๆ ที่มาจากต่างประเทศ[67] นอกจากนี้ กฎหมายทั้งสองฉบับต่างตอกย้ำถึงแนวคิดเรื่องอธิปไตยไซเบอร์อย่างชัดเจน

สภาประชาชนแห่งชาติจีนได้ผ่านร่างกฎหมายต่อต้านการก่อการร้ายเมื่อวันที่ 27 ธันวาคม ค.ศ. 2015 โดยจะมีผลเริ่มบังคับใช้ในวันที่ 1 มกราคม ค.ศ. 2016 กฎหมายต่อต้านการก่อการร้ายนี้บังคับให้ผู้ให้บริการอินเทอร์เน็ต (ISP) และธุรกิจโทรคมนาคมให้การสนับสนุนทางเทคโนโลยีและความช่วยเหลือต่างๆ แก่เจ้าหน้าที่ความมั่นคงของทางการเพื่อการป้องกันและตรวจสอบกิจกรรมที่เกี่ยวข้องกับผู้ก่อการร้าย [68] และผู้ให้บริการอินเทอร์เน็ต (ISP) และธุรกิจโทรคมนาคมต่างมีหน้าที่ในการปกป้องความปลอดภัยทางไซเบอร์โดยการออกระเบียบหรือมาตรการทางเทคนิค เพื่อป้องการการกระจายของเนื้อหาที่เกี่ยวกับการก่อการร้ายและเนื้อหาที่มีลักษณะสุดโต่ง[69] นอกจากนี้แล้ว กฎหมายนี้ยังให้อำนาจแก่เจ้าหน้าที่ในการสั่งให้บุคคลที่เหมาะสม

---

[66] An, Bai Jie. 2017. "Xi's Guidance Focuses Push on Internet". Chinadaily. https://www.chinadaily.com.cn/china/2017-04/20/Content_29003244.htm.

[67] Iasiello, Emilio. 2017. "China’S Cyber Initiatives Counter International Pressure". Journal of Strategic Security 10 (1): 9. doi:10.5038/1944-0472.10.1.1548.

[68] 《中华人民共和国反恐怖主义法》第 18 条

[69] 《中华人民共和国反恐怖主义法》第 19 条

ในการหยุดส่งหรือลบข้อมูลซึ่งเกี่ยวข้องกับการก่อการร้ายหรือสุดโต่งได้ และเจ้าหน้าที่ยังมีอำนาจในการสั่งปิดเว็บไซด์ บล็อกเว็บไซด์จากต่างประเทศ หรือยุติการให้บริการกับบุคคลหรือเว็บไซด์ที่มีเนื้อหาเกี่ยวข้องกับสิ่งที่กล่าวมาข้างต้นได้อีกด้วย[70]

ในการร่างกฎหมายต่อต้านการก่อการร้ายเมื่อค.ศ. 2015 นั้น ในร่างกฎหมายรัฐบาลได้เสนอให้ผู้ให้บริการยอมรับการตรวจสอบจากทางรัฐบาลและต้องเก็บข้อมูลทุกอย่างที่ได้จากประชาชนของประเทศจีนไว้ในอาณาเขตของประเทศเท่านั้น (data localization) ทว่าในที่สุดมาตราดังกล่าวได้ถูกตัดออกไป และถูกนำมาบัญญัติไว้ในมาตรา 37 ของกฎหมายความปลอดภัยทางไซเบอร์แทน[71] อาจสรุปได้ว่า กฎหมายต่อต้านการก่อการร้ายเป็นเครื่องมือสนับสนุนการควบคุมเทคโนโลยีของรัฐบาลโดยอาศัยข้ออ้างเรื่องความมั่นคงเช่นเดียวกัน

3.2 การกำกับดูแลไซเบอร์สเปซก่อนการบัญญัติกฎหมายความปลอดภัยทางไซเบอร์ ค.ศ. 2017

ประธานาธิบดี สี จิ้นผิง ได้กล่าวไว้ตั้งแต่ค.ศ. 2014 ว่า “ชาติจะไม่มีความมั่นคงหากปราศจากความปลอดภัยไซเบอร์”[72] โดยประธานาธิบดี สี จิ้นผิง ได้เน้นย้ำถึงความสำคัญของความมั่นคงว่าเป็นสิ่งที่ขาดมิได้สำหรับการพัฒนาอินเตอร์เน็ต[73] ในเดือนกุมภาพันธ์ ค.ศ. 2014 พรรคคอมมิวนิสต์แห่งประเทศจีนได้จัดตั้งคณะกรรมาธิการข่าวสารและความปลอดภัยทางไซเบอร์ โดยมีประธานาธิบดี สี จิ้นผิง เป็นประธาน เพื่อรับมือกับปัญหาความปลอดภัยทางไซเบอร์ การจัดตั้งคณะกรรมาธิการดังกล่าวแสดงให้เห็นถึงความต้องการในการผลักดันให้ความปลอดภัยทางไซเบอร์เป็นวาระระดับชาติ

ก่อนที่จะมีการออกกฎหมายความปลอดภัยทางไซเบอร์นั้น ประเทศจีนมีระเบียบต่างๆ ที่ใช้บังคับกับซอฟแวร์ซึ่งคิดค้นโดยผู้ประกอบการชาติตะวันตก และมีมาตรการที่สนับสนุนนวัตกรรมที่คิดค้นโดยชาติจีน ในช่วงเวลาดังกล่าว มีรายงานว่ามีการแย่งชิงอำนาจกันในหลายๆ หน่วยงานเพื่อให้ได้มาซึ่งอำนาจในการออกระเบียบเกี่ยวกับไซเบอร์สเปซ[74] หน่วยงานเหล่านี้ ได้แก่ กระทรวงความมั่นคงสาธารณะ สำนักงานความลับแห่งชาติ กระทรวงอุตสาหกรรมและสารสนเทศ และกรมเสนาธิการกองกำลังปลดแอกประชาชน หน่วยงานเหล่านี้ได้ต่อสู้กัน เนื่องจากการทับซ้อนในอำนาจของพวกเขาบนไซบอร์สเปซ ปัจจุบัน การจัดตั้งคณะกรรมการความปลอดภัยไซเบอร์และสารสนเทศ (cyber security and informatization Leading Group) ที่แม้จะ

---

[70] 《中华人民共和国反恐怖主义法》第 19 条

[71] Sacks, Samm. 2017. "China’S Cybersecurity Law Takes Effect: What to Expect". Lawfare. https://www.lawfareblog.com/chinas-cybersecurity-law-takes-effect-what-expect.

[72] Gierow, Hauke Johannes. "Cyber Security in China: Internet Security, Protectionism and Competitiveness: New Challenges to Western Businesses".

[73] Yu, Liang. 2016. "China Focus: XI Calls for Developing China into World Science and Technology Leader". XINHUANET. http://www.xinhuanet.com/english/2016-04/19/c_135293965.htm.

[74] Shackelford, Scott, and Amanda Craig. "Beyond the New “Digital Divide”: Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cyber-Security": 164-165.

ขาดอำนาจเด็ดขาด แต่ก็ได้กลายเป็นกันชนและตัวประสานเพื่อหลีกเลี่ยงความขัดแย้งระหว่างหน่วยงานเหล่านั้น

กฎหมายความปลอดภัยทางไซเบอร์ ค.ศ. 2017 ยังคงรักษาระบบการปกป้องรักษาความปลอดภัยแบบเดิม ซึ่งใช้มาก่อนหน้านั้น คือระบบการคุ้มครองหลายลำดับชั้น (Multi-Level Protection Scheme หรือ MLPS)[75] ระบบนี้แบ่งประเภทของผู้ให้บริการเครือข่ายออกเป็น 5 ระดับ [76] ซึ่งผู้ให้บริการจะถูกจัดอยู่ในระดับใดนั้น ให้พิจารณาถึงความร้ายแรงของความเสียหายที่จะเกิดขึ้นเมื่อเครือข่ายของผู้ให้บริการถูกโจมตี โดยมีรายละเอียดดังต่อไปนี้[77]

ระดับ	เมื่อเครือข่ายที่ให้บริการนั้นถูกโจมตีหรือได้รับความเสียหาย อาจก่อให้เกิด...
ระดับ 1	- ความเสียหายธรรมดาต่อสิทธิตามกฎหมายและผลประโยชน์ของบุคคล นิติบุคคล และองค์กรอื่น ๆ แต่เพียงเท่านั้น
ระดับ 2	- ความเสียหายอย่างมากต่อสิทธิตามกฎหมายและผลประโยชน์ของบุคคล นิติบุคคล และองค์กรอื่น ๆ หรือ - ความเสียหายธรรมดาต่อความสงบเรียบร้อยหรือผลประโยชน์สาธารณะ
ระดับ 3	- ความเสียหายอย่างรุนแรงต่อสิทธิตามกฎหมายและผลประโยชน์ของบุคคล นิติบุคคล และองค์กรอื่น ๆ หรือ - ความเสียหายอย่างมากต่อความสงบเรียบร้อยหรือผลประโยชน์สาธารณะ หรือ - ความเสียหายธรรมดาต่อความมั่นคงของชาติ
ระดับ 4	- ความเสียหายอย่างรุนแรงต่อความสงบเรียบร้อยหรือผลประโยชน์สาธารณะ หรือ - ความเสียหายอย่างมากต่อความมั่นคงของชาติ
ระดับ 5	- ความเสียหายอย่างรุนแรงต่อความมั่นคงของชาติ

ที่มา: ReedSmith

การจัดระดับประเภทผู้ให้บริการจะเริ่มตั้งแต่ช่วงที่มีการออกแบบระบบ โดยผู้ให้บริการต้องทำการประเมินตนเอง หลังจากนั้น หากระดับของผู้ให้บริการถูกจัดว่าเป็นระดับ 2 ขึ้นไป การออกแบบระบบต้องถูกพิจารณาโดยผู้เชี่ยวชาญ และเจ้าหน้าที่ด้วย เพื่อให้ทางการออกใบอนุญาตประกอบกิจการให้ต่อไป[78]

อย่างไรก็ดี มีข้อสังเกตว่า คำว่า “ความมั่นคงของชาติ” มิได้ถูกนิยามไว้ว่าหมายถึงสิ่งใดโดยเฉพาะเจาะจง และคำว่า “ความเสียหายอย่างรุนแรง” และ “ความเสียหายอย่างมาก” ก็ไม่ได้ถูกนิยามไว้ด้วย

[75] Gierow, Hauke Johannes. "Cyber Security in China: Internet Security, Protectionism and Competitiveness: New Challenges to Western Businesses".

[76] เรื่องเดียวกัน.

[77] Jing, Catherine, and Amy Yin. 2018. "New Regulations on Cybersecurity: Release Of Draft Regulations On The Cybersecurity Multi-Level Protection Scheme". Reedsmith. https://www.reedsmith.com/en/perspectives/2018/08/new-regulations-on-cyber-security.

[78] เรื่องเดียวกัน.

และในกรณีที่ผู้ให้บริการถูกโจมตีและก่อให้เกิดความเสียหายต่อสิทธิตามกฎหมายและผลประโยชน์ของบุคคล นิติบุคคล และองค์กรอื่น ๆ หากปรากฏว่าผู้ให้บริการนั้นใช้ข้อมูลส่วนบุคคล เจ้าหน้าที่อาจตีความว่าความเสียหายนั้นจะเป็น“ความเสียหายอย่างรุนแรง” ทำให้จากผู้ให้บริการประเภทที่ 2 อาจถูกผลักไปเป็นผู้ให้บริการประเภทที่ 3 ได้โดยง่าย ทั้งนี้ ผู้ให้บริการประเภทที่ 3 ขึ้นไปนั้น โดยมากมักหมายถึงผู้ให้บริการเครือข่ายที่เกี่ยวข้องกับระบบโครงสร้างพื้นฐานสำคัญ ซึ่งกฎหมายก็บัญญัติไว้โดยกว้างเช่นกัน[79] ผลที่เกิดขึ้นเมื่อผู้ให้บริการใดถูกจัดว่าเป็นผู้ให้บริการประเภทที่สูงขึ้น ภาระอื่นตามกฎหมายก็จะมากขึ้นตามไปด้วย

ตัวอย่างเช่น เมื่อผู้ให้บริการประเภทที่ 3 เช่นธุรกิจการเงิน หรือตั้งแต่ระดับ 3 เป็นต้นไปประสงค์จะใช้ผลิตภัณฑ์อิเล็กทรอนิกส์ ผู้ให้บริการต้องตรวจสอบว่าผลิตภัณฑ์นั้นได้รับการรับรองให้ใช้งานแล้วหรือไม่ และสอดคล้องกับกฎระเบียบที่เจ้าหน้าที่ตั้งไว้เพียงใด โดยมีรายละเอียดดังนี้คือ[80]

(1) ผลิตภัณฑ์นั้นถูกพัฒนาโดยประชาชนจีน นิติบุคคล หรือบริษัทที่รัฐจีนได้ร่วมลงทุนด้วย

(2) ส่วนสำคัญของผลิตภัณฑ์นั้นได้รับความคุ้มครองโดยทรัพย์สินทางปัญญาที่ถือครองโดยประเทศจีน

(3) ผลิตภัณฑ์ถูกสร้างขึ้นโดยบุคคลที่ไม่เคยมีประวัติการก่ออาชญากรรมมาก่อน

(4) ผลิตภัณฑ์นั้นไม่มีช่องโหว่หรือไวรัสโทจัน

(5) ผลิตภัณฑ์นั้นไม่กระทบต่อความมั่นคงของชาติ ความสงบเรียบร้อย และผลประโยชน์สาธารณะ และ

(6) ผลิตภัณฑ์นั้นได้รับการรับรองจากหน่วยงานความมั่นคงของชาติ

ตัวอย่างเช่น บริษัท Microsoft ถูกกีดกันการขายผลิตภัณฑ์ของพวกเขาให้กับผู้ใช้งานระดับ 3 หรือมากกว่า ในประเทศจีนตามระเบียบ MLPS การปกป้องเช่นนี้นับว่าสมเหตุสมผลในมุมมองของจีนเอง เพราะนโยบายเหล่านี้มีไว้เพื่อระบบการรักษาความปลอดภัยไซเบอร์ในหน่วยงานที่สำคัญของรัฐ นอกจากนี้นโยบายดังกล่าวยังเป็นประโยชน์ต่อผู้ผลิตภายในประเทศของตน การปกป้องคุ้มครองเช่นนี้มิได้เพียงปรากฏอยู่แต่ในประเทศจีน สหรัฐอเมริกาเองก็มีนโยบายกีดกันไม่ให้รัฐบาลกลางใช้ผลิตภัณฑ์อิเล็กทรอนิกส์ของประเทศจีนด้วยเช่นกัน[81]

[79] เรื่องเดียวกัน.

[80] Gierow, Hauke Johannes. "Cyber Security in China: Internet Security, Protectionism and Competitiveness: New Challenges to Western Businesses".

[81] เรื่องเดียวกัน.

เมื่อบริษัทต่างชาติต้องการมีปฏิสัมพันธ์กับสาธารณชนของจีนผ่านอินเตอร์เน็ต รัฐบาลจีนได้ออกมาตรการต่างๆ มากมายสำหรับบริษัทต่างชาติเหล่านั้น[82] หนึ่งในมาตรการที่เป็นมาตรฐานสำหรับทุก ๆ บริษัท คือการช่วยเหลือรัฐบาลในการเซ็นเซอร์เนื้อหาที่มีความรุนแรง หากบริษัทใดที่ล้มเหลวในการกระทำการดังกล่าวจะถูกแบนจากประเทศจีน[83]

3.3 โครงสร้างเนื้อหาของกฎหมายความปลอดภัยทางไซเบอร์ ค.ศ. 2017

โครงสร้างเนื้อหาของกฎหมายความปลอดภัยทางไซเบอร์ สามารถสรุปได้โดยสังเขป ดังนี้

ในหมวดแรกของกฎหมายใหม่ระบุถึงเจตนารมณ์ของกฎหมาย และกล่าวถึงหน่วยงานซึ่งมีหน้าที่รับผิดชอบต่อกฎหมายฉบับนี้[84] โดยหนึ่งในเจตนารมณ์นั้นรวมไปถึงการเผยแพร่ “แก่นคุณค่าของสังคมนิยม”[85] และสร้างความรับผิดชอบให้แก่หน่วยงานต่างๆ ของรัฐในการวางแผน ทำงานร่วมกัน กำกับดูแล และบริหารจัดการความมั่นคงของเครือข่าย[86] มาตราดังกล่าวยังกำหนดหน้าที่ของเอกชนและองค์กรต่างๆ ให้รายงานการกระทำต่างๆ ที่เป็นภัยต่อความมั่นคงบนอินเตอร์เน็ต ในขณะที่รัฐเองก็มีหน้าที่ต้องตอบกลับอย่างทันท่วงที[87] นอกจากนี้ ยังมีมาตรการที่ใช้บังคับ “องค์กรอุตสาหกรรมต่างๆ ที่เกี่ยวข้องกับเครือข่าย” ให้เสริมสร้างระบบการรักษาความปลอดภัยของพวกเขา โดยไม่จำเป็นต้องรายงานให้ทางการทราบถึงวิธีการที่ทำให้บรรลุวัตถุประสงค์ดังกล่าว[88] และในมาตรา 12 บังคับให้ทั้งบุคคลและองค์กรทั้งหมดงดเว้นการกระทำใดๆ ที่อาจส่งผลเสียต่อนโยบายสังคมนิยมของชาติ[89]

ในหมวดที่ 2 ของกฎหมายนี้สร้างแนวทางพื้นฐานว่ารัฐบาลควรจะทำอย่างไรเพื่อเสริมสร้างความปลอดภัยไซเบอร์[90] โดยมีการบังคับให้หน่วยงานรัฐทุกระดับ ตั้งแต่คณะรัฐมนตรีจนไปถึงเทศบาลในเขตปกครองตนเองจัดทำแผนการต่างๆ ที่เกี่ยวข้อง[91] นอกจากนี้ รัฐยังให้การสนับสนุนด้านต่างๆ ที่เกี่ยวกับการเสริมสร้างความปลอดภัยไซเบอร์ด้วย ยกตัวอย่างเช่น การให้การสนับสนุนนวัตกรรมเทคโนโลยีที่เกี่ยวข้องกับความมั่นคง การสนับสนุนการศึกษาเกี่ยวกับความปลอดภัยไซเบอร์ในการศึกษาระดับมหาวิทยาลัยหรือการศึกษาระดับวิชาชีพขั้นสูง ซึ่งรวมไปถึงการปลูกฝังในความตระหนักรู้เกี่ยวกับความปลอดภัยไซเบอร์ด้วย[92]

---

[82] Ruan, Lotus. 2016. "What Does China’s New Cybersecurity Law Mean for Chinese Internet Companies?". The Diplomat. https://thediplomat.com/2016/11/what-does-chinas-new-cybersecurity-law-mean-for-chinese-internet-companies/.

[83] เรื่องเดียวกัน.

[84] 《中华人民共和国网络安全法》第 1 章

[85] 《中华人民共和国网络安全法》第 6 章

[86] 《中华人民共和国网络安全法》第 8 章

[87] 《中华人民共和国网络安全法》第 12 章

[88] 《中华人民共和国网络安全法》第 11 条

[89] 《中华人民共和国网络安全法》第 12 条

[90] 《中华人民共和国网络安全法》第 2 章

[91] 《中华人民共和国网络安全法》第 16 条

[92] 《中华人民共和国网络安全法》第 20 条

ในหมวดที่ 3 เป็นบทที่ใช้บังคับแก่ผู้ให้บริการเครือข่ายที่ให้บริการบนอินเตอร์เน็ต หรือผู้ให้บริการ[93] โดยกฎหมายได้บัญญัติถึงหน้าที่ทั่วไปที่ผู้ให้บริการต้องดำเนินการ[94] พร้อมทั้งหน้าที่พิเศษสำหรับการจัดการ “ระบบข้อมูลที่มีความอ่อนไหว” ซึ่งเกี่ยวข้องกับระบบโครงสร้างพื้นฐาน[95] โดยบังคับให้ผู้ให้บริการต้องเก็บข้อมูลตัวตนของบุคคลผู้ใช้งานที่แท้จริงไว้[96] และปฏิบัติตามคำสั่งที่หน่วยงานรัฐจะบังคับใช้แก่อุตสาหกรรมตนด้วย[97] ระบบโครงสร้างพื้นฐานประกอบด้วยระบบพลังงาน ระบบการบริหารจัดการน้ำ และเรื่องการธุรกรรม แต่สำหรับกฎหมายนี้ ระบบโครงสร้างพื้นฐานอาจรวมไปถึงสิ่งอื่นๆ ซึ่งเมื่อเกิดการรั่วไหลของข้อมูล ณ ส่วนนั้นแล้ว “อาจเป็นอันตรายต่อความมั่นคงของชาติ สวัสดิการแห่งรัฐ ความเป็นอยู่ของประชาชน หรือประโยชน์สาธารณะ” [98] นอกจากนี้ รัฐบาลยังสนับสนุนให้ผู้ให้บริการที่ไม่ใช่ระบบโครงสร้างพื้นฐานให้มามีหน้าที่ตามกฎหมายเช่นเดียวกันกับผู้ให้บริการเครือข่ายที่เกี่ยวข้องกับระบบโครงสร้างพื้นฐานสำคัญด้วย[99] กรณีนี้เป็นประเด็นที่สำคัญมาก เนื่องจากว่า ผู้ให้บริการเครือข่ายที่เกี่ยวข้องกับระบบโครงสร้างพื้นฐานสำคัญต้องยินยอมให้หน่วยงานของรัฐที่เกี่ยวข้องตรวจสอบเสมอ เมื่อพวกเขาต้องการซื้อผลิตภัณฑ์หรือบริการที่เกี่ยวกับเครือข่ายซึ่ง “อาจกระทบต่อความปลอดภัยของพวกเขา” [100] ผู้ให้บริการเครือข่ายที่เกี่ยวข้องกับระบบโครงสร้างพื้นฐานสำคัญต้องเก็บข้อมูลที่ได้มาจากการสะสมหรือผลิตขึ้นไว้ภายในอาณาเขตของประเทศ และในกรณีที่มีความต้องการนำข้อมูลเหล่านั้นไปแสดง ณ ต่างประเทศ ข้อมูลเหล่านี้ต้องผ่านการประเมินด้านความปลอดภัยจากรัฐบาล[101] นอกจากนี้ ผู้ให้บริการเครือข่ายที่เกี่ยวข้องกับระบบโครงสร้างพื้นฐานสำคัญต้องยอมอยู่ภายใต้การกำกับดูแลของรัฐและทำการส่งเนื้อหาต่าง ๆ ที่มีความอ่อนไหวให้แก่รัฐบาล[102]

ในหมวดที่ 4 กล่าวถึงมาตรฐานของผู้ให้บริการทั่วไป[103] โดยมาตราส่วนใหญ่ในบทนี้กล่าวถึงข้อพึงปฏิบัติต่างๆ ที่ผู้ให้บริการต้องดำเนินการ เช่น ข้อมูลใดจะถูกเก็บสะสมได้บ้าง[104] ซึ่งเกี่ยวข้องกับการที่บุคคลจะถูกบังคับให้แสดงตัวตนที่แท้จริงทุกครั้งที่มีการเชื่อมถึงอินเตอร์เน็ต การจดทะเบียนโดเมน หรือเข้าถึงบริการข้อมูลสาธารณะ[105] และมีมาตราหนึ่งที่บังคับผู้ให้บริการต้องเฝ้าระวังการเผยแพร่เนื้อหาของผู้ใช้งานที่มีลักษณะต้องห้ามตามระเบียบของฝ่ายบริหารหรือกฎหมายอื่นอีกด้วย[106] กฎหมายฉบับนี้กำหนดให้ผู้ให้บริการมีหน้าที่ทั้งเป็นผู้เซ็นเซอร์แทนหน่วยงานรัฐและยังเป็นหูเป็นตาให้รัฐบาลในการสอดส่องดูแล ซึ่งสังเกตได้จาก

[93] 《中华人民共和国网络安全法》第 76 条
[94] 《中华人民共和国网络安全法》第 21 条
[95] 《中华人民共和国网络安全法》第 34 条
[96] 《中华人民共和国网络安全法》第 24 条
[97] 《中华人民共和国网络安全法》第 32 条
[98] เรื่องเดียวกัน.
[99] เรื่องเดียวกัน.
[100] 《中华人民共和国网络安全法》第 35 条
[101] 《中华人民共和国网络安全法》第 37 条
[102] 《中华人民共和国网络安全法》第 39 条
[103] 《中华人民共和国网络安全法》第 4 章
[104] 《中华人民共和国网络安全法》第 40-45 条
[105] 《中华人民共和国网络安全法》第 24 条
[106] 《中华人民共和国网络安全法》第 47 条

การที่กฎหมายนี้ให้ผู้ให้บริการรายงานความพยายามในการเผยแพร่ข้อมูลที่ไม่เหมาะสมนี้ไปให้ “หน่วยงานรัฐที่เกี่ยวข้อง”[107] ทั้งนี้ ผู้ให้บริการต้องอยู่ภายใต้การบริหารจัดการและการกำกับดูแลของรัฐ[108]

ในหมวดที่ 5 กล่าวถึงวิธีการที่หน่วยงานต่างๆ ของรัฐจะกำกับดูแลความปลอดภัยไซเบอร์ พร้อมทั้งกำหนดว่าหน่วยงานใดบ้างของรัฐที่มีหน้าที่ในการเตรียมพร้อมรับมือกับสถานการณ์อันเสี่ยงต่อความมั่นคง[109] มาตราสุดท้ายในหมวดนี้น่าสนใจเป็นอย่างยิ่ง เนื่องจากให้อำนาจคณะรัฐมนตรี พร้อมทั้งรัฐบาลในระดับอื่นซึ่งได้รับอนุญาตจากคณะรัฐมนตรี ในการบังคับใช้มาตรการชั่วคราวเพื่อควบคุมระบบเครือข่ายในกรณีที่เกิดสถานการณ์ฉุกเฉิน หรืออุบัติเหตุต่างๆ จากผลิตภัณฑ์ได้ [110] ในขณะที่มาตรการอื่นๆ คือการระงับการเข้าถึงอย่างตรงไปตรงมา[111]

หมวดที่ 6 ได้กล่าวถึงความรับผิดทางกฎหมายของผู้ให้บริการที่ฝ่าฝืนหรือไม่ปฏิบัติมาตรการในกฎหมายนี้[112] เป็นที่น่าสนใจว่ารัฐบาลได้มุ่งจะเอาผิดแก่ตัวบุคคลและบังคับให้จ่ายค่าปรับ แทนที่จะเป็นการนำโทษปรับนั้นไปใช้กับองค์กรธุรกิจซึ่งใหญ่กว่า[113] และมีอีกสองมาตราที่กล่าวถึงการเซ็นเซอร์ของรัฐ โดยผู้ผู้ให้บริการที่ล้มเหลวในการเซ็นเซอร์เนื้อหาที่ต้องห้ามนั้นจะถูกปรับและระงับการอนุญาตการให้บริการ[114] นอกจากนี้ ในมาตรา 70 ยังขยายขอบเขตของเนื้อหาต้องห้าม ด้วยการอ้างถึงมาตรา 12 (มาตราที่บังคับว่าห้ามมิให้ผู้ใดใช้อินเตอร์เน็ตเพื่อทำลาย “แก่นคุณค่าแห่งสังคมนิยม) [115]

กฎหมายความปลอดภัยทางไซเบอร์ ค.ศ. 2017 กำหนดหน้าที่และบทลงโทษไว้อย่างชัดเจน ขณะเดียวกันก็ยังมีอีกหลายส่วนที่เว้นว่างไว้ให้หน่วยงานของรัฐที่เกี่ยวข้องไปบัญญัติเพิ่มเองได้ จะเห็นได้ว่าประเทศจีนมีความพยายามที่จะดึงให้ผู้ให้บริการมาเป็นส่วนของของระบบเซ็นเซอร์ของตัวเอง เสมือนหนึ่งผู้ให้บริการนั้นเป็นแขนขาให้กับทางการ[116] จึงมีนักวิเคราะห์บางคนมองว่ากฎหมายฉบับนี้เป็นมากกว่าการต้องการคุ้มครองรักษาข้อมูล แต่หากเป็นการที่รัฐพยายามจะปิดหูปิดตาประชาชน[117] และการอ้างเรื่องความปลอดภัยไซเบอร์แสดงให้เห็นถึงความเชื่อในสำนัก Cyber Paternalism โดยอ้างว่าทำไปเพื่อคุ้มครองความปลอดภัยในไซเบอร์สเปซ[118]

---

[107] 《中华人民共和国网络安全法》第 47 条

[108] 《中华人民共和国网络安全法》第 50 条

[109] 《中华人民共和国网络安全法》第 5 章

[110] 《中华人民共和国网络安全法》第 58 条

[111] เรื่องเดียวกัน.

[112] 《中华人民共和国网络安全法》第 6 章

[113] 《中华人民共和国网络安全法》第 60 条

[114] 《中华人民共和国网络安全法》第 68-69 条

[115] 《中华人民共和国网络安全法》第 70 条

[116] 《中华人民共和国网络安全法》第 50 条

[117] Allen-Ebrahimian, Bethany. 2015. "The 'Chilling Effect' Of China’s New Cybersecurity Regime". Foreign Policy. https://foreignpolicy.com/2015/07/10/china-new-cybersecurity-law-internet-security/.

[118] Shackelford, Scott, and Amanda Craig. "Beyond the New “Digital Divide”: Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cyber-Security": 121.

3.4 ประเด็นกฎหมายสำคัญ

3.4.1 หน้าที่ตามกฎหมายของผู้ให้บริการทางเครือข่าย

กลุ่มเป้าหมายของกฎหมายความมั่นคงไซเบอร์ใช้บังคับแก่บุคคลที่เป็นตัวกลางในการสื่อสารบนโลกอินเทอร์เน็ต เช่น หน่วยงานที่ให้บริการเชื่อมต่อเข้ากับเครือข่าย (ISP) เสิร์ชเอนจิน และ ผู้ให้บริการสื่อออนไลน์ต่างๆ บุคคลที่เป็นตัวกลางเหล่านี้ โดยเฉพาะอย่างยิ่งหน่วยงานที่ให้บริการเชื่อมต่อเข้ากับเครือข่าย (ISP) มีส่วนสำคัญยิ่งในการบล็อกและเซ็นเซอร์เนื้อหาต่างๆ บนเว็บไซต์ของต่างประเทศที่ไม่พึงประสงค์[119]

นอกจากนี้ กฎหมายนี้ยังสร้างหน้าที่ตามกฎหมายมากมายให้กับกลุ่มเป้าหมายเหล่านั้น ไม่ว่าจะเป็นผู้ให้บริการทางเครือข่ายทั่วไป ผู้ให้บริการข้อมูลโครงสร้างพื้นฐานที่มีความอ่อนไหวสูง หรือแม้กระทั่งผู้ผลิตสินค้าหรือบริการที่เกี่ยวข้องกับเครือข่าย ตัวอย่างเช่น กฎหมายความปลอดภัยทางไซเบอร์ มาตรา 25 บังคับให้ผู้ให้บริการพัฒนามาตรการฉุกเฉินเพื่อรับมือกับความเสี่ยงและภยันตรายที่อาจเกิดขึ้น เช่น ช่องโหว่ของระบบ ไวรัส หรือการโจมตีทางไซเบอร์ รวมถึงหน้าที่ในการรายงานเหตุการณ์ต่างๆ ที่เกิดขึ้นให้แก่เจ้าหน้าที่ทราบ หรือ มาตรา 38 บังคับให้ผู้ให้บริการข้อมูลโครงสร้างพื้นฐานที่มีความอ่อนไหวสูงต้องทำการประเมินผลและพัฒนามาตรการเฝ้าระวังของตนเอง หรือ มาตรา 22 ซึ่งบังคับให้ผู้ผลิตสินค้าหรือบริการที่เกี่ยวข้องกับเครือข่ายปฏิบัติตามมาตรฐานของชาติ ห้ามการใช้โปรแกรมที่มีวัตถุประสงค์ชั่วร้าย และหากมีช่องโหว่เกิดขึ้น ผู้ผลิตจะต้องแจ้งให้ผู้ใช้งานและหน่วยงานที่เกี่ยวข้องทราบทันทีและดำเนินการแก้ไขโดยเร็ว

กฎหมายได้ให้นิยามคำว่า “ผู้ให้บริการทางเครือข่าย” หรือผู้ให้บริการ ว่าคือ เจ้าของโครงข่าย ผู้บริการโครงข่าย และผู้ให้บริการทางเครือข่ายโดยตรง ซึ่งเป็นนิยามที่ถูกวิพากษ์วิจารณ์อย่างมากเนื่องจากความกว้างขวางของนิยาม เพราะคลอบคลุมถึงผู้ประกอบธุรกิจทุกภาคส่วนที่มีส่วนเกี่ยวข้องกับอินเทอร์เน็ต[120] มีผู้ให้ความเห็นว่า รัฐบาลประสงค์จะให้นิยามมีความกว้างขวาง เพื่อใช้รับมือกับการตีความในอนาคต[121]

หน้าที่หลักของผู้ให้บริการถูกบัญญัติไว้ในมาตรา 21 ของกฎหมายความมั่นคงปลอดภัยไซเบอร์ ดังนี้

1. หน้าที่กำหนดระบบมาตรการรักษาความปลอดภัยภายในองค์กรและการควบคุมให้ปฏิบัติกฎต่างๆ ว่าด้วยความรับผิดชอบของผู้ดูแลรักษาความปลอดภัย รวมไปถึงหน้าที่ในการรับความรับผิดต่างๆ อันเกิดจากระบบรักษาความปลอดภัยนั้น

---

[119] Lee, Jyh-An, and Ching-Yi Liu. 2012. "Forbidden City Enclosed by The Great Firewall". Minnesota Journal of Law, Science, And Technology 13 (1): 148-150.

[120] Cohen, Bret, Britanie Hall, and Charlie Wood. 2017. "Data Localization Laws and Their Impact on Privacy, Data Security and The Global Economy". ANTITRUST 32 (1): 107,109.

[121] Xia, Sara. 2017. "China Cybersecurity and Data Protection Laws: Change Is Coming". China Law Blog. https://www.chinalawblog.com/2017/05/china-cybersecurity-and-data-protection-laws-change-is-coming.html.

2. หน้าที่ในการนำเอามาตรการทางเทคโนโลยีต่างๆ มาใช้เพื่อป้องกันไวรัส การโจมตีหรือการบุกรุกผ่านเครือข่าย และสิ่งอื่นสิ่งใดที่เป็นอันตรายต่อความปลอดภัยของเครือข่าย
3. หน้าที่ในการนำเอามาตรการทางเทคโนโลยีต่างๆ มาใช้เพื่อกำกับดูแลและบันทึกสถานการณ์การให้บริการต่างๆ บนอินเทอร์เน็ต ภยันตรายต่างๆ ที่เกิดขึ้น และวิธีการในการเก็บข้อมูลสิ่งที่บันทึกนั้น โดยบันทึกเหล่านั้นต้องสามารถตรวจสอบย้อนหลังได้ไม่น้อยกว่า 6 เดือน
4. หน้าที่ในการนำเอามาตรการว่าด้วยการคัดแยกข้อมูล การสำรองข้อมูลสำคัญ และการเข้ารหัส รวมไปถึงมาตรการอื่น ๆ ซึ่งบัญญัติไว้ในกฎหมายหรือระเบียบบริหารที่เกี่ยวข้องมาปรับใช้

นอกจากนี้ ผู้ให้บริการต้องพัฒนามาตรการเพื่อรับมือกับภยันตรายไซเบอร์ด้วย และหากมีภยันตรายเหล่านั้นเกิดขึ้น ผู้ให้บริการต้องทำการแก้ไขที่เหมาะสมโดยเร็วและรายงานเหตุการณ์นั้นให้แก่หน่วยงานที่เกี่ยวข้องทราบด้วย หากผู้ให้บริการล้มเหลวในการปฏิบัติตามมาตรการเหล่านี้ เจ้าหน้าที่อาจสั่งให้แก้ไขหรือตักเตือนได้ และหากผู้ให้บริการไม่ปฏิบัติตามคำสั่งหรือคำเตือนนั้น ผู้ให้บริการจะถูกปรับเป็นเงิน 10,000 หยวน ถึง 100,000 หยวน และผู้ที่รับผิดชอบโดยตรงจะถูกปรับเป็นการส่วนตัวอีก 5,000 หยวน ถึง 50,000 หยวน

มาตรา 24 มอบหน้าที่ให้ผู้ให้บริการบังคับผู้ใช้งานของตนแสดงชื่อจริงเมื่อมีการสมัครการใช้บริการเพื่อเข้าถึงบริการทางอินเทอร์เน็ต จดทะเบียนโดเมน ใช้บริการโทรศัพท์บ้านหรือโทรศัพท์มือถือ การเผยแพร่ข้อมูลสาธารณะ และการใช้บริการส่งข้อความต่างๆ นอกจากนี้ กฎหมายยังห้ามไม่ให้ผู้ให้บริการให้บริการกับผู้ใช้งานที่ไม่ได้แสดงชื่อจริงของตน โดยหากผู้ให้บริการไม่ปฏิบัติตามมาตรการนี้ หน่วยงานที่เกี่ยวข้องจะมีคำสั่งให้แก้ไข และหากผู้ให้บริการยังเพิกเฉย หรือปรากฏว่าการฝ่าฝืนของผู้ให้บริการก่อให้เกิดผลร้ายแรง พวกเขาจะถูกปรับเป็นเงิน 50,000 หยวน ถึง 500,000 หยวน และหน่วยงานอาจสั่งระงับการประกอบกิจการไว้ชั่วคราว สั่งปิดเว็บไซต์ หรือเพิกถอนการอนุญาตการให้บริการที่เกี่ยวข้องนั้น จนถึงขั้นสั่งเพิกถอนใบอนุญาตให้ประกอบธุรกิจ ในขณะที่บุคคลที่มีหน้าที่รับผิดชอบโดยตรงจะต้องรับผิดส่วนตัวด้วย โดยถูกปรับเป็นเงิน 10,000 หยวน ถึง 100,000 หยวน สำหรับการฝ่าฝืนนั้น

มาตรา 28 ยังบังคับให้ผู้ให้บริการทางเครือข่ายต้องให้ความช่วยเหลือทางเทคนิคและให้การสนับสนุนต่างๆ แก่เจ้าหน้าที่รัฐในการรักษาความมั่นคงของชาติและสืบสวนอาชญากรรม ด้วยเหตุนี้ จึงทำให้เจ้าหน้าที่ของรัฐที่เกี่ยวข้องมีอำนาจกำกับดูแล ตรวจสอบ และบังคับใช้กฎหมายที่กว้างขวางมากขึ้น อย่างไรก็ดี การที่ผู้ให้บริการทางเครือข่ายให้ความร่วมมือกับเจ้าหน้าที่ของรัฐนั้นก็อาจทำให้ข้อมูลของพวกเขามีความเสี่ยงที่จะรั่วไหลได้สูงขึ้นด้วย เนื่องจากเจ้าหน้าที่ของรัฐเองอาจสั่งให้ผู้ให้บริการทางเครือข่ายช่วยเหลือในการเข้าถึงหรือถอดรหัสข้อมูลเพื่อให้ได้มาซึ่งข้อมูลส่วนตัวของผู้ใช้ก็ได้[122] โดยไม่ต้องใช้คำสั่งศาลหรือหมายศาลใด นอกจากนี้

[122] Kelley, Katherine W. 2017. "China's Cybersecurity Law Goes into Effect June 1, 2017—Are You Ready?". National Association of Corporate Directors. https://blog.nacdonline.org/posts/chinas-cybersecurity-law-goes-into-effect-june-1-2017-are-you-ready.

ผู้ให้บริการทางเครือข่ายต้องสร้างช่องทางพิเศษไว้ในระบบของพวกเขาเสมอเพื่อให้รัฐบาลสามารถเข้าถึงข้อมูลต่างๆ ได้[123]

น่าสังเกตว่า กฎหมายความปลอดภัยทางไซเบอร์คล้ายคลึงกับกฎหมายต่อต้านการก่อการร้ายของประเทศจีนเป็นอย่างยิ่ง ซึ่งบังคับให้ผู้ประกอบกิจการโทรคมนาคมและผู้ให้บริการทางอินเทอร์เน็ตต้องส่งมอบวิธีการถอดรหัสข้อมูลรักษาความปลอดภัยและความช่วยเหลือทางเทคนิคต่างๆ ให้แก่รัฐบาลเพื่อป้องกันและสืบสวนกิจกรรมของผู้ก่อการร้าย[124] ถึงแม้รัฐบาลจีนจะอ้างว่า กฎหมายต่อต้านการก่อร้ายร้ายมิได้เรียกร้องให้บริษัทต้องจัดทำช่องทางลัดแก่รัฐบาลแต่อย่างใด แต่ในกฎหมายความปลอดภัยทางไซเบอร์ บริษัทอินเทอร์เน็ตต่างชาติซึ่งอยู่นอกเขตอำนาจศาลของจีนต้องให้ความร่วมมือกับรัฐบาลจีนในการให้ความช่วยเหลือด้านการถอดรหัสข้อมูลหรือสร้างช่องทางพิเศษให้แก่รัฐบาลในการเข้าถึงข้อมูลส่วนบุคคล นอกจากนี้แล้ว กฎหมายฉบับนี้ยังไม่ได้กำหนดขอบเขตการใช้กฎหมายนี้แต่เพียงในเฉพาะกรณีที่จำเป็นหรือวางแนวปฏิบัติให้แก่เจ้าหน้าที่รัฐในการใช้อำนาจแต่อย่างใด

ในกฎหมายความมั่นคงปลอดภัยไซเบอร์จีน ยังได้มอบหน้าที่เฉพาะให้แก่ผู้ให้บริการทางเครือข่ายที่เกี่ยวข้องกับข่าวสารโดยเฉพาะด้วย โดยผู้ให้บริการต้องบริหารจัดการและสอดส่องการกระจายข้อมูลข่าวสารของผู้ใช้งานของตนโดยเข้มงวด หากปรากฏว่าข้อมูลนั้นมีเนื้อหาที่ขัดต่อกฎหมายหรือกฎของฝ่ายบริหาร โดยหากเนื้อหานั้นปรากฏขึ้น ผู้ให้บริการต้องลบและสกัดกั้นการแพร่กระจายของเนื้อหานั้น พร้อมทั้งบันทึกเหตุการณ์ดังกล่าวและรายงานแก่หน่วยงานที่มีส่วนเกี่ยวข้องให้ทราบ[125] หากผู้ให้บริการไม่ปฏิบัติตาม ในเบื้องต้นจะถูกตักเตือนและสั่งให้แก้ไขโดยเร็ว แต่หากผู้ให้บริการนั้นไม่ปฏิบัติตาม หรือก่อให้เกิดความเสียหายร้ายแรง ผู้ให้บริการจะถูกปรับตั้งแต่ 1 แสนหยวนขึ้นไปแต่ไม่เกิน 550,000 หยวน พร้อมทั้งถูกสั่งให้ระงับการประกอบกิจการในส่วนที่เกี่ยวข้อง ปิดเว็บไซต์ หรือระงับการประกอบกิจการทุกภาคส่วน รวมทั้งการระงับใบอนุญาตประกอบกิจการทั้งชั่วคราวหรือถาวร และผู้ที่มีหน้าที่รับผิดชอบในการดูแลส่วนนั้นโดยตรงจะถูกปรับตั้งแต่ 1 หมื่นหยวนขึ้นไปแต่ไม่เกิน 1 แสนหยวน[126]

ตัวอย่างที่มีชื่อเสียงคือ ในเดือนสิงหาคม ค.ศ. 2017 หลังจากที่กฎหมายความมั่นคงปลอดภัยไซเบอร์ประกาศใช้ไปแล้วประมาณ 2 เดือน คณะกรรมการไซเบอร์เสปซมลฆลกวางตุ้ง ได้ประกาศว่าบริษัทวีแชทและเทนเซนยังไม่ได้ทำตามหน้าที่ที่กฎหมายกำหนดไว้สำหรับผู้ให้บริการทางเครือข่ายที่เกี่ยวข้องกับข่าวสารโดยเฉพาะ เทนเซนยังไม่สามารถระงับการแพร่กระจายข้อเนื้อหาที่ก่อให้เกิดการจลาจล ข่าวปลอม และสื่อลามกต่าง ๆ ได้ ในขณะที่บริษัทวีแชทมีปัญหาในการยับยั้งการแพร่กระจายของเนื้อหาลามก และเนื้อหาที่

[123] itnews. 2016. "China's New Cyber Security Laws Will 'Lock Out' Businesses". Nextmedia. https://www.itnews.com.au/news/chinas-new-cyber-security-laws-will-lock-out-businesses-440929.

[124] Shackelford, Scott, Scott Russell, and Andreas Kuehn. 2016. "Unpacking the International Law on Cybersecurity Due Diligence: Lessons from The Public and Private Sectors". Chicago Journal of International Law 17 (1): 1, 25.

[125] 《中华人民共和国网络安全法》第 47 条

[126] 《中华人民共和国网络安全法》第 68 条 第一款

ก่อให้เกิดความเกลียดชัง และกำหนดจำนวนค่าปรับที่ต้องจ่ายในอัตราสูงสุดคือ 550,000 หยวน แก่ทั้งสองบริษัท

กรณีศึกษา: เว็บไซต์ถูกเจาะระบบและเปลี่ยนแปลงข้อมูล

ในช่วงประมาณปลายเดือนสิงหาคม ค.ศ. 2019 บริษัทหนึ่งในจังหวัดหลิงเป่า มลฑลเหอหนาน ได้ถูกเจาะระบบและทำการเปลี่ยนแปลงข้อมูล โดยเมื่อมีบุคคลใดเข้าไปเยี่ยมชมเว็บไซต์ของบริษัท เว็บไซต์นั้นจะแสดงเนื้อหาของการชักชวนให้เล่นการพนันแทน ด้วยเหตุนี้ตำรวจไซเบอร์จังหวัดเป่าหลิงจึงได้ทำการส่งหนังสือแจ้งเตือนไปยังบริษัท บริษัทได้รับทราบ และส่งรายงานกลับไปว่าตนได้ทำการแก้ไขเรียบร้อย[127]

จนกระทั่งวันที่ 2 เดือนตุลาคม ค.ศ. 2019 ตำรวจได้รับรายงานว่าเว็บไซต์ของบริษัทได้ถูกเจาะระบบและทำการเปลี่ยนแปลงข้อมูลอีกครั้ง ทว่าในท้ายที่สุด กลับสืบพบว่าบริษัทนั้นไม่เคยทำการเปลี่ยนแปงแก้ไขข้อมูลนั้นเลยมาตั้งแต่ต้น ด้วยเหตุนี้ บริษัทนั้นจึงถูกปรับเป็นเงินจำนวน 1 หมื่นหยวน และผู้รับผิดชอบในการดูแลเรื่องความปลอดภัยไซเบอร์โดยตรงของบริษัทก็ถูกปรับอีกเป็นเงิน 5 พันหยวน[128] ตามมาตรา 21 ประกอบกับมาตรา 59 วรรคแรกของกฎหมายความปลอดภัยทางไซเบอร์เนื่องจาก ผู้ให้บริการเพิกเฉยไม่ยอมป้องกันระบบของตนให้รอดพ้นจากการถูกเจาะ

จากคดีนี้ อาจสันนิษฐานได้ว่าบริษัทที่เพิกเฉยต่อหนังสือเตือนจากตำรวจไซเบอร์นั้น อาจมีส่วนรู้เห็นในการเผยแพร่เนื้อหาที่เกี่ยวกับการพนันมาก่อน เพราะหากทางบริษัทไม่มีส่วนรู้เห็นในเรื่องดังกล่าวจริง บริษัทก็ควรจะแก้ไขให้เสร็จโดยเร็วแล้ว แต่อย่างไรก็ดี หากจะเอาผิดทางอาญาในฐานเผยแพร่เนื้อหาที่เกี่ยวกับการพนันแก่บริษัทในฐานะตัวการร่วมด้วยแล้ว ก็อาจเป็นการยากในการพิสูจน์เจตนา เนื่องจากบริษัทสามารถต่อสู้ได้ว่าข้อมูลผิดกฎหมายที่ปรากฏบนเว็บไซต์ตนเองนั้นเกิดขึ้นจากการถูกเจาะระบบข้อมูลโดยบุคคลที่สามซึ่งตนไม่รู้ไม่เห็นด้วย ลำพังเพียงการเพิกเฉยต่อคำเตือนของเจ้าหน้าที่ตำรวจนั้นก็คงไม่สามารถทำให้ศาลนำสืบไปอย่างสิ้นสงสัยได้ว่าบริษัทมีส่วนเกี่ยวข้องกับธุรกิจการพนันจริงหรือไม่

ด้วยเหตุนี้ การที่กฎหมายฉบับนี้เอาผิดแก่ผู้ให้บริการทางเครือข่ายอย่างกว้างขวาง จนบางครั้งราวกับว่าเป็นการซ้ำเติมเหยื่อที่ถูกโจมตี ก็อาจไม่ใช่แนวคิดที่แย่เสียทีเดียว เนื่องจากโทษอาญาจากกฎหมายฉบับนี้สามารถใช้ในการปรามการแพร่กระจายของผู้เผยแพร่เนื้อหาที่ผิดกฎหมายได้ในเบื้องต้น และทำให้อาชญากรก่ออาชญากรรมลำบากขึ้น แม้จะใช้บริษัทประกอบธุรกิจที่ถูกกฎหมายมาเป็นเกราะกำบังการกระทำผิดของตนก็ตาม

อย่างไรก็ดี เป็นที่น่าพิจารณาว่า ถ้าหากบริษัทได้ทำการแก้ไขและปรับปรุงระบบไซเบอร์ของตนให้ดีแล้ว และในภายหลังถูกโจมตีระบบสำเร็จอีก บริษัทจะเป็นอย่างไร ณ ที่นี้เห็นว่าบริษัทก็น่าจะได้รับการ

[127] 大河网. 2019. "违反网络安全法这个企业被罚了". 大河网. http://newpaper.dahe.cn/jrab/html/2019-10/14/content_374468.htm.
[128] เรื่องเดิม

ตักเตือนอีกครั้ง เพราะหากการโจมตีครั้งที่สองสำเร็จ แม้บริษัทจะได้ปรับปรุงระบบป้องกันของตนแล้ว ก็ถือได้ว่าการโจมตีระบบในครั้งหลังเกิดจากการโจมตีคนละรูปแบบกัน และกรณีนี้จึงไม่ใช่การที่บริษัทเพิกเฉยต่อคำสั่งของเจ้าหน้าที่รัฐ

กรณีศึกษา: เครื่องแม่ข่ายที่ให้บริการถูกโจมตีด้วยไวรัสคอมพิวเตอร์และถูกแบล็กเมล

เมื่อวันที่ 30 เมษายน ปี 2020 ตำรวจไซเบอร์ร่วมกับตำรวจจังหวัดคุนหมิง มณฑลยูนนานได้ร่วมกันเข้าตรวจสอบบริษัทสองบริษัท โดยบริษัททั้งสองนี้ได้ร่วมร้องเรียนไปยังทางตำรวจว่า เครื่องแม่ข่ายที่ให้บริการถูกโจมตีด้วยไวรัสคอมพิวเตอร์และถูกแบล็กเมล ข้อมูลบริษัทที่สำคัญถูกเข้ารหัสไว้ให้ไม่สามารถใช้งานได้ตามปกติ และกระทบต่อการประกอบกิจการของบริษัทเป็นอย่างมาก สร้างความเสียหายทั้งในทางทรัพย์สินและชื่อเสียงของบริษัท[129]

ภายหลังการตรวจสอบเครื่องแม่ข่ายที่ให้บริการถูกโจมตีด้วยไวรัส ทางตำรวจได้พบว่าบริษัททั้งสองนี้ต่างขาดความรู้ความเข้าใจเรื่องการรักษาความมั่นคงปลอดภัยไซเบอร์ ทั้งเว็บไซต์และระบบไม่มีระบบป้องกันไวรัสคอมพิวเตอร์ หรือการเจาะระบบใด ๆ ทำให้ง่ายต่อการถูกโจรกรรมข้อมูล จนเป็นเหตุให้บริษัททั้งสองนี้ถูกแบล็กเมลและข้อมูลสำคัญของบริษัทถูกเข้ารหัสในท้ายที่สุด ในเบื้องต้น ทางตำรวจจึงได้ทำการตักเตือนและสั่งให้แก้ไขสถานการณ์ดังกล่าว ตามมาตรา 21 ประกอบกับมาตรา 59 วรรคของกฎหมายความปลอดภัยทางไซเบอร์ [130]

จากคดีนี้ แสดงให้เห็นอีกบทบาทหนึ่งของกฎหมายความมั่นคงปลอดภัยไซเบอร์ของประเทศจีนในการสร้างความตระหนักรู้ให้แก่ผู้ประกอบการ โดยทั่วไปแล้ว ปัจเจกบุคคลย่อมหวงแหนทรัพย์สินใด ๆ ก็ตามที่เป็นของตน โดยเห็นได้จากการที่ประชาชนนำเงินหรือของมีค่าที่ตนหามาได้ไปเก็บรักษาไว้กับธนาคาร หรือไม่ก็เก็บไว้ในที่มิดชิด สิ่งเหล่านี้ล้วนเป็นสามัญสำนึกที่ทุกคนควรตระหนักได้ อย่างไรก็ดี เนื่องด้วยการพัฒนาด้านเทคโนโลยีที่รวดเร็ว ถึงแม้ว่าข้อมูลข่าวสารจะกลายเป็นสิ่งที่มีค่าเช่นเดียวกันกับวัตถุเหล่านั้นแล้ว ความตระหนักรู้ของคนทั่วไปก็ยังตามไปไม่ทัน เส้นแบ่งของสิ่งที่จับต้องได้หรือไม่ทางกายภาพนั้นทำให้ผู้คนละเลยถึงคุณค่าของสิ่งที่จับต้องไม่ได้ ผู้คนยังจำเพียงว่าข้อมูลคือสิ่งที่สามารถคัดลอก จัดวาง สร้างใหม่ หรือกู้คืนได้อย่างไม่จำกัดจำนวน แต่ละเลยความจริงไปว่าข้อมูลบางประเภทก็สามารถใช้ในการหาผลประโยชน์ได้ด้วย ด้วยเหตุนี้ เพื่อรักษาผลประโยชน์ของเอกชนเอง กฎหมายฉบับนี้จึงได้ถูกจัดให้มีขึ้น เพื่อให้ผู้ที่ครอบครองข้อมูลพึงระวังตนมากขึ้น และในขณะเดียวกัน ก็เป็นการป้องกันไม่ให้สังคมนี้เกิดเรื่องวุ่นวายจากการที่ต่างคนต่างเพิกเฉยในการดูแลข้อมูลของตน และสร้างความเดือดร้อนแก่รัฐในการต้องมากำหนดมาตรการเยียวยาใน

[129] 韩，帅南．2020．″昆明西山网警 “一案双查” 构筑网络安全屏障″． 中国新闻网. http://www.yn.chinanews.com/news/2020/0430/56680.html.

[130] เรื่องเดิม

ภายหลัง ทั้งนี้ รัฐอาจมองว่าตนมีความชอบธรรมที่จะเข้ามาก้าวก่ายการบริหารจัดการของเอกชนอยู่เสมอตามแนวคิดแบบสังคมนิยม

ทว่า หากพิจารณาในอีกมุมหนึ่ง การมีอยู่ของข้อกฎหมายนี้ก็เป็นการผลักภาระให้แก่เอกชน โดยเฉพาะอย่างยิ่ง หากเอกชนนั้นเป็นธุรกิจขนาดเล็กหรือกลาง การจัดให้มีระบบรักษาความปลอดภัยไซเบอร์เลยตั้งแต่แรกอาจเป็นอุปสรรคต่อการจัดตั้งธุรกิจในระยะเริ่มต้น ทั้งที่จริงแล้ว ธุรกิจขนาดเล็กหรือกลางมีโอกาสเป็นเป้าหมายของการถูกโจมตีหรือแบล็กเมลน้อยกว่าเมื่อเทียบกับธุรกิจขนาดใหญ่ เนื่องจากมีสินทรัพย์ในบริษัทน้อยกว่า และการเจาะระบบหรือการโจมตีทางไซเบอร์เองก็มีต้นทุนในการดำเนินการเช่นกัน คงไม่มีผู้ร้ายคนใดประสงค์จะ “รีดเลือดจากปู” หรือ “ขี่ช้างจับตั๊กแตน” ดังนั้นแล้ว จึงมีเสียงอีกส่วนหนึ่งโจมตีกฎหมายนี้ว่าเป็นกฎหมายของรัฐพี่เลี้ยงเด็ก (a nanny state) และรัฐไม่เข้าใจความลำบากของผู้ประกอบธุรกิจขนาดเล็กหรือกลางดีพอ

3.4.2 การปกป้องระบบโครงสร้างพื้นฐานสำคัญ

“ระบบโครงสร้างพื้นฐานสำคัญ” หมายถึง สิ่งอำนวยความสะดวก ระบบ และเครือข่ายที่สำคัญของประเทศในทางเศรษฐกิจหรือสังคม ซึ่งเกี่ยวข้องกับสินค้าหรือบริการที่มีประเด็นของความมั่นคงของชาติ เสถียรภาพทางเศรษฐกิจ สุขอนามัยของประชาชนเข้ามาเกี่ยวข้อง จะเห็นได้ว่ามีความหมายที่กว้างขวางมาก อันอาจรวมไปถึงการเกษตร อาหาร น้ำ พลังงาน สุขอนามัย การสื่อสาร การคมนาคม ระบบการเงิน เป็นต้น

ระบบโครงสร้างพื้นฐานสำคัญมีแนวโน้มว่าจะตกเป็นเหยื่อจากการโจมตีทางไซเบอร์ได้สูง ด้วยเหตุนี้ การปกป้องระบบโครงสร้างพื้นฐานสำคัญจึงกลายเป็นนโยบายสำคัญที่มีส่วนเกี่ยวข้องโดยตรงกับความมั่นคงปลอดภัยไซเบอร์ เมื่อปรากฏว่าระบบโครงสร้างพื้นฐานสำคัญมักอยู่ในการครอบครองของเอกชน การรักษาความปลอดภัยจากการถูกโจมตีนั้นอาจถูกละเลย เนื่องจากเอกชนขาดแรงจูงใจที่จะจัดการรักษาความปลอดภัยอย่างเพียงพอ ดังนั้น รัฐบาลจึงควรสร้างมาตรการจูงใจ เพื่อสนับสนุนให้เอกชนลงทุนในด้านความมั่นคงไซเบอร์ด้วย

ตั้งแต่ค.ศ. 2003 ประเทศจีนได้เล็งเห็นถึงความสำคัญของการปกป้องความมั่นคงไซเบอร์และระบบโครงสร้างพื้นฐานสำคัญ จนนำมาสู่การออกกฎหมายความปลอดภัยทางไซเบอร์ในปัจจุบัน โดยมาตรา 31 ของกฎหมายนี้ได้เน้นถึงความสำคัญของระบบโครงสร้างพื้นฐานสำคัญที่เกี่ยวกับข้อมูล โดยข้อมูลเหล่านั้นรวมไปถึง การโทรคมนาคม การจัดการน้ำ ธนาคารและการเงิน พลังงาน การคมนาคม และไฟฟ้า และสิ่งอื่นๆ ซึ่งหากถูกทำลาย ทำให้เสียหาย หรือเกิดการรั่วไหล จะทำให้เกิดผลเสียมหาศาลต่อความมั่นคงของชาติ สวัสดิการสาธารณะ ความเป็นอยู่ของประชาน หรือประโยชน์สาธารณะ

ถึงแม้กฎหมายนี้จะกำหนดให้คณะรัฐมนตรีกำหนดขอบเขตและมาตรการป้องกันความปลอดภัยของระบบโครงสร้างพื้นฐานสำคัญให้ชัดเจน ทำให้เกิดความกังวลว่ากฎหมายนี้มีเนื้อหาที่กว้างเกินไป เนื่องจากคณะรัฐมนตรีย่อมจะมีดุลพินิจที่จะกำหนดได้ว่าธุรกิจอินเทอร์เน็ตใดมีความเกี่ยวข้องกับ “ความมั่นคงของชาติ สวัสดิการสาธารณะ ความเป็นอยู่ของประชาน หรือประโยชน์สาธารณะ ” บ้าง เมื่อบริษัทใดจัดว่าเป็นผู้ทำธุรกิจที่เกี่ยวข้องกับระบบโครงสร้างพื้นฐานสำคัญด้านข้อมูล หรือมีข้อมูลของประชาชนหรือบริษัทจีนอยู่เป็นจำนวนมาก กรณีนี้ก็อาจถือได้ว่าบริษัทนั้นเป็น “ผู้ให้บริการเครือข่ายที่เกี่ยวข้องกับระบบโครงสร้างพื้นฐานสำคัญ” ได้ โดยนิยามนี้มีความกว้างขวางมากจนอาจรวมไปถึงบริษัทขนส่งอาหารในประเทศจีนด้วย นอกจากนี้ ในมาตรา 31 ยังใช้ศัพท์ซึ่งกำกวม โดยคำว่า “ความเป็นอยู่ของประชาชน” และ “ประโยชน์สาธารณะ” ก็เป็นคำที่มีความหมายกว้างขวางและอาจตีความขยายความให้คลอบคลุมได้หลายกิจการ

ถึงแม้ผู้ให้บริการระบบโครงสร้างพื้นฐานสำคัญจะเป็นส่วนหนึ่งในนิยามของคำว่า ผู้ให้บริการทางเครือข่าย แต่การให้บริการระบบโครงสร้างพื้นฐานสำคัญกลับมีภาระทางกฎหมายมากกว่าผู้ให้บริการทางเครือข่ายประเภทอื่น จากมาตรา 34 ผู้ให้บริการทางเครือข่ายที่เกี่ยวข้องกับระบบโครงสร้างพื้นฐานสำคัญ

นอกจากจะต้องปฏิบัติตามหน้าที่ที่ผู้ให้บริการทางเครือข่ายทั่วไปต้องปฏิบัติตามแล้ว ยังต้องปฏิบัติตามหน้าที่เพิ่มเติมดังต่อไปนี้ด้วยคือ[131]

1. จัดให้มีเครื่องมือและบุคคลที่รับผิดชอบเกี่ยวกับความปลอดภัยเฉพาะด้านเพื่อปกป้องข้อมูลของระบบโครงสร้างพื้นฐานสำคัญโดยเฉพาะ และจัดให้มีการตรวจสอบประวัติเบื้องหลังของผู้ที่จะมาทำหน้าที่ดังกล่าวนั้นด้วย

2. จัดให้มีการอบรมและการทดสอบความรู้ทางเทคนิคแก่บุคลากรที่ทำหน้าที่รับผิดชอบในด้านนี้เป็นประจำ โดยระบุระยะเวลาไว้อย่างชัดเจน

3. จัดให้มีการสำรองข้อมูลในกรณีฉุกเฉินแก่ระบบและข้อมูลที่สำคัญ

4. จัดให้มีแผนการรับมือกรณีที่มีการคุกคามทางไซเบอร์ฉุกเฉิน และมีการซ้อมการรับมือ โดยระบุระยะเวลาไว้อย่างชัดเจน

5. ทำตามที่กฎหมายหรือมาตรการของฝ่ายบริหารกำหนด

หากผู้ให้บริการทางเครือข่ายที่เกี่ยวข้องกับระบบโครงสร้างพื้นฐานสำคัญไม่ปฏิบัติตามมาตรา 34 ในเบื้องต้นจะถูกหน่วยงานที่เกี่ยวข้องตักเตือนและสั่งให้แก้ไข หากไม่แก้ไขหรือเพราะการไม่ปฏิบัติตามกฎหมายนั้นก่อให้เกิดผลกระทบที่ร้ายแรงต่อความมั่นคงปลอดภัยไซเบอร์ ผู้ให้บริการทางเครือข่ายจะถูกปรับตั้งแต่ 1 แสนหยวนขึ้นไปแต่ไม่เกิน 1 ล้านหยวน และผู้ที่มีหน้าที่รับผิดชอบในการดูแลความมั่นคงปลอดภัยไซเบอร์โดยตรงจะถูกปรับตั้งแต่ 1 หมื่นหยวนขึ้นไปแต่ไม่เกิน 1 แสนหยวน[132]

3.4.3 การเก็บรวบรวมข้อมูลไว้ภายในท้องที่

“การเก็บรวบรวมข้อมูลไว้ภายในท้องที่” (data localization) คือ มาตรการที่ใช้บังคับแก่บริษัทในการเก็บข้อมูลของผู้ใช้ในเซิฟเวอร์ซึ่งอยู่ในเขตอำนาจของประเทศนั้น โดยต้องเก็บข้อมูลไว้แต่เพียงในประเทศนั้นเท่านั้น[133] ตัวอย่างเช่น ในประเทศเบลเยียม เดนมาร์ก ฟินแลน เยอรมัน รัสเซีย สวีเดน และสหราชอาณาจักร ต่างก็มีกฎเกณฑ์ลักษณะนี้บังคับใช้กับการเก็บข้อมูลทางการเงิน[134] ในขณะที่บางประเทศ เช่น ออสเตรเลีย หรือ สหราชอาณาจักร บังคับไปถึงการเก็บข้อมูลสุขภาพประจำตัวบุคคลด้วย[135]

การเก็บรวบรวมข้อมูลไว้ภายในท้องที่เป็นอีกส่วนสำคัญในกฎหมายความปลอดภัยทางไซเบอร์ของจีน ซึ่งตั้งอยู่บนฐานของหลักการอธิปไตยไซเบอร์ อันนำไปสู่การบังคับให้ข้อมูลต่างๆ ที่ถูกเก็บไว้ในอาณาเขตของ

[131] 《中华人民共和国网络安全法》第 34 条
[132] 《中华人民共和国网络安全法》第 59 条 第二款
[133] Shah, Reema. 2015. "Law Enforcement and Data Privacy: A Forward-Looking Approach". Yale Law Journal 125 (2): 543, 548.
[134] Savelyev, Alexander. 2016. "Russia's New Personal Data Localization Regulations: A Step Forward or A Self-Imposed Sanction?". Computer Law & Security Review 32 (1): 128, 140.
[135] Chander, Anupam, and Uyên P. Lê. 2015. "Data Nationalism". Emory Law Journal 64: 677, 680.

ประเทศตนต้องได้รับความคุ้มครองที่รัดกุมขึ้น แนวคิดเรื่องการเก็บรวบรวมข้อมูลไว้ภายในท้องที่ก็ทำให้รัฐบาลสามารถอ้างสิทธิการควบคุมข้อมูลทั้งหลายได้ง่ายขึ้น เพื่อป้องกันการสอดแนวข้อมูลจากต่างชาติ และเป็นเครื่องมือที่สนับสนุนการเก็บข้อมูลต่างๆ ในประเทศ รวมไปถึงการเป็นผู้สอดแนมข้อมูลเหล่านั้นเสียเองด้วย การเก็บรวบรวมข้อมูลไว้ภายในท้องที่จึงไม่ได้ช่วยยกระดับความปลอดภัยของระบบมากนัก หากแต่ทำให้การสอดแนมจากรัฐเจ้าของข้อมูลและการบังคับใช้กฎหมายบนโลกออนไลน์เป็นไปได้อย่างสะดวกขึ้น

จากมาตรา 37 ผู้ให้บริการเครือข่ายที่เกี่ยวข้องกับระบบโครงสร้างพื้นฐานสำคัญด้านข้อมูลต้องเก็บข้อมูลส่วนบุคคลและข้อมูลสำคัญต่างๆ ไว้ในประเทศจีน การถ่ายโอนข้อมูลออกไปนอกประเทศนี้จะทำได้ก็ต่อเมื่อได้ทำตามขั้นตอนที่กฎหมายกำหนดไว้ รวมไปถึงการขออนุญาตจากเจ้าหน้าที่ด้วย หากไม่ปฏิบัติตามผู้ให้บริการอาจได้รับคำเตือน หรืออาจรวมไปถึงการปิดเว็บไซต์ การเพิกถอนใบอนุญาต และโทษปรับตั้งแต่ 50,000 หยวน ถึง 5,000,000 หยวน และบุคคลที่มีหน้าที่รับผิดชอบโดยตรงจะต้องถูกปรับส่วนตัวอีกเป็นเงิน 10,000 หยวน ถึง 100,000 หยวน[136] ได้มีบุคคลให้ความเห็นว่ามาตรการดังกล่าวเป็นนโยบายการเก็บรวบรวมข้อมูลไว้ภายในท้องที่ที่เข้มงวดที่สุดในโลก ในความเป็นจริงแล้ว มาตรการการเก็บรวบรวมข้อมูลไว้ภายในท้องที่ของจีนได้ถูกใช้มานานแล้วในบางธุรกิจ เช่น ธุรกิจธนาคาร และสุดท้ายจึงกลายเป็นใช้บังคับกับทุกธุรกิจในที่สุด[137]

บริษัทต่างชาติส่วนมากวิตกกังวลกับมาตรการนี้ของจีนเป็นอย่างมาก สิ่งแรกที่บริษัทเหล่านั้นกังวลคือต้นทุนที่สูงขึ้นจากการบริหารข้อมูลเหล่านั้น[138] เนื่องจากในทางปฏิบัติแล้ว บริษัทข้ามชาติหลายบริษัทมักทำการเก็บข้อมูลเหล่านั้นแยกเป็นส่วนๆ ไว้ในหลายๆ ประเทศเพื่อบรรเทาภาระในการบริหารจัดการกลุ่มข้อมูลขนาดใหญ่และภาระด้านภาษี บางบริษัทก็ย้ายเซิฟเวอร์ของตนออกจากประเทศจีนเพื่อป้องกันการสอดแนมและการเซ็นเซอร์[139] เมื่อกฎหมายฉบับนี้บังคับใช้ บริษัททุกบริษัทกลับต้องสร้างศูนย์รวมข้อมูลในประเทศจีนหรือใช้บริการศูนย์เก็บข้อมูลในท้องถิ่น หรือไม่ก็ต้องทำการปรับเปลี่ยนโครงสร้างการเก็บข้อมูล การเก็บรวบรวมข้อมูลไว้ภายในท้องที่ซึ่งอยู่ในกฎหมายความมั่นคงปลอดภัยไซเบอร์อาจถือได้ว่าเป็นการกีดกันทางการค้าสำหรับผู้ประกอบการ และปัจจุบัน มาตรการนี้ได้กลายเป็นคดีพิพาทซึ่งอยู่ในองค์กรการค้าโลก ซึ่งมีคู่พิพาทคือสหรัฐอเมริกา[140]

---

[136] 《中华人民共和国网络安全法》第 66 条

[137] Sacks, Samm. 2017. "China's Cybersecurity Law Takes Effect: What to Expect". Lawfare. https://www.lawfareblog.com/chinas-cybersecurity-law-takes-effect-what-expect.

[138] Horwitz, Josh. 2017. "A Key Question at The Heart of China's Cybersecurity Law: Where Should Data Live?". Quartz. https://qz.com/999613/a-key-question-at-the-heart-of-chinas-cybersecurity-law-where-should-data-live/.

[139] Sargsyan, Tatevik. 2016. "Data Localization and The Role of Infrastructure for Surveillance, Privacy, And Security". International Journal of Communication 10: 2221, 2225-2226.

[140] Miles, Tom. 2017. "U.S. Asks China Not to Enforce Cyber Security Law". REUTERS. http://www.reuters.com/article/us-usa-china-cyber-trade/u-s-asks-china-not-to-enforce-cyber-security-law-idUSKCNC11D1.

ในขณะเดียวกัน บริษัทอินเทอร์เน็ตในประเทศก็มีความกังวลเกี่ยวกับมาตรการนี้ด้วยเช่นกัน โดยมองว่าอาจเป็นอุปสรรคในการผลักดันธุรกิจของตนให้ไปสู่ระดับสากลได้ มาตรการนี้ยังอาจนำไปสู่ “การแบ่งแยกบนโลกอินเทอร์เน็ต” ด้วยการเปลี่ยนแปลงสาระสำคัญของโลกอินเทอร์เน็ตที่มีความไร้พรมแดนและมีความเสรีในการโอนถ่ายข้อมูล

อีกหนึ่งข้อกังวลที่เกิดขึ้นคือความเสี่ยงที่ไม่สามารถควบคุมได้จากการรั่วไหลของข้อมูล บริษัทข้ามชาติบางบริษัทกังวลว่ามาตรการนี้จะเปิดช่องให้รัฐบาลจีนเข้าถึงข้อมูลทรัพย์สินและความลับทางการค้า นอกจากนี้ บริษัทอาจตกเป็นเป้าหมายของการถูกเซ็นเซอร์หรือสอดแนมจากรัฐบาลได้อีกด้วย ซึ่งจะทำลายความปลอดภัยของผู้ใช้บริการไปในตัว ทั้งนี้ กลุ่มข้อมูลที่มารวมตัวกันเป็นกลุ่มเดียวมีแนวโน้มว่าจะถูกแฮคได้สูงกว่า ด้วยเหตุนี้ มาตรการการเก็บข้อมูลไว้ในท้องที่อาจทำลายมากกว่าส่งเสริมความปลอดภัยไซเบอร์

แม้ว่าในมาตรา 37 จะให้คำนิยามของคำว่า “ข้อมูลส่วนบุคคล” ไว้ แต่คำว่า “ข้อมูลสำคัญ” กลับไม่ได้ให้นิยามในกฎหมาย โดยคณะกรรมการไซเบอร์เสปซจีนได้นิยามไว้ว่า “ข้อมูลสำคัญ” หมายถึง “ข้อมูลซึ่งเกี่ยวข้องใกล้ชิดกับความมั่นคงของชาติ การพัฒนาทางเศรษฐกิจ และประโยชน์สาธารณะ”[141] จึงเปิดช่องให้รัฐบาลสามารถตีความ “ความมั่นคงของชาติ การพัฒนาทางเศรษฐกิจ และประโยชน์สาธารณะ” ตามดุลยพินิจของรัฐบาลเองอย่างกว้างขวาง และสร้างต้นทุนมหาศาลให้กับบริษัทต่างๆ ในการปฏิบัติตามมาตรการดังกล่าว

กรณีศึกษา: มาตรการอุปสรรรคทางการค้าด้านเทคนิค

ปัจจุบัน ยังไม่พบว่ามีการทำตามผิดตามข้อกฎหมายนี้ในประเทศจีน อย่างไรก็ดี ในเวทีโลก ได้มีประเด็นพิพาทระหว่างประเทศจีนกับสหภาพยุโรปและสหรัฐอเมริกา โดยสหภาพยุโรปและสหรัฐอเมริกาได้แสดงความกังวลว่ากฎหมายนี้เป็นมาตรการอุปสรรคทางการค้าด้านเทคนิค (Technical Barriers to Trade: TBT) และในขณะนี้ ประเด็นพิพาทดังกล่าวได้อยู่ในระหว่างการพิจารณาของคณะกรรมการวินิจฉัยอุปสรรคทางการค้าแห่งองค์กรการค้าโลก (World Trade Organization)[142] โดยทางสหภาพยุโรปได้แสดงความกังวลต่อรัฐบาลจีนว่า กฎหมายความมั่นคงไซเบอร์ของจีนไม่ได้กำหนดคำว่า “ระบบโครงสร้างพื้นฐานสำคัญ” ให้มีความชัดเจน[143] ดังนั้น หากผู้ให้บริการใดถูกจัดว่าเป็นผู้ให้บริการเครือข่ายที่เกี่ยวข้องกับระบบโครงสร้างพื้นฐานสำคัญก็จะต้องมีภาระในการเก็บข้อมูลไว้ในประเทศ ในขณะที่สหรัฐอเมริกานั้น นอกจากจะมีความกังวลเช่นเดียวกันกับทางฝั่งสหภาพยุโรปแล้ว ยังได้แสดงความเห็นอีกว่า ภายใต้มาตรการการเก็บข้อมูลไว้ภายในท้องที่ การที่โอนข้อมูลออกไปนอกประเทศจีนโดยต้องได้รับอนุญาตก่อนนั้นจะเป็นการเพิ่มภาระให้แก่ผู้ประกอบธุรกิจ นอกจากนี้ ยังมีข้อมูลบางประเภทที่ห้ามโอนไปหากกระทบสิ่งเหล่านี้ เช่น “ความมั่นคงของ

[141] 《关键信息基础设施安全保护条例（征求意见稿）》（保护条例）第 17 条

[142] World Trade Organization. 2020. "WTO Documents". World Trade Organization.

[143] China - Cybersecurity Law Statement by the European Union to the Committee on Technical Barriers to Trade 6 and 7 March 2019 Paragraph 6.

ประเทศ” “การพัฒนาทางเศรษฐกิจ” หรือ “ผลประโยชน์สาธารณะ” กฎที่กว้างขวางและไม่มีความชัดเจนเช่นนี้ทำให้ข้อมูลหลายอย่างอาจถูกตีความเข้าประเภทเช่นว่านั้น และทำให้การโอนข้อมูลไม่สามารถทำได้[144] ซึ่งปัจจุบันยังไม่มีความคืบหน้าใด ๆ เกี่ยวกับเรื่องนี้

กฎหมายฉบับนี้ถูกมองว่าเป็นมาตรการอุปสรรคทางการค้าด้านเทคนิคก็เนื่องจากว่า มาตรานี้บังคับให้ผู้ให้บริการในประเทศจีนต้องเก็บข้อมูลส่วนบุคคลและข้อมูลที่สำคัญไว้ในประเทศ ซึ่งจากการตีความมาตรานี้จะเห็นได้ว่าถ้าหากมีการส่งข้อมูลจากนอกประเทศเข้ามาในประเทศจีน ประเทศจีนก็จะได้รับข้อมูลนี้ไปด้วย คล้ายกับหลักการว่า “เข้าได้ ออกไม่ได้” ทั้งที่จริงแล้ว ข้อมูลเหล่านั้นอาจไม่ได้เก็บมาจากพลเมืองของประเทศจีนเลยก็ตาม ประการถัดมา เนื่องจากในการให้บริการทางเครือข่ายที่เกี่ยวข้องกับระบบโครงสร้างพื้นฐานสำคัญ ผู้ให้บริการจะต้องใช้อุปกรณ์ในการรักษาความปลอดภัยที่ผลิตในประเทศจีนและรับรองโดยหน่วยงานของจีนเท่านั้น ซึ่งมีแนวโน้มว่าไม่ได้มีมาตรฐานในการรักษาความปลอดภัยที่ดีเท่าใดนัก ดังนั้น การนำข้อมูลจากนอกประเทศ ซึ่งเกี่ยวข้องกับทรัพย์สินทางปัญญา หรือข้อมูลต่าง ๆ มาเก็บไว้ในประเทศจีน ก็ยิ่งทำให้ข้อมูลเหล่านั้นรั่วไหลได้ง่ายขึ้น เพราะอุปกรณ์ที่ไม่ได้มาตรฐาน และสิ่งที่น่ากังวลที่สุด คือการที่ผู้ทำการเจาะระบบนั้นเป็นเจ้าหน้าที่รัฐเสียเอง เนื่องจากกฎหมายความมั่นคงปลอดภัยไซเบอร์จีน ให้อำนาจเจ้าหน้าที่อย่างกว้างขวางด้วยการอ้างเหตุผลด้านความมั่นคง ดังนั้น หากการเจาะระบบดังกล่าวได้ถูกทำโดยชอบด้วยกฎหมายแล้ว โอกาสที่ผู้ให้บริการจะได้รับการเยียวยาจากการรั่วไหลของข้อมูลก็ยิ่งน้อยลงไปอีก

จากความเสี่ยงในข้างต้น จึงทำให้กลุ่มธุรกิจจำนวนมากทั้งในสหรัฐอเมริกาและสหภาพยุโรปไม่กล้าที่จะเข้ามาลงทุนในประเทศจีน และจึงพิจารณาได้ว่าเป็นมาตรการอุปสรรคทางการค้าด้านเทคนิคในที่สุด

3.4.4 การรับรองมาตรฐานความปลอดภัย และการตรวจสอบ

ความปลอดภัยทางไซเบอร์จะเกิดขึ้นได้ก็เมื่อผู้ให้บริการเครือข่ายที่เกี่ยวข้องกับระบบโครงสร้างพื้นฐานสำคัญและผู้ให้บริการทั่วไปเลือกใช้ผลิตภัณฑ์หรือบริการที่มีมาตรฐานทางความปลอดภัยที่สูง ด้วยเหตุนี้ การกำหนดมาตรฐานจึงกลายเป็นอีกส่วนสำคัญของกฎหมายความปลอดภัยทางไซเบอร์ ตั้งแต่ค.ศ. 2007 ประเทศจีนได้ทำการออกแผนระดับความปลอดภัยหลายระดับ อย่างไรก็ดี แผนนี้ได้รับการวิพากจารณ์ว่าขัดแย้งกันกับมาตรฐานสากลว่าด้วยความปลอดภัยทางไซเบอร์และเป็นมาตรการที่เข้มงวดเกินไปอันอาจทำให้บริษัทในประเทศไม่สามารถแข่งขันกับบริษัทอื่นในตลาดโลกได้[145]

กฎหมายความปลอดภัยทางไซเบอร์กล่าวถึงการรับรองความปลอดภัยที่ซับซ้อนและวิธีการตรวจสอบ โดยในมาตรา 23 กำหนดให้อุปกรณ์ที่ใช้เพื่อบริการระบบโครงสร้างพื้นฐานสำคัญและผลิตภัณฑ์ที่ใช้เพื่อรักษาความปลอดภัยของโครงข่ายบางประเภทต้องเป็นไปตามมาตรฐานของชาติและข้อบังคับที่กำหนดไว้ และผ่าน

[144] Communication from the United States Measures Adopted and under Development by China Relating to Its Cybersecurity Law Paragraph 3 d.

[145] Blinderman, Eric, and Myra Din. 2017. "Hidden by Sovereign Shadows: Improving the Domestic Framework for Deterring State-Sponsored Cybercrime". Vanderbilt Journal of Transnational Law 50: 889, 896-897.

การรับรองมาตรฐานจากสถาบันที่กำหนดไว้หรือผ่านการตรวจสอบอย่างละเอียด นอกจากนี้ มาตรานี้ยังกำหนดให้หน่วยงานที่เกี่ยวข้องกับคณะรัฐมนตรีจัดแบ่งประเภทของอุปกรณ์เหล่านั้น และวางกฎเกณฑ์การรับรองหรือตรวจสอบมาตรฐานไม่ให้ซ้ำซ้อนกัน

ภายใต้มาตรา 35 ผลิตภัณฑ์และบริการที่เกี่ยวเนื่องกับโครงข่ายซึ่งถูกซื้อโดยผู้ให้บริการเครือข่ายที่เกี่ยวข้องกับระบบโครงสร้างพื้นฐานสำคัญด้านข้อมูลข่าวสาร ซึ่งอาจมีผลกระทบต่อความมั่นคงของชาติ ต้องนำผลิตภัณฑ์หรือบริการนั้นเข้าสู่กระบวนการพิจารณาโดยรัฐบาลเสียก่อน โดยทั้งมาตรา 23 และ 35 ต่างเป็นการสิ้นเปลืองเวลาและเป็นภาระทั้งสิ้น เพื่อบังคับใช้มาตรา 35 คณะกรรมการไซเบอร์เสปซของจีนได้ประกาศมาตรการว่าด้วยการพิจารณาความปลอดภัยสำหรับผลิตภัณฑ์และบริการที่เกี่ยวเนื่องกับโครงข่าย เมื่อวันที่ 2 พฤษภาคม ค.ศ. 2017 จากมาตรการนี้ คณะกรรมการไซเบอร์เสปซจะตั้งคณะกรรมการขึ้นมาเพื่อทำการพิจารณา[146] โดยมุ่งเน้นไปที่ว่าผลิตภัณฑ์นั้นปลอดภัยและสามารถควบคุมจัดการได้หรือไม่[147] โดยการพิจารณามีหลายขั้นตอนได้แก่ การตรวจสอบความปลอดภัย การตรวจสอบด้วยผลวิจัยทางแล็บ การตรวจสอบสถานที่ การตรวจสอบออนไลน์ และการตรวจสอบประวัติย้อนหลัง[148]

ถึงแม้ว่าในกฎหมายฉบับนี้ไม่ได้บังคับให้ผู้ผลิตเหล่านั้นต้องแสดงโค๊ดที่ใช้ในการเขียนให้กับกรรมการพิจารณา แต่กรรมการอาจร้องขอให้ผู้ผลิตแสดงสิ่งของรายการเช่นว่านั้นหรือขอให้ติดตั้งช่องทางพิเศษเพื่อให้รัฐบาลเข้าถึงลงไปในผลิตภัณฑ์หรือบริการ ซึ่งมาตรการนี้ได้นำมาใช้ในภาคธนาคารแล้วตั้งแต่ค.ศ. 2014 นอกจากนี้ มาตรการดังกล่าวยังมิได้บอกไว้อย่างชัดเจนว่าวิธีการอุทธรณ์คำสั่งคณะกรรมการเป็นเช่นไร ข้อมูลใดบ้างจะถูกร้องขอโดยคณะกรรมการ และในกรณีที่สินค้านั้นไม่ผ่านการพิจารณา ผู้ผลิตจะขอคืนได้อย่างไร และจากประโยคที่ว่า “...อาจมีผลกระทบต่อความมั่นคงของชาติ” ก็เปิดช่องให้รัฐบาลสามารถตีความได้อย่างกว้างขวางและใช้ในวัตถุประสงค์ทางการเมืองได้

มาตรการเหล่านี้มีวัตถุประสงค์สำคัญอย่างหนึ่งเพื่อป้องกันไม่ให้สินค้าหรือบริการเหล่านั้นถูกควบคุมโดยต่างชาติ[149] ประเทศจีนเชื่อว่าโครงข่ายดิจิทัลในประเทศจะเป็นเป้าหมายของการถูกโจมตี หากส่วนประกอบผลิตภัณฑ์ที่ระบบโครงสร้างพื้นฐานสำคัญใช้ผลิตโดยต่างชาติ ทั้งนี้ มาตรการตรวจสอบยังคงถูกวิจารณ์ในประเด็นความไม่ชัดเจนของกระบวนการและหลักเกณฑ์ที่ใช้ในการพิจารณา อันอาจนำไปสู่การสอดแนมของรัฐจีนอีกวิธีหนึ่งก็เป็นได้ ซึ่งย่อมส่งผลให้เกิดการรั่วไหลของข้อมูลต่างๆ รวมไปถึงความลับทางการค้าได้ สำนักงานผู้แทนการค้าสหรัฐ (the Office of United States Trade Representative : USTR) ก็ได้แสดงความกังวลเรื่องนี้ไว้อย่างชัดเจนในรายงานพิเศษมาตรา 301 ค.ศ. 2017 ว่าหลายบริษัทอาจถูกบังคับให้ต้องเปิดเผยเรื่องทรัพย์สินทางปัญญา เพื่อให้สอดคล้องกับมาตรการพิจารณานี้

---

[146] 《关键信息基础设施安全保护条例（征求意见稿）》（保护条例）第 5 条

[147] 《关键信息基础设施安全保护条例（征求意见稿）》（保护条例） 第 4 条

[148] 《关键信息基础设施安全保护条例（征求意见稿）》（保护条例）第 3 条

[149] Hoffmann, Richard. 2017. "Update: China Releases New Draft Regulations regarding Cyber Security of Online Services and Products". Ecovis BEIJING. http://www.ecovis-beijing.com/enfblog-en/articles/810-update-china.

นอกจากนี้แล้ว การรับรองมาตรฐานความปลอดภัยและการตรวจสอบในมาตรา 23 และ 35 ยังเป็นการแทรกแซงตลาด โดยใช้อำนาจทางการเมืองในการปิดกั้นหรือประวิงเวลาไม่ให้ผู้ผลิตสามารถนำสินค้าหรือบริการเหล่านั้นไปขายให้กับผู้ให้บริการเครือข่ายที่เกี่ยวข้องกับระบบโครงสร้างพื้นฐานสำคัญได้ ในขณะเดียวกันก็ส่งผลกระทบต่อการตัดสินใจของผู้ประกอบการในการเลือกซื้อสินค้าหรือบริการที่เกี่ยวข้อง[150] มาตรการดังกล่าวอาจมีขึ้นเพื่อลดการพึ่งพาเทคโนโลยีความปลอดภัยจากต่างชาติและสนับสนุนการลงทุนสินค้าและบริการดังกล่าวในประเทศจีนแทน

3.4.5 การคุ้มครองข้อมูลส่วนบุคคล

การควบคุมความสมดุลระหว่างความปลอดภัยทางไซเบอร์ ความมั่นคงของชาติ และการปกป้องความเป็นส่วนตัว นับเป็นโจทย์ท้าทาย ก่อนจะมีการบังคับใช้กฎหมายความปลอดภัยทางไซเบอร์ รัฐบาลจีนได้ผ่านกฎหมายมากมายเพื่อคุ้มครองข้อมูลส่วนบุคคล ดังเช่น Decision of the Standing Committee of the National People's Congress to Strengthen the Protection of Internet Data (2012) และ The Guidelines for Personal Information Protection within Public and Commercial Services Information Systems (2013) และ the Provisions on Protecting the Personal Information of Telecommunication and Internet Users (2013) จนกระทั่งมาถึงกฎหมายความปลอดภัยทางไซเบอร์ซึ่งบัญญัติเรื่องการคุ้มครองข้อมูลส่วนบุคคลไว้อย่างชัดเจน

กฎหมายความปลอดภัยทางไซเบอร์ได้ให้นิยามคำว่า “ข้อมูลส่วนบุคคล” ไว้ว่า ข้อมูลที่ด้วยตัวมันเองหรือเมื่อนำไปรวมกับข้อมูลอื่นสามารถระบุตัวตนของบุคคลใดบุคคลหนึ่งหรือกลายเป็นข้อมูลใดข้อมูลหนึ่งอันอาจชี้ถึงตัวบุคคลนั้นๆ ได้ อาทิ ชื่อของบุคคลนั้น วันเกิด เลขบัตรประจำตัวประชาชน ข้อมูลรูปพรรณสัณฐาน ที่อยู่ และหมายเลขโทรศัพท์[151] ดังนั้น หากข้อมูลเหล่านี้ได้รับการปกปิดหรือไม่ได้แสดงออกมาแต่แรก ก็จะไม่จัดว่าเป็นข้อมูลส่วนบุคคลตามกฎหมายนี้

จากกฎหมายความปลอดภัยทางไซเบอร์ ผู้ให้บริการโครงข่ายจะต้องรวบรวมหรือใช้ข้อมูลส่วนบุคคลอย่างถูกกฎหมาย เหมาะสม และเท่าที่จำเป็น และผู้ให้บริการต้องเปิดเผยวัตถุประสงค์ วิธีการ และขอบเขตในการรวบรวมข้อมูลของพวกเขา และได้รับความยินยอมจากบุคคลผู้นั้นก่อนที่จะทำการเก็บข้อมูลนั้นได้[152] ทั้งเจ้าของข้อมูลยังมีสิทธิในการเปลี่ยนแปลงแก้ไข หรือลบข้อมูลนั้นได้ด้วย[153] ทั้งนี้ ข้อมูลส่วนตัวใดที่ไม่เกี่ยวข้องกับการให้บริการ ห้ามผู้ให้บริการเก็บข้อมูลนั้น[154] นอกจากนี้ ห้ามผู้ให้บริการเปิดเผยข้อมูลเหล่านั้นกับบุคคล

---

[150] Reuters. 2017. "China’s Tough Cybersecurity Law to Come into Force This Week". South China Morning Post. http://www.scmp.com/news/china/policies-politics/article/2096094/chinas-tough-cybersecurity-law-come-force-week.

[151] 《中华人民共和国网络安全法》第 76 条
[152] 《中华人民共和国网络安全法》第 41 条
[153] 《中华人民共和国网络安全法》第 47 条
[154] 《中华人民共和国网络安全法》第 41 条

อื่น เว้นแต่ข้อยกเว้นดังนี้ 1. บุคคลที่ให้ข้อมูลนั้นได้ให้ความยินยอมแล้ว 2. ข้อมูลนั้นได้รับการแปลงสภาพให้ไม่สามารถทราบได้แล้วว่าหมายถึงบุคคลใดโดยเฉพาะเจาะจง[155] สุดท้ายนี้ ผู้ให้บริการไม่สามารถเปิดเผย ดัดแปลง หรือทำลายข้อมูลที่พวกเขาเก็บมาได้[156]

หากผู้ให้บริการละเมิดบทบัญญัติที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลแล้ว ผู้ให้บริการอาจถูกตักเตือนและสั่งให้แก้ไข ยึดทรัพย์ หรือปรับไม่เกิน 1 ล้านหยวน และปรับผู้ที่มีส่วนรับผิดชอบโดยตรงและผู้บังคับบัญชาตั้งแต่ 1 หมื่นหยวน แต่ไม่เกิน 1 แสนหยวน ทว่าหากความเสียหายร้ายแรง ผู้ให้บริการอาจถูกสั่งให้ระงับการให้บริการในส่วนที่เกี่ยวข้อง ปิดเว็บไซต์ หรือระงับการประกอบกิจการทั้งหมด รวมไปถึงการระงับใบอนุญาตประกอบกิจการชั่วคราวหรือถาวร[157]

มีข้อสังเกตในประเด็นของกฎหมายอาญาคือการที่บุคคลต้องรับผิดเมื่อมีการฝ่าฝืนบทบัญญัติกฎหมายในส่วนข้อมูลส่วนบุคคล มิใช่เพียงผู้ที่มีหน้าที่ต้องรับผิดชอบโดยตรงเท่านั้นที่จะถูกโทษปรับ หากแต่ผู้บังคับบัญชาของผู้นั้นก็จะถูกโทษปรับไปด้วย ซึ่งขัดกับหลักที่ว่าบุคคลจะต้องรับผิดในทางอาญาก็ต่อเมื่อได้ทำโดยเจตนา อย่างไรก็ตาม กฎหมายอาจมองว่าผู้บังคับบัญชามีหน้าที่ต้องกำกับดูแลผู้ใต้บังคับบัญชาอยู่แล้ว หากผู้ใต้บังคับบัญชาตนทำงานผิดพลาด ส่วนหนึ่งย่อมเป็นเพราะผู้บังคับบัญชาประมาทเลิกเล่อ เพิกเฉย ไม่กวดขันผู้ใต้บังคับบัญชาของตนเองให้ดี จนทำให้เกิดการละเมิดข้อมูลส่วนบุคคลได้ในที่สุด

หากพิจารณาในมาตรา 64 วรรคหนึ่งแล้วจะพบว่ามีวิธีการลงโทษที่หลากหลาย และยืดหยุ่นมาก ตั้งแต่ตักเตือน จนถึงโทษปรับ และระงับใบอนุญาตประกอบกิจการ ซึ่งเป็นการให้อำนาจแก่เจ้าหน้าที่ในการใช้ดุลพินิจที่กว้างขวางมาก จนทำให้การบังคับกฎหมายอาจไม่เป็นไปตามมาตรฐาน ดังเช่นในตัวอย่างคดีที่ 1 และ 2 ด้านล่าง แม้จะมีข้อเท็จจริงเดียวกันว่าแอปพลิเคชันเหล่านั้นไม่ได้ขอความยินยอมผู้ใช้ในการเก็บข้อมูลส่วนบุคคลแต่แรกเหมือนกัน ผลกลับปรากฏว่าผู้ให้บริการรายหนึ่งนอกจากจะถูกสั่งให้แก้ไขแล้ว ทั้งผู้บังคับบัญชาและผู้ที่มีหน้าที่รับผิดชอบโดยตรงกลับต้องโดนปรับอีกคนละ 1 หมื่นหยวน ในขณะที่ผู้ให้บริการอีกหนึ่งรายนั้นกลับเพียงถูกตักเตือนแต่เพียงอย่างเดียวเท่านั้น กรณีนี้จึงมีข้อกังวลว่ากฎหมายที่มอบอำนาจดุลพินิจให้แก่เจ้าหน้าที่มากเกินไปจะทำให้การบังคับใช้กฎหมายเป็นไปตามอำเภอใจ และอาจเป็นการส่งเสริมให้ผู้กระทำผิดให้สินบนแก่เจ้าหน้าที่เพื่อหลีกเลี่ยงโทษสถานหนักแทน

ทั้งนี้ ในมาตรา 64 วรรคหนึ่ง เมื่อมีการละเมิดข้อมูลส่วนบุคคลเกิดขึ้นแล้ว กฎหมายได้ให้ดุลพินิจเจ้าหน้าที่ในการตักเตือนและสั่งให้แก้ไขได้ โดยไม่บังคับให้ลงโทษด้วยวิธีอื่นไปด้วยพร้อมกันแต่อย่างใด อำนาจนี้อาจสันนิษฐานได้ว่าผู้ร่างกฎหมายอาจยอมรับว่า การละเมิดข้อมูลส่วนบุคคลอาจเป็นความผิดที่เกิดขึ้นเพราะกฎหมายกำหนดให้เป็นความผิด (mala prohibita) ดังนั้นเป็นไปไม่ได้เลยที่สามัญสำนึกของมนุษย์จะทราบได้ว่าการเก็บข้อมูลอย่างถูกต้องนั้น ผู้ให้บริการต้องขอความยินยอมจากผู้ใช้งาน ดังนั้นผู้ร่างกฎหมายจึงกำหนดทางแก้ไขไว้ โดยให้มีการตักเตือนขึ้น เพื่อเปิดโอกาสให้บุคคลนั้นทำการแก้ไข และเพื่อให้ไม่เกิดการ

[155] 《中华人民共和国网络安全法》第 41 条
[156] 《中华人民共和国网络安全法》第 42 条
[157] 《中华人民共和国网络安全法》第 64 条 第一款

ลงโทษแก่ผู้บริสุทธิ์โดยไม่จำเป็น โดยมากแล้ว ผู้ให้บริการที่กระทำผิดตามมาตรา 64 วรรคหนึ่ง ด้วยการไม่ได้ขออนุญาตเก็บข้อมูลส่วนบุคคลก่อน หรือละเลยปล่อยข้อมูลเหล่านั้นไปบนเว็บไซต์ของตนเองมักจะถูกตักเตือนเสียมาก มีคดีจำนวนน้อยรายมากที่การทำผิดครั้งแรกจะมีโทษปรับเกิดขึ้น

นอกจากผู้ให้บริการมีหน้าที่ตามกฎหมายที่จะต้องปฏิบัติตามเพื่อไม่ให้ละเมิดข้อมูลส่วนบุคคลแล้ว กฎหมายฉบับนี้ยังบังคับกับบุคคลอื่นโดยทั่วไปด้วยว่า “ห้ามมิให้ผู้ใดทำการโจรกรรมข้อมูลหรือทำการด้วยวิธีที่มิชอบด้วยกฎหมายอื่นใด เพื่อให้ได้มาซึ่งข้อมูลส่วนบุคคล รวมทั้งห้ามมิให้ทำการขายข้อมูลเหล่านั้นหรือมอบข้อมูลเหล่านั้นให้แก่ผู้อื่น”[158] หากผู้ใดฝ่าฝืนบทบัญญัติดังกล่าว ไม่ว่าจะมีการกระทำความผิดตามกฎหมายนี้เกิดขึ้นหรือไม่ก็ตาม ให้ตำรวจยึดทรัพย์ที่ได้มาจากการกระทำความผิดนี้ และปรับได้ตั้งแต่ 1 ถึง 10 เท่าของราคาทรัพย์นั้น และหากไม่มีทรัพย์ที่ได้มาจากการกระทำความผิด ให้ปรับไม่เกิน 1 ล้านหยวน

เมื่อพิจารณาโทษของการทำเพื่อให้ได้มาซึ่งข้อมูลส่วนบุคคลโดยมิชอบด้วยกฎหมาย หรือมอบข้อมูลเหล่านั้นให้แก่บุคคลอื่น จะพบว่ามีข้อสังเกต 2 ประการ ประการแรก กฎหมายข้อนี้ไม่ให้ดุลพินิจเจ้าหน้าที่ในการตักเตือนผู้กระทำผิดเลย อาจสันนิษฐานได้ว่าผู้ร่างกฎหมายมองว่าการโจรกรรมข้อมูลบุคคลอื่นเป็นการกระทำที่มีความผิดในตัวเอง (mala in se) และบุคคลทั่วไปสามารถเข้าใจได้เช่นเดียวกับการที่ตนเข้าใจว่าการขโมยทรัพย์สินผู้อื่นเป็นความผิด ดังนั้นการลงโทษผู้ที่กระทำการเช่นนี้จึงไม่ต้องมีการผ่อนปรน

ประการถัดมา บทลงโทษนี้มีมาตรการริบทรัพย์เด็ดขาด แม้ในกรณีที่บุคคลหนึ่งได้รับข้อมูลส่วนบุคคลของผู้อื่นมาโดยสุจริต เช่น สำคัญผิดว่าข้อมูลเหล่านั้นได้รับการยินยอมจากเจ้าของข้อมูลส่วนบุคคลจริงทั้งในการรวบรวมและจำหน่ายต่อไปยังบุคคลที่สาม ทั้งที่จริงแล้ว ข้อมูลเหล่านั้นเป็นข้อมูลที่มิจฉาชีพเอามาปล่อยทิ้งไว้เพื่อสร้างความวุ่นวาย ถึงกระนั้น บุคคลที่รับข้อมูลมาโดยสุจริต และได้ทำการจำหน่ายไป เงินนั้นก็คงเป็นทรัพย์สินที่ได้มาจากการกระทำความผิดอยู่ ดังนั้น แม้บุคคลที่สุจริตนั้นจะไม่ต้องรับผิดในกฎหมายอาญาอื่นที่เกี่ยวข้อง บุคคลที่สุจริตนั้นก็ยังคงต้องถูกยึดเงินที่ได้มาจากการขายข้อมูลนั้น พร้อมทั้งถูกปรับด้วย บทบัญญัติที่เข้มงวดนี้แสดงให้เห็นถึงความเด็ดขาดในการพยายามที่จะป้องกันไม่ให้บุคคลใดก็ตามไม่ว่าจะสุจริตหรือไม่ได้ไปซึ่งผลประโยชน์จากการใช้ข้อมูลส่วนบุคคลที่ได้มาโดยมิชอบ จนอาจคิดไปได้ว่ากฎหมายนี้ต่างจากกฎหมายลักษณะทรัพย์ที่คุ้มครองการได้มาของทรัพย์สินของผู้ที่เสียค่าตอบแทนโดยสุจริต ซึ่งอาจแสดงให้เห็นว่าข้อมูลส่วนบุคคลแม้จะมีค่า แต่ก็ไม่ได้มีถูกคุ้มครองในฐานะทรัพย์สินอย่างที่เข้าใจกัน หากแต่เป็นส่วนหนึ่งของบุคคล ๆ หนึ่ง และได้รับการเคารพในฐานะสิทธิส่วนบุคคลที่มีความสำคัญยิ่งกว่า ดังนั้นการคุ้มครองข้อมูลส่วนบุคคลจึงมีมาตรการที่เด็ดขาดกว่ามากเพื่อป้องกันความเสียหายต่าง ๆ ที่จะเกิดขึ้น

แม้กฎหมายนี้จะคุ้มครองความเป็นส่วนตัวของประชาชน โดยสร้างหน้าที่ให้กับผู้ให้บริการ ทว่าเจ้าหน้าที่รัฐกลับไม่ต้องอยู่ภายใต้บังคับของหน้าที่นี้ กล่าวคือภายในกฎหมายฉบับเดียวกัน แต่ในหมวดอื่นกฎหมายกลับเป็นเครื่องมือให้เจ้าหน้าที่รัฐใช้ในการควบคุมและสอดแนมข้อมูลส่วนบุคคลและโยนภาระต่างๆ ให้กับผู้ให้บริการ ตัวอย่างเช่น ผู้ให้บริการมีหน้าที่ให้ความช่วยเหลือทางเทคนิคแก่เจ้าหน้าที่รัฐในการรักษา

[158] 《中华人民共和国网络安全法》第 44 条

ความมั่นคงของชาติและสอบสวนอาชญากรรม ทำให้เจ้าหน้าที่รัฐสามารถใช้ช่องทางพิเศษเข้าถึงข้อมูลส่วนบุคคลได้โดยชอบด้วยกฎหมาย และด้วยการที่กฎหมายบังคับให้ผู้ให้บริการต้องเก็บข้อมูลส่วนตัวผู้ใช้บริการให้สามารถดูย้อนหลังได้ไม่น้อยกว่า 6 เดือน ซึ่งเพิ่มความเสี่ยงในการรั่วไหล ก็ฝ่าฝืนหลักการในการคุ้มครองข้อมูลส่วนบุคคลด้วยเช่นกัน และการเก็บข้อมูลในระยะเวลาที่ยาวนานเช่นนี้ก็เป็นการเพิ่มภาระแก่บริษัทรายย่อยด้วย

กฎหมายความปลอดภัยทางไซเบอร์นี้ รวมไปถึงการบังคับให้ผู้ใช้งานแสดงตัวตนของตนก่อนเข้าใช้งาน โดยมอบหน้าที่นี้ให้กับผู้ให้บริการ และห้ามผู้ให้บริการให้บริการกับผู้ใช้งานที่ไม่ยอมแสดงตัวตน ซึ่งมาตรการนี้ถูกอ้างว่ามีวัตถุประสงค์เพื่อใช้ปราบปรามข่าวลือ การใช้คำไม่สุภาพ สื่อลามกอนาจาร และข่าวสารที่เกี่ยวกับการก่อการร้าย อย่างไรก็ดี ในอีกมุมหนึ่ง กฎหมายนี้ก็เป็นเครื่องมือของรัฐบาลในการป้องกันไม่ให้ผู้ใช้งานอินเทอร์เน็ตวิพากษ์วิจารณ์รัฐบาลหรือกระจายข่าวของรัฐบาลว่าด้วยการทุจริต ดังนั้นระบบนี้จึงมีขึ้นเพื่อขัดขวางไม่ให้ผู้คนแสดงความคิดเห็นในที่สาธารณะ นอกจากนี้ นโยบายแสดงตัวตนอาจสร้างโอกาสให้แฮ็คเกอร์ทำการแฮ็คข้อมูลส่วนบุคคลเหล่านั้นจากผู้ให้บริการหลายรายได้อีกด้วย

กรณีศึกษา: ตัวอย่างคดีการคุ้มครองข้อมูลส่วนบุคคล

1. ในค.ศ. 2019 ตำรวจจังหวัดซูโจว มณฑลเจียงซูได้พบว่ามีบริษัทเทคโนโลยีทางการแพทย์หนึ่งได้จัดทำแอปพลิเคชันที่ให้คำแนะนำด้านการแพทย์ขึ้น แต่ในการเก็บข้อมูลส่วนบุคคลนั้นกลับไม่ได้แจ้งข้อตกลงความเป็นส่วนตัวแก่ผู้ใช้บริการโดยชัดแจ้งว่าตนจะทำการเก็บข้อมูล หรือแจ้งวัตถุประสงค์ในการเก็บข้อมูล ดังนั้นตำรวจจึงได้ทำการปรับผู้ที่มีส่วนรับผิดชอบโดยตรงและผู้บังคับบัญชาคนละ 1 หมื่นหยวน และสั่งให้แก้ไขภายในระยะเวลาที่กำหนด ตามมาตรา 41 ประกอบกับมาตรา 64 วรรคหนึ่งของกฎหมายความมั่นคงปลอดภัยไซเบอร์ [159]

2. ในค.ศ. 2019 ตำรวจจังหวัดฉางโจว มณฑลเจียงซูได้รับแจ้งรายงานว่าแอปพลิเคชันนำทางได้เก็บข้อมูลผู้ใช้โดยที่ผู้ใช้ไม่รู้ตัว จากการตรวจสอบพบว่าแอปพลิเคชันได้เก็บทั้งข้อมูลสถานที่หมาย สถานที่รอบข้าง และวิธีการเดินทางของผู้ใช้จริง โดยมิได้ทำการขอความยินยอมก่อน ดังนั้นตำรวจจึงได้ตักเตือนและสั่งให้แก้ไขในระยะเวลาที่กำหนด ตามมาตรา 41 ประกอบกับมาตรา 64 วรรคหนึ่งของกฎหมายความมั่นคงปลอดภัยไซเบอร์ [160]

3. ในค.ศ. 2019 ตำรวจจังหวัดเซียงเซียง มณฑลหูหนานได้รับรายงานว่าบริษัทขายอุปกรณ์เชิงอุตสาหกรรมไฟฟ้าแห่งหนึ่งทำให้ข้อมูลส่วนบุคคลรั่วไหล เมื่อตำรวจทำการตรวจสอบโดยเข้าไปที่เว็บไซต์ของบริษัท จึงได้พบว่ามีข้อมูลของพนักงานบริษัททั้งหมด 296 คนถูกแสดงอย่างละเอียด อันประกอบไปด้วยชื่อ

[159] เรื่องเดียวกัน.

[160] เรื่องเดียวกัน.

สกุล หมายเลขบัตรประจำตัวประชาชน และเบอร์โทรศัพท์ ดังนั้น ในเบื้องต้น ตำรวจจึงได้ทำการตักเตือนและสั่งให้แก้ไข ตามมาตรา 41 ประกอบกับมาตรา 64 วรรคหนึ่งของกฎหมายความมั่นคงปลอดภัยไซเบอร์ [161]

4. วันที่ 22 เมษายน ค.ศ. 2020 ตำรวจไซเบอร์จังหวัดซู่เชียน มณฑลเจียงซู ได้ทำการตรวจสอบความปลอดภัยไซเบอร์ของสถานออกกำลังกายแห่งหนึ่งและพบว่าในการเก็บรูปภาพใบหน้าของผู้ใช้บริการนั้น ผู้ให้บริการไม่ได้ทำการแจ้งเตือนแก่เจ้าของใบหน้า และไม่ได้แจ้งถึงวัตถุประสงค์ในการเก็บข้อมูลดังกล่าว นอกจากนี้ การเก็บรูปภาพเหล่านั้นก็ไม่ได้ทำการเข้ารหัสไว้เลย ด้วยเหตุนี้ ตำรวจไซเบอร์จึงได้ทำการตักเตือนและสั่งให้แก้ไข[162] ตามมาตรา 41 ประกอบกับมาตรา 64 วรรคหนึ่งของกฎหมายความมั่นคงปลอดภัยไซเบอร์นี้

5. ในปี 2018 ตำรวจจังหวัดหนานทง มณฑลเจียงซูได้รับรายงานว่ามีกลุ่มนักวิเคราะห์การตลาดของบริษัทโฆษณาแห่งหนึ่งได้ทำการเก็บข้อมูลส่วนบุคคลโดยมิชอบด้วยกฎหมาย และได้ส่งต่อให้แก่บริษัทต่าง ๆ ที่ขายวัสดุตกแต่งอาคารให้ใช้ประโยชน์ต่อ โดยบริษัทเหล่านี้ได้ใช้เบอร์โทรศัพท์ส่วนตัวนั้นเสนอขายอุปกรณ์ตกแต่งบ้าน และเฟอร์นิเจอร์ให้แก่เจ้าของเบอร์โทรศัพท์มือถือในท้ายที่สุด การกระทำนี้เกิดขึ้นนับครั้งไม่ถ้วน จนมีผู้ใช้ที่ถูกละเมิดข้อมูลส่วนบุคคลกว่า 4 แสนคน ด้วยเหตุนี้จึงมีบุคคลที่เกี่ยวข้องกับการกระทำนี้กว่า 261 คนถูกลงโทษตามมาตรา 44 ประกอบกับมาตรา 64 วรรคสองของกฎหมายความมั่นคงปลอดภัยไซเบอร์ และมีอีก 8 ผู้ต้องสงสัยว่าได้กระทำความผิดถูกดำเนินคดีอาญาอื่นต่อไป[163]

6. ในปี 2019 บริษัทหนึ่งในจังหวัดเหยียนเฉิง มณฑลเจียงซูได้ซื้อข้อมูลส่วนบุคคลมาจากบุคคลอื่นกว่า 6 หมื่นรายการ โดยข้อมูลเหล่านั้นประกอบด้วยชื่อสกุล และเบอร์โทรศัพท์ บริษัทนี้ได้ใช้ข้อมูลดังกล่าวเพื่อเพิ่มยอดขาย แต่มิได้ส่งข้อมูลเหล่านั้นไปขายต่อแต่อย่างใด ดังนั้น เจ้าหน้าที่ตำรวจจึงปรับบริษัทเป็นเงินจำนวน 1 แสนหยวน ตามมาตรา 44 ประกอบกับมาตรา 64 วรรคสองของกฎหมายความมั่นคงปลอดภัยไซเบอร์[164]

7. ในปี 2019 ในขณะที่บริษัทหนึ่งในจังหวัดฉางโจว มณฑลเจียงซูกำลังเสนอขายสินค้าผ่านทางแอปพลิเคชัน TikTok เพื่อโฆษณาธุรกิจของตน บริษัทได้ทำการแสดงหนังสือยืนยันสถานะการพำนักในญี่ปุ่นของบุคคล 22 คน โดยมีทั้งรูปถ่ายของบุคคลนั้น ชื่อสกุล และวันเดือนปีเกิด เจ้าหน้าที่ตำรวจจึงปรับบริษัทเป็นเงิน

[161] 娄底网警巡查执法. 2019. "「净网 2019」网络安全行政执法十大类典型案例". Baidu. https://baijiahao.baidu.com/s?id=1649618195170303205&wfr=spider&for=pc.
[162] 季，雨. 2020. "违规进行人脸采集，江苏宿迁一健身中心被罚！". *腾讯网*. https://xw.qq.com/cmsid/20200509A0A0JZ00.
[163] 南通网警巡查执法. 2020. "国家安全教育日丨网络安全 人人有责". *Baidu*. https://baijiahao.baidu.com/s?id=1664003149856685134&wfr=spider&for=pc.
[164] 保定网警巡查执法. 2020. "公安机关"净网 2019"网络安全相关典型案例". Baidu. https://baijiahao.baidu.com/s?id=1655167701544954540&wfr=spider&for=pc.

จำนวน 2 หมื่นหยวน ตามมาตรา 44 ประกอบกับมาตรา 64 วรรคสองของกฎหมายความมั่นคงปลอดภัยไซเบอร์[165]

3.5 ปัญหาความไม่ชัดเจนและกำกวมของภาษาที่ใช้ในกฎหมาย

กฎหมายความปลอดภัยทางไซเบอร์ของจีนได้รับการวิพากษ์วิจารณ์อย่างกว้างขวางในเรื่องความไม่แน่นอนและความกำกวมของตัวบท ที่พบเห็นได้ ได้แก่คำว่า “ระบบโครงสร้างพื้นฐานสำคัญ” ซึ่งเป็นคำที่มีความหมายกว้างขวางมาก ราวกับว่าผู้ให้บริการทุกคนอาจพร้อมถูกจัดให้อยู่ในประเภทนี้ และกลายเป็นต้องปฏิบัติหน้าที่ตามกฎหมายที่มากขึ้น หรือในประเด็นเรื่องระบบการคุ้มครองหลายลำดับชั้น (Multi-Level Protection Scheme หรือ MLPS) ที่แบ่งประเภทของผู้ให้บริการเครือข่ายออกเป็น 5 ระดับ โดยพิจารณาจากความเสียหาย ก็พบว่า “ความเสียหายมาก” และ “ความเสียหายอย่างรุนแรง” ก็ไม่ได้มีนิยามที่ชัดเจน และเวลาผู้ให้บริการจะทราบว่าตนเป็นผู้ให้บริการระดับใด ก็คือเวลาที่ผู้ให้บริการได้ทำการจัดตั้งระบบและรอการประเมินจากผู้เชี่ยวชาญและเจ้าหน้าที่แล้วเท่านั้น ทำให้ผู้ให้บริการไม่สามารถคำนวณต้นทุนเพื่อนำมาใช้จ่ายเพื่อปฏิบัติตามกฎหมายได้ดีเท่าที่ควร หรือในประเด็นเรื่องการเก็บรวบรวมข้อมูลไว้ในท้องที่ ซึ่งมีข้อกำหนดห้ามไม่ให้โอนข้อมูลไป หากกระทบต่อ “ความมั่นคงของประเทศ” “การพัฒนาทางเศรษฐกิจ” หรือ “ผลประโยชน์สาธารณะ” ซึ่งกฎหมายก็ไม่ได้บอกไว้ชัดเจนเช่นกัน แสดงให้เห็นถึงเจตนาของผู้ร่างกฎหมายที่จะออกแบบให้เจ้าหน้าที่ตามกฎหมายนี้สามารถใช้ดุลยพินิจได้อย่างกว้างขวาง

การบัญญัติกฎหมายด้วยคำที่กว้างและกำกวมนี้ เป็นที่พบเห็นได้โดยปกติทั่วไปในประเทศจีน ซึ่งมักจะให้อำนาจหน่วยงานบริหารในการตีความและบังคับใช้กฎหมายนั้นอย่างยืดหยุ่น และความยืดหยุ่นนี้เองก็มีไว้เพื่อรับมือกับสภาพของสังคมและเศรษฐกิจที่เปลี่ยนแปลงไปอย่างรวดเร็ว ส่วนในการบังคับใช้กฎหมายนั้น หน่วยงานบริหารและกำกับดูแลต่างต้องสร้างระเบียบบริหารที่มีรายละเอียดชัดเจนขึ้น ทว่า สิ่งที่เกิดขึ้นคือกฎหมายจีนมักมีความขัดแย้งกันและเปิดช่องให้ใช้ดุลพินิจได้มาก ความอ่อนแอของหลักนิติธรรมนี้ได้สร้างความรู้สึกไม่แน่นอนใจกับภาระทางการเงินที่สูงขึ้นให้แก่ผู้ประกอบธุรกิจ ดังเช่นที่ปรากฏอยู่ในกฎหมายความปลอดภัยทางไซเบอร์ในปัจจุบัน

ความกว้างของภาษาที่ใช้ในกฎหมายความปลอดภัยทางไซเบอร์แสดงให้เห็นถึงความต้องการของรัฐในการใช้กฎหมายเพื่อควบคุมอุตสาหกรรม โดยมีผู้ตั้งข้อสังเกตว่ากฎหมายฉบับนี้ถูกออกแบบขึ้นเพื่อสร้างความยืดหยุ่นให้แก่เหล่าเจ้าหน้าที่ในการตีความและปรับใช้[166] ผู้กำกับดูแลอาจใช้กฎหมายนี้บังคับแก่ผู้คนหรือบริษัทที่ไม่เชื่อฟัง หรือถึงขั้นว่าใช้กำจัดผู้ที่เป็นเสี้ยนหนามของรัฐ ความกำกวมของภาษาที่ใช้ในกฎหมายฉบับ

[165] เรื่องเดียวกัน.

[166] Iasiello, Emilio. 2017. "China’s Cyber Initiatives Counter International Pressure". Journal Of Strategic Security 10 (1): 8.

นี้ทำให้บริษัทอินเทอร์เน็ตต่างๆ ต้องเสียเวลาในการสำรวจและทำความเข้าใจว่ารัฐบาลจีนจะใช้กฎหมายฉบับนี้อย่างไร และผู้กำกับดูแลจะมีทิศทางในการตีความไปในทางใด

กฎหมายความปลอดภัยทางไซเบอร์ของจีนในปัจจุบันส่งผลกระทบต่อความมั่นคงปลอดภัยไซเบอร์และสิทธิมนุษยชนบนโลกดิจิทัล และสะท้อนให้เห็นถึงความไม่ไว้เนื้อเชื่อใจของรัฐที่มีต่อกลไกการทำของเอกชนในด้านการจัดการความมั่นคงไซเบอร์ ด้วยเหตุนี้ กฎหมายฉบับดังกล่าว จึงบัญญัติด้วยศัพท์ที่มีความหมายกว้างซึ่งทำให้ผู้ใช้อำนาจสามารถตีความได้หลากหลายและสร้างความไม่แน่นอนให้กับภาคธุรกิจในอุตสาหกรรมต่างๆ

ภายใต้การบังคับใช้ของกฎหมายความมั่นคงปลอดภัยไซเบอร์นี้ ผู้ให้บริการทางโครงข่ายซึ่งประกอบกิจการอันเกี่ยวข้องกับระบบโครงสร้างพื้นฐานสำคัญจะถูกบังคับให้มีส่วนร่วมในการปกป้องความมั่นคงปลอดภัยไซเบอร์ด้วย ประเทศจีนเชื่อมั่นในระบบบังคับและจะทดลองมาตรการต่างๆ เพื่อนำไปสู่การให้ความคุ้มครองระบบโครงสร้างพื้นฐานที่มีประสิทธิภาพและยั่งยืน สำหรับประเด็นเรื่องการเก็บรวบรวมข้อมูลในท้องที่นั้น ก็จัดว่าเป็นอีกภาระหนึ่งที่ยุ่งยากสำหรับผู้ให้บริการเครือข่ายที่เกี่ยวข้องกับระบบโครงสร้างพื้นฐานสำคัญ และไม่มีความแน่ชัดว่ามาตรการดังกล่าวจะช่วยเสริมสร้างความแข็งแกร่งให้กับความปลอดภัยไซเบอร์ในระยะยาวได้จริง ทั้งนี้ มาตรการการเก็บรวบรวมข้อมูลในท้องที่อาจทำให้ผู้ประกอบธุรกิจได้รับความเสี่ยงจากการถูกสอดแนมโดยรัฐบาลท้องที่ และถึงแม้ว่ากฎหมายจะมีบทบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลเกิดขึ้นมาแล้วก็ตาม แต่กฎหมายความปลอดภัยทางไซเบอร์ก็ยังให้อำนาจรัฐบาลในการเข้าถึงข้อมูลเหล่านั้น อันนำไปสู่การรั่วไหลของข้อมูลอยู่นั่นเอง

บทที่ 4

ศึกษาเปรียบเทียบแนวทางการรักษาความปลอดภัยทางไซเบอร์

ของประเทศสหรัฐอเมริกาและสหภาพยุโรป

ในบทนี้ จะดำเนินการศึกษาเปรียบเทียบแนวทางการรักษาความปลอดภัยทางไซเบอร์ของจีนกับแนวทางของประเทศสหรัฐอเมริกาและสหภาพยุโรป โดยจะเน้นการเปรียบเทียบในประเด็นกฎหมายสำคัญต่างๆ ในขณะเดียวกัน จะมีการอภิปรายเพิ่มเติมเกี่ยวกับกรณีศึกษาที่น่าสนใจเกี่ยวกับกฎหมายของประเทศออสเตรเลียนอกจากนั้น ในตอนท้ายของบท ยังมีกรณีศึกษาเกี่ยวกับกรอบความร่วมมือระหว่างประเทศที่เกี่ยวข้องกับการรักษาความปลอดภัยทางไซเบอร์เพิ่มเติมด้วย แท้จริงแล้วแม้ว่าองค์กรเหล่านี้จะไม่ได้ออกกฎหมาย แต่เป็นเวทีที่ทำการวิเคราะห์ปัญหาและหาแนวทางการแก้ไขแบบแสวงฉันทามติ (consensus) ซึ่งย่อมส่งอิทธิพลทางความคิดและมีผลให้เกิดกลไกที่จะตอบโต้การโจมตีที่มีเทคนิคใหม่ๆ จะเห็นได้ว่าแนวคิดนี้เป็นแบบอย่างที่สำนัก cyber commons ถือเป็นหลักในการแสวงหาแนวทางแก้ไขปัญหาความมั่นคงปลอดภัยทางไซเบอร์ บทบาทของเวทีเหล่านี้จึงเป็นเรื่องสำคัญในการช่วงชิงการเป็นผู้นำ ดังที่จีนเองได้จัดให้มี World Internet Conference ขึ้นมา ตั้งแต่ปี ค.ศ. 2014 และจัดต่อเนื่องเป็นประจำทุกปี

4.1 แนวทางการรักษาความปลอดภัยทางไซเบอร์ของประเทศสหรัฐอเมริกา

สหรัฐอเมริกามักเป็นที่ครหาในเรื่องความย้อนแย้ง จากการที่สนับสนุนเสรีภาพในการแสดงออกและการไหลเวียนของข้อมูลข่าวสาร แต่ปรากฏเรื่องอื้อฉาวของสำนักงานความมั่นคงแห่งชาติตามมา อย่างไรก็ดี แนวทางการรักษาความปลอดภัยทางไซเบอร์ของสหรัฐอเมริกาก็แตกต่างกับแนวทางของประเทศจีนอย่างชัดเจน

ในสหรัฐอเมริกา การบริหารความมั่นคงคือการผสมผสานกันระหว่างการควบคุมในเชิงสถาบัน ความรับผิดตามกฎหมายจารีตประเพณี (ตัวอย่างเช่น การเพิกเฉย หรือ หลักความไว้วางใจ) และกรอบระหว่างผู้มี

ส่วนได้เสียของเอกชน สามสิ่งเหล่านี้ได้รวมกันผลักดันให้เกิดการพัฒนาเครือข่ายของสหรัฐอเมริกา[167] ในทางการควบคุมผ่านทางสถาบัน สหรัฐอเมริกาจะควบคุมเป็นภาคส่วนไป โดยผ่านกฎหมายที่ใช้บังคับเฉพาะในแต่ละอุตสาหกรรม[168] และมีระเบียบเกี่ยวกับความปลอดภัยซึ่งบังคับใช้ในแต่ละมลรัฐ เนื่องจากว่ามีกฎหมายประเภทเดียวกันที่หลากหลาย จึงทำให้เกิดปัญหาในเรื่องความซับซ้อนและไม่สอดคล้องกันเองของระเบียบต่างๆ

สถาบันมาตรฐานทางเทคโนโลยีแห่งชาติ (The National Institute for Standards and Technology - NIST) ได้รับมอบหมายให้ร่างแนวทางที่บริษัทต่าง ๆ สามารถนำไปใช้เพื่อรับมือกับการโจมตีทางไซเบอร์ได้ และแนวทางว่าบริษัทควรทำอย่างไรเพื่อพัฒนาความพร้อมในการรับมือกับสถานการณ์ดังกล่าว ซึ่งเป็นเกณฑ์หน้าที่ในการเฝ้าระวัง (due diligence) สิ่งที่น่าสนใจสำหรับแนวทางดังกล่าวนี้คือ ใช้ภาษาที่ธุรกิจไซเบอร์สามารถเข้าใจได้เพื่อให้ธุรกิจเหล่านั้นสามารถประเมินสถานการณ์และรู้วิธีตอบโต้[169]

แนวทางดังกล่าวแบ่งออกเป็น 3 ส่วนคือ เนื้อหาของแนวทาง ระดับการใช้บังคับแนวทาง และบทสรุปของแนวทาง[170] ในส่วนเนื้อหาของแนวทางจะระบุถึงขั้นตอนการปฏิบัติเพื่อให้เกิดความปลอดภัยไซเบอร์ พร้อมทั้งตัวอย่างของวิธีการ[171] ซึ่งไม่ได้ระบุรายละเอียดที่เจาะจงหรือมีไว้เพื่อบริหารความเสี่ยงไซเบอร์สำหรับอุตสาหกรรมใดอุตสาหกรรมหนึ่งโดยเฉพาะ และใช้ศัพท์เทคนิคทั่วไปทำให้การติดต่อประสานงานภายในองค์กรเป็นไปอย่างมีประสิทธิภาพมากขึ้น[172] โดยแนวทางปฏิบัติเหล่านี้อยู่ในบทอ้างอิง อันเป็นรายการสุดท้าย โดยเรียงจากบนลงล่างตั้งแต่ กระบวนการทำงาน ประเภทหลัก ประเภทย่อย และสุดท้ายคือบทอ้างอิง[173]

---

[167] Shackelford, Scott, Scott Russell, and Jeffrey Haut. 2015. "Bottoms Up: A Comparison Of Voluntary Cybersecurity Frameworks". Kelley School Of Business Research Paper 16 (2): 217, 223.

[168] Shackelford, Scott, Andrew A. Proia, Brenton Martell, and Amanda Craig. 2014. "Toward A Global Cybersecurity Standard Of Care? Exploring The Implications Of The 2014 NIST Cybersecurity Framework On Shaping Reasonable National And International Cybersecurity Practices". Texas International Law Journal 2015, 321.

[169] Shackelford, Scott, Scott Russell, and Jeffrey Haut. "Bottoms Up: A Comparison Of Voluntary Cybersecurity Frameworks": 221 -223.

[170] เรื่องเดียว,

[171] National Institute of Standards and Technology. 2018. Framework For Improving Critical Infrastructure Cybersecurity Version 1.1: 4-5.

[172] Shackelford, Scott, Scott Russell, and Jeffrey Haut. "Bottoms Up: A Comparison Of Voluntary Cybersecurity Frameworks": 224.

[173] Shackelford, Scott J., Andrew A. Proia, Brenton Martell and Amanda N. Craig. “Toward a Global Cybersecurity Standard of Care? Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices.”: 330-331.

การบังคับใช้แนวทางแบ่งออกเป็น 4 ระดับ ซึ่งแต่ละระดับจะแสดงให้เห็นว่าบริษัทนั้นสามารถบริหารจัดการความเสี่ยงทางไซเบอร์ได้มากน้อยเพียงใด เมื่อพิจารณาจากแนวทางปฏิบัติเหล่านั้น รวมถึงภยันตรายจากไซเบอร์ในยุคปัจจุบัน มาตรฐานความปลอดภัย วัตถุประสงค์และข้อจำกัดขององค์กรธุรกิจ องค์กรธุรกิจควรรู้ได้ว่าพวกเขาควรปฏิบัติตามแนวบังคับระดับใด

ถัดจากหมวดแนวทางปฏิบัติและประเภท จะเป็นหมวดบทสรุปของแนวทาง ซึ่งทำให้องค์กรทราบได้ว่ามาตรการใดที่พวกเขาควรมีก่อนที่จะเผชิญหน้ากับภยันตรายไซเบอร์ประเภทต่าง ๆ โดยเนื้อหาเหล่านี้สกัดมาจากส่วนแรกและส่วนที่สองที่ได้กล่าวมาข้างต้น รวมไปถึงวิธีการประเมินตนเองและสืบหาตัวตนของฝั่งตรงข้าม รวมทั้งวิธีการปฏิบัติเพื่อให้ทราบถึงข้อมูลของผู้โจมตี[174]

แนวทางปฏิบัติของสถาบันมาตรฐานทางเทคโนโลยีแห่งชาตินั้นสามารถนำไปปรับใช้ได้ง่าย และสามารถใช้ได้ทั่วโลกเนื่องจากว่ามาจากแนวทางปฏิบัติที่ได้รับการยอมรับในระดับสากล ด้วยเหตุนี้เอง ต่อไปจึงอาจกลายเป็นระเบียบการรักษาความปลอดภัยไซเบอร์ระดับสากลได้[175] ทว่าแนวทางดังกล่าวจะได้รับการยอมรับหรือไม่ย่อมขึ้นอยู่กับแต่ละองค์กรธุรกิจ และต้องอาศัยระยะเวลาเพื่อให้มาตรฐานดังกล่าวได้รับการพัฒนาในฐานะกฎหมาย[176] และถึงแม้แนวทางดังกล่าว จะได้กลายเป็นกฎหมายแล้ว นักวิชาการยังให้ความเห็นว่า “ยังไม่พอที่จะบังคับใช้ให้สัมฤทธิ์ผลได้” [177]

ในส่วนของการป้องกันระบบโครงสร้างพื้นฐานนั้น ประธานาธิบดีบารัค โอบามา ได้เสนอคำสั่งพิเศษหมายเลข 13,636 เพื่อสนับสนุนให้เอกชนแบ่งปันข้อมูลวิธีการป้องกันระบบโครงสร้างพื้นฐาน และเพื่อจัดตั้งกรอบแนวปฏิบัติ (framework) ของสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (National Institute of Standards and Technology หรือ NIST) ขึ้นมาเพื่อรวบรวมวิธีปฏิบัติต่างๆ ที่มีประสิทธิภาพของเอกชนมาไว้ด้วยกัน โดยมุ่งเน้นไปที่ภยันตรายจากไซเบอร์ที่รุนแรงเท่านั้น ไม่ได้มุ่งเน้นไปที่อันตรายโดยทั่วไปแต่อย่างใด อย่างไรก็ดี ผู้ประกอบการมิได้มีหน้าที่ต้องปฏิบัติตามกรอบแนวปฏิบัติเหล่านั้นดังเช่นประเทศจีน หากแต่อยู่บนพื้นฐานของความสมัครใจ

---

[174] Shackelford, Scott, Scott Russell, and Jeffrey Haut. "Bottoms Up: A Comparison Of Voluntary Cybersecurity Frameworks": 225.

[175] Shackelford, Scott, Andrew A. Proia, Brenton Martell, and Amanda Craig. "Toward A Global Cybersecurity Standard Of Care? Exploring The Implications Of The 2014 NIST Cybersecurity Framework On Shaping Reasonable National And International Cybersecurity Practices": 336-337.

[176] Shackelford, Scott, Scott Russell, and Jeffrey Haut. "Bottoms Up: A Comparison Of Voluntary Cybersecurity Frameworks": 225-226.

[177] Shackelford, Scott. 2016. "Protecting Intellectual Property And Privacy In The Digital Age: The Use Of National Cybersecurity Strategies To Mitigate Cyber Risk". Chapman Law Review, 2016 Forthcoming, 445, 460.

เพื่อรับประกันความมั่นคงปลอดภัยไซเบอร์ การพัฒนาหน่วยงานที่ทำหน้าที่รับประกันคุณภาพและตรวจสอบสินค้าโครงข่ายเป็นสิ่งที่จำเป็น โดยในสหรัฐอเมริกา เมื่อปี ค.ศ. 2015 ฝ่ายบริหารได้ประกาศมาตรฐาน CyberUL เพื่อยกระดับคุณภาพในการรักษาความปลอดภัยของผลิตภัณฑ์ โดยมีที่มาจากการแนวทางมาตรฐานขององค์กรรับรองมาตรฐานสินค้าเอกชน หรือ Underwriters Laboratories ซึ่งเป็นที่รู้จักกันดีว่าเป็นองค์กรที่ให้บริการที่น่าเชื่อถือเกี่ยวกับการตรวจสอบผลิตภัณฑ์และรับรองมาตรฐานของผลิตภัณฑ์นั้น[178]

วิธีการนี้นอกจากจะช่วยให้การตัดสินใจของเจ้าหน้าที่รัฐเป็นไปอย่างสมเหตุสมผล เนื่องจากมีฐานการตัดสินใจมาจากข้อมูลที่เพียงพอแล้ว ยังช่วยบรรเทาความล้มเหลวของตลาดอันมีที่มาจากความเห็นแก่กำไรของเอกชนจากการขาดแรงจูงใจอีกด้วย เมื่อเปรียบเทียบแล้ว ประเทศจีนไม่มีองค์กรเอกชนที่มาทำหน้าที่เป็นตัวกลางดังเช่นสหรัฐอเมริกา ประกอบกับความดื้อรั้นของประเทศจีนที่ต้องการควบคุมอินเทอร์เน็ต กฎหมายความปลอดภัยทางไซเบอร์ของจีนจึงมอบอำนาจในการรับประกันคุณภาพและการตรวจสอบให้แก่หน่วยงานรัฐทั้งหมด

4.2 แนวทางการรักษาความปลอดภัยทางไซเบอร์ของสหภาพยุโรป

จากการศึกษาเบื้องต้นพบว่า สหภาพยุโรปมีจุดเด่นที่น่าสนใจ 2 ประการคือ หนึ่ง มีความพยายามปรับใช้มาตรการต่าง ๆ ของประเทศในสหภาพยุโรปให้เป็นมาตรฐานเดียวกัน และสอง เป็นตัวอย่างของรัฐที่มารวมกลุ่มกันและใช้อำนาจในการออกกฎหมายร่วมกัน[179]

สหภาพยุโรปยังพยายามสร้างความสมดุลระหว่างการไหลเวียนของข้อมูลข่าวสารและการบริหารจัดการด้านความมั่นคง เมื่อเปรียบเทียบกับสหรัฐอเมริกา สหภาพยุโรปมีความพยายามที่จะควบคุมความปลอดภัยไซเบอร์ในทุก ๆ อุตสาหกรรมให้อยู่ภายใต้กฎหมายเดียว กลยุทธ์ความปลอดภัยไซเบอร์ของสหภาพยุโรป ณ ปัจจุบันมีทั้งหมด 5 เป้าหมาย: [180]

(1) สร้างความยืดหยุ่นและคล่องตัวในไซเบอร์สเปซ;

(2) ลดการก่ออาชญากรรมไซเบอร์;

(3) จัดให้มีนโยบายการป้องกันไซเบอร์;

---

[178] Carte, William A., and Daniel G. Sofio. 2017. "Cybersecurity Legislation And Critical Infrastructure Vulnerabilities". Foundations Of Homeland Security, 223-224.

[179] Shackelford, Scott, Scott Russell, and Jeffrey Haut. "Bottoms Up: A Comparison Of Voluntary Cybersecurity Frameworks": 237.

[180] Shackelford, Scott, and Amanda Craig. "Beyond The New “Digital Divide”: Analyzing The Evolving Role Of National Governments In Internet Governance And Enhancing Cyber-Security": 156.

(4) พัฒนาอุตสาหกรรมและเทคโนโลยีที่เกี่ยวข้องกับความปลอดภัยไซเบอร์; และ

(5) สร้างนโยบายไซเบอร์สเปซระหว่างประเทศเพื่อส่งเสริมคุณค่าแห่งสหภาพยุโรป

เพื่อให้เป้าหมายแรกสำเร็จ ทั้งภาครัฐและเอกชนจำต้องร่วมมือกันตอบโจทย์ว่ามาตรฐานขั้นต่ำที่ควรใช้ในการรักษาความปลอดภัยไซเบอร์นั้นควรมีรูปร่างอย่างไร และสำหรับเป้าหมายที่ 2 กรณีนี้มุ่งไปที่การตอบโต้อันตรายที่มาจากบอทเน็ต เครือข่ายของคอมพิวเตอร์ที่ติดโปรแกรมให้สามารถถูกควบคุมได้โดยผู้โจมตี มาตรการป้องกันไซเบอร์ดังกล่าวเป็นผลของความร่วมมือกันระหว่างภาคประชาชนและกองทัพเพื่อร่วมกันปกป้องสินทรัพย์ไซเบอร์ที่สำคัญ ในท้ายที่สุด สหภาพยุโรปก็มีความต้องการที่จะ “ส่งเสริมเสรีภาพบนโลกอินเตอร์เน็ต ทำลายพรมแดนที่กั้นระหว่างกัน และสร้างนโยบายที่ได้รับการยอมรับในระดับสากล” [181]

ปัจจุบัน สหภาพยุโรปได้บังคับใช้นโยบายไซเบอร์ ซึ่งโดยมากยกร่างโดยหน่วยงานปกป้องคุ้มครองข้อมูล (General Data Protection Regulation GDPR) GDPR อนุญาตให้บริษัททำการถ่ายโอนข้อมูลออกไปได้หากปรากฏว่ามีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสมทั้งในฝั่งของผู้โอนและรับข้อมูลนั้น ซึ่งมาตรการนี้แต่เดิมถูกริเริ่มโดยสหรัฐอเมริกา และในภายหลังสหภาพยุโรปจึงได้รับแนวคิดดังกล่าวมาด้วย

4.3 ศึกษาเปรียบเทียบในประเด็นกฎหมายสำคัญ

4.3.1 หน้าที่ตามกฎหมายของผู้ให้บริการทางเครือข่าย

กฎหมายสหรัฐอเมริกา

จากการศึกษา ไม่พบว่าประเทศสหรัฐอเมริกามีกฎหมายเกี่ยวกับประเด็นนี้

กฎหมายสหภาพยุโรป

ในปี ค.ศ. 2016 สหภาพยุโรปได้ออกกฎหมายชื่อ Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union ขึ้น โดยในมาตรา 16 ได้กำหนดให้ประเทศสมาชิกต้องจัดให้ผู้ให้บริการดิจิทัลในประเทศของตนมีมาตรการที่เหมาะสมในการบริหารจัดการความเสี่ยงที่อาจเกิดต่อระบบข้อมูลและเครือข่าย โดยระบบข้อมูลและเครือข่ายที่ว่านี้คือระบบข้อมูลและเครือข่ายในธุรกิจที่เป็นไปตามเอกสารแนบท้ายหมายเลข 3 ของกฎหมายนี้ อันได้แก่ การตลาดออนไลน์ (online marketplace) การให้บริการเครื่องมือค้นหาออนไลน์ (online search engine) และการจัดเก็บข้อมูลออนไลน์ (cloud computing service)

เมื่อปี ค.ศ. 2018 สหราชอาณาจักรได้ออกกฎหมายฉบับแรกที่ให้หน้าที่แก่ผู้บริการทางเครือข่ายเพื่อให้เป็นไปตามกฎหมายของสหภาพยุโรป โดยกฎหมายนั้นคือระเบียบว่าด้วยระบบข้อมูลและเครือข่าย

[181] เรื่องเดียวกัน.

(Network and Information Systems Regulations) ได้ให้นิยามคำว่า ผู้ให้บริการดิจิทัล (digital service provider) ไว้ว่า[182] “บุคคลใดก็ตามที่ให้บริการดิจิทัล” ซึ่งโดยทั่วไปแล้ว ไม่มีหน้าที่ใดโดยเฉพาะเจาะจงตามกฎหมายฉบับนี้ อย่างไรก็ดี หากผู้ให้บริการดิจิทัลนั้นจัดเป็นผู้ให้บริการดิจิทัลที่เกี่ยวข้อง (relevant digital service provider) คือ[183] “เป็นผู้ให้บริการดังกล่าวในสหภาพยุโรปและมีคุณสมบัติทั้งสองข้อพร้อมกันต่อไปนี้ คือ 1. มีบริษัทหลักอยู่ในสหราชอาณาจักร และ 2. เป็นองค์กรธุรกิจที่มิใช่ขนาดกลางหรือขนาดเล็ก” ผู้ให้บริการดิจิทัลที่เกี่ยวข้องจะต้องมีหน้าที่ตามกฎหมายดังต่อไปนี้คือ หากปรากฏว่าผู้ให้บริการดิจิทัลให้บริการใดให้บริการเครื่องมือค้นหาออนไลน์ ตลาดออนไลน์ หรือจัดเก็บข้อมูลออนไลน์ จัดทำมาตรการในการบริหารจัดการความเสี่ยงที่อาจเกิดขึ้นต่อความปลอดภัยของระบบข้อมูลและเครือข่าย โดยมาตรการเช่นว่านั้นต้องเหมาะสม มีประสิทธิภาพในการป้องกันอันตรายที่จะเกิดขึ้นได้จริง ทั้งนี้ให้คำนึงถึงขีดจำกัดความสามารถของเทคโนโลยีในขณะนั้น (state of art) และหากมีภยันตรายเกิดขึ้น ผู้ให้บริการดิจิทัลก็มีหน้าที่ต้องแจ้งให้คณะกรรมการทราบด้วย[184]

เปรียบเทียบกับกฎหมายจีน

สหรัฐอเมริกาไม่ได้มีกฎหมายซึ่งบังคับให้ผู้ให้บริการทางเครือข่ายต้องปฏิบัติการใด ๆ ในขณะที่สหภาพยุโรปเพียงบังคับให้ผู้ให้บริการเครือข่ายที่ให้บริการในธุรกิจเฉพาะ คือ การตลาดออนไลน์ (online marketplace) การให้บริการเครื่องมือค้นหาออนไลน์ (online search engine) และการจัดเก็บข้อมูลและการคำนวณออนไลน์ (cloud computing service) เท่านั้นที่ต้องมีหน้าที่ในการใช้มาตรการที่เหมาะสมเพื่อป้องกันการโจมตีไซเบอร์ ในขณะที่ประเทศจีน นอกจากจะบังคับให้ผู้ให้บริการทางเครือข่ายในธุรกิจทุกประเภทมีหน้าที่ในการจัดสร้างมาตรการเพื่อรับมือกับการโจมตีทางไซเบอร์แล้ว ผู้ให้บริการทางเครือข่ายยังต้องช่วยรัฐบาลเซ็นเซอร์เนื้อหาที่ไม่พึงประสงค์บนอินเทอร์เน็ต พร้อมทั้งให้ความช่วยเหลือทางเทคนิคแก่หน่วยงานรัฐเสมอเมื่อหน่วยงานรัฐร้องขอด้วย

ข้อแตกต่างเหล่านี้ ทำให้เห็นได้ว่า กฎหมายของสหรัฐอเมริกาไม่ได้มอบหน้าที่ใด ๆ แก่ผู้ให้บริการทางเครือข่ายเลย อาจเป็นไปได้ว่ารัฐได้เชื่อในเรื่องระบบทุนนิยมอย่างเต็มที่ จึงพยายามที่จะเข้าไปยุ่งเกี่ยวกับตลาดและผู้ประกอบการให้น้อยที่สุด หากรัฐเข้าไปบังคับให้เอกชนใช้มาตรการตามที่รัฐกำหนดไว้ ก็อาจเป็นการเพิ่มภาระให้แก่ผู้ประกอบการ ทำให้ประชาชนต้องใช้บริการในราคาที่แพงขึ้น ทว่า สำหรับสหภาพยุโรปนั้นอาจนำแนวคิดเรื่องประโยชน์สาธารณะเข้ามาพิจารณาเพื่อถ่วงดุลกับผลประโยชน์ของผู้ประกอบการด้วย โดยสหภาพยุโรป เลือกที่จะไม่มอบภาระให้แก่ผู้ประกอบการคล้ายคลึงกับแนวคิดของสหรัฐอเมริกา แต่ในการประกอบธุรกิจบางประเภท มีความเสี่ยงว่าหากธุรกิจเหล่านั้นไม่ป้องกันตนเองเลย ความเสียหายที่จะเกิดต่อประชาชนนั้นย่อมมากกว่าผลประโยชน์ที่ผู้ประกอบการจะได้รับ ขอให้สังเกตว่าธุรกิจ การตลาดออนไลน์

[182] ส่วนที่ 1 (1) Network and Information Systems Regulations

[183] ส่วนที่ 1 (3)(e) Network and Information Systems Regulations

[184] ส่วนที่ 4 Network and Information Systems Regulations

(online marketplace) การให้บริการเครื่องมือค้นหาออนไลน์ (online search engine) และการจัดเก็บข้อมูลออนไลน์ (cloud computing service) ล้วนเป็นธุรกิจที่เข้าถึงประชาชนได้โดยง่ายทั้งสิ้น โดยมีผลต่อความรับรู้ พฤติกรรมการบริโภค รวมไปถึงข้อมูลส่วนตัวของประชาชน ซึ่งเป็นสิ่งที่สุ่มเสี่ยงต่อการถูกโจมตีทางไซเบอร์ได้ง่าย ไม่ว่าจะเป็นการเจาะระบบเครื่องมือค้นหาออนไลน์เพื่อปล่อยข่าวเท็จ การเจาะระบบการตลาดออนไลน์เพื่อขายสินค้าที่ผิดกฎหมาย หรือการเจาะฐานข้อมูลออนไลน์เพื่อโจรกรรมข้อมูลส่วนตัว ด้วยเหตุนี้สหภาพยุโรปจึงต้องมีกฎหมายเพื่อให้ผู้ให้บริการทางเครือข่ายให้ความคุ้มครองธุรกิจของตนเองอย่างเหมาะสม

การออกกฎหมายของสหรัฐอเมริกาและสหภาพยุโรปคือการถ่วงดุลน้ำหนักระหว่างผลประโยชน์ของผู้ประกอบการกับประชาชน อย่างไรก็ดี สำหรับประเทศจีนนั้นจะแตกต่างไป กล่าวคือ การออกกฎหมายของประเทศจีนมีแนวโน้มว่าจะเป็นการถ่วงดุลน้ำหนักระหว่างความมั่นคงของรัฐกับผลประโยชน์ของประชาชนเสียมากกว่า เนื่องจากการที่ประเทศจีนบังคับให้ผู้ให้บริการทางเครือข่ายในทุกธุรกิจต้องมีมาตรการที่เหมาะสมเพื่อป้องกันการโจมตีทางไซเบอร์ก็คือการเพิ่มต้นทุนให้กับผู้ประกอบการโดยไม่จำเป็น เพราะ ธุรกิจหลายประเภทก็ไม่ได้มีโอกาสตกเป็นเป้าหมายในการโจมตีไซเบอร์เท่าใดนัก ในท้ายที่สุดแล้ว ประชาชนก็อาจต้องเผชิญกับค่าใช้จ่ายที่เพิ่มขึ้นอันมีเหตุเนื่องจากต้นทุนในการประกอบกิจการที่สูงอันเนื่องมาจากการจัดให้มีมาตรการรักษาความปลอดภัยดังกล่าว นอกจากนี้ ยังมีประเด็นว่า กฎหมายฉบับนี้เป็นการที่ประเทศจีนผลักภาระของรัฐมาให้แก่เอกชน โดยรัฐไม่ใส่ใจที่จะดูแลความปลอดภัยไซเบอร์ด้วยตนเอง แต่ในขณะเดียวกันก็ยอมไม่ได้ที่จะเห็นบุคคลวิพากษ์วิจารณ์รัฐบาลอย่างไม่เหมาะสม ในท้ายที่สุดจึงกลายเป็นเอกชนต้องจ้างพนักงานมาเพื่อนั่งเฝ้าเครือข่ายของตัวเองเพื่อช่วยเซ็นเซอร์เนื้อหาที่ไม่พึงประสงค์ให้แก่รัฐบาลจีน และสุดท้ายคือประเด็นว่า การที่รัฐบาลจีนออกกฎหมายบังคับให้ผู้ให้บริการทางเครือข่ายมาให้ความช่วยเหลือแก่หน่วยงานรัฐเสมอเมื่อได้รับการร้องขอนั้น เป็นมาตรการเพื่อลดค่าใช้จ่ายของตนในการ จ้างพนักงานรัฐมาจัดการปัญหาทางเทคนิคเหล่านั้นด้วยตนเอง และหากการกระทำนั้นไม่ชอบด้วยกฎหมาย เช่น ขอให้ผู้ให้บริการทางเครือข่ายช่วยเจาะระบบ เพื่อให้ได้มาซึ่งข้อมูลส่วนบุคคลของผู้อื่นโดยไม่มีเหตุจำเป็น เจ้าหน้าที่รัฐอาจออกจากปัญหานี้ได้อย่างง่ายดาย ปล่อยให้ผู้ให้บริการทางเครือข่ายระงับข้อพิพาทกับตัวเจ้าของข้อมูลเองเพียงลำพัง

4.3.2 การปกป้องระบบโครงสร้างพื้นฐานสำคัญ

กฎหมายสหรัฐอเมริกา

กระทรวงความมั่นคงแห่งมาตุภูมิ (Department of Homeland Security) ได้ให้นิยามความหมายของคำว่าระบบโครงสร้างพื้นฐานสำคัญไว้ว่า[185] “เป็นสินทรัพย์หรือระบบ ไม่ว่าจะปรากฏในรูปกายภาพหรือในพื้นที่ไซเบอร์ อันมีความสำคัญอย่างยิ่งต่อประเทศชาติ โดยหากสินทรัพย์หรือระบบดังกล่าวหยุดทำงานหรือถูกทำลาย ประเทศชาติ เศรษฐกิจ สังคมหรือสุขอนามัยของคนในชาติจะได้รับความเสียหายอย่างยิ่ง”

เมื่อปี ค.ศ. 2018 ประธานาธิบดีโดนัลด์ ทรัมป์ ได้ลงนามในกฎหมายชื่อว่า รัฐบัญญัติองค์การความมั่นคงปลอดภัยไซเบอร์และระบบโครงสร้างพื้นฐานสำคัญ (Cybersecurity and Infrastructure Security Agency Act) โดยกฎหมายฉบับนี้ได้จัดตั้งองค์การความมั่นคงปลอดภัยไซเบอร์และระบบโครงสร้างพื้นฐานสำคัญขึ้นมา โดยให้อยู่ในสังกัดของกระทรวงความมั่นคงแห่งมาตุภูมิ[186] และมีหน่วยงานภายในแยกย่อยซึ่งมีหน้าที่ดูแลเกี่ยวกับระบบโครงสร้างพื้นฐานสำคัญไว้โดยเฉพาะ คือ หน่วยงานความมั่นคงปลอดภัยของโครงสร้างพื้นฐาน (Infrastructure Security Division)

หน่วยงานความมั่นคงปลอดภัยของโครงสร้างพื้นฐานมีหน้าที่ในการเป็นตัวกลางประสานงานและให้ความร่วมมือกับทั้งภาครัฐและเอกชน เพื่อช่วยให้ระบบโครงสร้างพื้นฐานสำคัญปลอดภัยจากการถูกโจมตี พร้อมทั้งช่วยเสริมสร้างความรู้ความเข้าใจเกี่ยวกับความเสี่ยงและอันตรายที่อาจเกิดขึ้นต่อระบบโครงสร้างพื้นฐานนั้น รวมไปถึงการแบ่งปันข้อมูลต่าง ๆ ที่อาจเป็นประโยชน์ต่อการปกป้องระบบโครงสร้างพื้นฐานให้แก่กัน โดยไม่ว่าระบบโครงสร้างพื้นฐานนั้นจะอยู่ในรูปแบบทางกายภาพหรือในพื้นที่ไซเบอร์ก็ตาม [187]

สำหรับระบบโครงสร้างพื้นฐานสำคัญนั้น เป็นรูปแบบระบบโครงสร้างพื้นฐานที่เสี่ยงต่อการถูกโจมตีมากกว่าระบบโครงสร้างพื้นฐานธรรมดา ด้วยเหตุนี้ หน่วยงานความมั่นคงปลอดภัยของโครงสร้างพื้นฐานจึงได้ทำการระบุให้ชัดเจนว่าสิ่งใดบ้างเป็นระบบโครงสร้างพื้นฐานสำคัญ โดยแต่ละประเภทต่างมีแผนการจัดการเฉพาะ (Sector-Specific Plan) ซึ่งอาจแบ่งออกได้เป็น 16 ประเภทดังต่อไปนี้คือ:[188]

1. ภาควิทยาศาสตร์การเคมี

---

[185] Department Of Homeland Security. 2020. "Critical Infrastructure Security". Cisa.Gov. https://www.dhs.gov/topic/critical-infrastructure-security.

[186] Department Of Homeland Security. 2020. "ABOUT CISA". Cisa.Gov. https://www.cisa.gov/about-cisa.

[187] Department Of Homeland Security. 2020. "Infrastructure Security Division | CISA". Cisa.Gov. https://www.cisa.gov/infrastructure-security-division.

[188] Department Of Homeland Security. 2020. "Critical Infrastructure Sectors". Cisa.Gov. https://www.cisa.gov/critical-infrastructure-sectors.

2. ภาคหน่วยงานเชิงพาณิชย์
3. ภาคการโทรคมนาคม
4. ภาคอุตสาหกรรมการผลิตสำคัญ
5. ภาคการบริหารจัดการน้ำ
6. ภาคอุตสาหกรรมป้องกันประเทศ
7. ภาคการให้บริการฉุกเฉิน
8. ภาคอุตสาหกรรมพลังงาน
9. ภาคการให้บริการทางการเงิน
10. ภาคอาหารและการเกษตร
11. ภาคหน่วยงานรัฐ
12. ภาคสาธารณสุข
13. ภาคเทคโนโลยีและการสื่อสาร
14. ภาคอุตสาหกรรมนิวเคลียร์
15. ภาคการคมนาคม
16. ภาคการบริหารจัดการเขื่อน

หากพิจารณาแผนการจัดการเฉพาะของแต่ละภาคจะพบว่าทุกแผนการจัดการจะมีบทของเนื้อหาที่กล่าวถึงความมั่นคงปลอดภัยไซเบอร์ไว้เป็นการเฉพาะ ว่าอุตสาหกรรมนั้นควรใช้เทคโนโลยีใด หรือวางระบบเช่นไร โดยมีเป้าหมายเดียวกันคือเพื่อป้องกันการถูกรุกรานจากภายนอก อย่างไรก็ดี ทั้งในรัฐบัญญัติองค์การความมั่นคงปลอดภัยไซเบอร์และระบบโครงสร้างพื้นฐานสำคัญ และในแผนการจัดการเฉพาะล้วนต่างไม่ได้กล่าวถึงบทลงโทษหากไม่มีการปฏิบัติตาม จึงอาจสรุปได้ว่าทั้งหน่วยงานภาครัฐและเอกชนที่มีภารกิจหรือกิจการเกี่ยวข้องกับระบบโครงสร้างพื้นฐานสำคัญ อาจไม่ต้องทำตามมาตรการเหล่านั้นก็ได้ และการจะป้องกันหรือไม่นั้น ขึ้นอยู่กับความสมัครใจของหน่วยงานรัฐหรือเอกชนเอง

กฎหมายสหภาพยุโรป

จาก COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve

their protection ระบบโครงสร้างพื้นฐานสำคัญ (critical infrastructure) หมายถึง[189] “สินทรัพย์ ระบบหรือส่วนใดของสิ่งดังกล่าวในข้างต้น ซึ่งตั้งอยู่ในอาณาเขตของประเทศสมาชิก และมีส่วนสำคัญต่อความเป็นอยู่ของสังคม สุขอนามัย ความปลอดภัย ความมั่นคง เศรษฐกิจ หรือความเป็นอยู่ของประชาชน และการทำลายหรือการรบกวนซึ่งสิ่งนั้นอาจก่อให้เกิดผลกระทบรุนแรงต่อประเทศสมาชิก” และกฎหมายฉบับนี้มีเนื้อหาโดยรวมคือการให้ประเทศสมาชิกร่วมกันปกป้องระบบโครงสร้างพื้นฐานสำคัญเหล่านั้น หากปรากฏว่าการรบกวนหรือทำลายระบบโครงสร้างพื้นฐานสำคัญนั้นกระทบต่อผลประโยชน์ของประเทศสมาชิกตั้งแต่ 2 ประเทศเป็นต้นไป แต่ทั้งนี้ ไม่ได้กล่าวถึงการบังคับให้ประเทศสมาชิกปกป้องระบบโครงสร้างพื้นฐานสำคัญที่อยู่แต่เฉพาะในประเทศตนเองเท่านั้นแต่อย่างใด

จนกระทั่งในปี ค.ศ. 2013 สหภาพยุโรปได้ออกกฎหมายอีกหนึ่งฉบับที่เกี่ยวกับการปกป้องระบบโครงสร้างพื้นฐานคือ Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 โดยกฎหมายนี้ได้จัดตั้งองค์กรเพื่อความมั่นคงของของเครือข่ายและข้อมูลข่าวสารแห่งสหภาพยุโรปขึ้น (European Union Agency for Network and Information Security) และภายหลังได้เปลี่ยนชื่อเป็นองค์กรเพื่อความมั่นคงปลอดภัยไซเบอร์ (European Union Agency for Cybersecurity) เพื่อสร้างความตระหนักรู้ในเรื่องความมั่นคงของเครือข่ายและข้อมูล อันอาจเป็นประโยชน์ต่อประชาชน ผู้บริโภค องค์กรธุรกิจ และหน่วยงานภาครัฐของประเทศสมาชิกเอง[190] โดยไม่ต้องพิจารณาอีกว่าการรบกวนหรือทำลายระบบโครงสร้างพื้นฐานนั้นจะกระทบต่อประเทศสมาชิกอื่นหรือไม่

ในบทนำของกฎหมายฉบับนี้เน้นให้เห็นถึงความสำคัญว่า ความมั่นคงของข้อมูลข่าวสารและบริการที่เกี่ยวข้องมีความสำคัญเช่นเดียวกันกับระบบโครงสร้างพื้นฐานสำคัญอื่น อาทิ ระบบการบริหารจัดการน้ำ หรือการจัดการไฟฟ้า และหากข้อมูลข่าวสารและบริการที่เกี่ยวข้องถูกรบกวน ผลเสียจะเกิดขึ้นแก่เศรษฐกิจและสังคม ด้วยเหตุเช่นนี้ จึงเป็นที่มาของการจัดตั้งองค์กรดังกล่าวขึ้น และให้มีหน้าที่ในการให้คำแนะนำแก่ประเทศสมาชิกเพื่อยกระดับมาตรฐานความปลอดภัยของระบบโครงสร้างพื้นฐานสำคัญ

เมื่อปี ค.ศ. 2019 สหภาพยุโรปได้ออกกฎหมายฉบับใหม่ขึ้น คือ REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology

---

[189] มาตรา 2 (a) COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection

[190] มาตรา 1 Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004

cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) เพื่อเพิ่มบทบาทหน้าที่ขององค์กรนี้ในด้านของการรับรองมาตรฐานความปลอดภัยและการตรวจสอบคุณภาพอุปกรณ์ แต่ทั้งนี้ ในด้านการปกป้องระบบโครงสร้างพื้นฐานสำคัญนั้น องค์กรนี้ยังคงมีหน้าที่เพียงให้คำแนะนำต่าง ๆ แก่ประเทศสมาชิกหรือหน่วยงานเอกชนเท่านั้น เพื่อให้ประเทศสมาชิกนำไปออกกฎหมายภายในของประเทศตนต่อไป หรือเพื่อให้เอกชนรับมาตรการเหล่านั้นไปปฏิบัติเองตามสมควร

เปรียบเทียบกับกฎหมายจีน

ระบบโครงสร้างพื้นฐานสำคัญ คือสินทรัพย์หรือเครือข่าย ซึ่งหากถูกรบกวนหรือทำลาย จะส่งผลร้ายต่อสังคมในวงกว้าง อย่างไรก็ดี แม้ว่าผลกระทบจากการที่ระบบโครงสร้างพื้นฐานสำคัญถูกรบกวนหรือทำลายจะรุนแรงเพียงใด สหรัฐอเมริกาและสหภาพยุโรปยังคงเห็นพ้องต้องกันว่ามาตรการในการปกป้องระบบโครงสร้างพื้นฐานสำคัญไม่จำเป็นต้องออกเป็นกฎหมายซึ่งมีสภาพบังคับ ในขณะที่ประเทศจีนกำหนดให้ผู้ให้บริการระบบโครงสร้างพื้นฐานสำคัญมีหน้าที่ในการตรวจสอบประวัติบุคคลที่เข้ามาร่วมงานด้วย รวมไปถึงการจัดให้มีการอบรมเรื่องความปลอดภัยไซเบอร์ และทำสำเนาข้อมูลเผื่อไว้ในกรณีที่เกิดเหตุร้าย และตรวจสอบความปลอดภัยของระบบประจำปี

จากข้อแตกต่างนี้ จะเห็นได้ว่ามุมมองในฐานะรัฐของสหรัฐอเมริกา และสหภาพยุโรป กับประเทศจีนที่มีต่อระบบโครงสร้างพื้นฐานสำคัญมีความแตกต่างกันอย่างสิ้นเชิง โดยในกรณีที่ระบบโครงสร้างพื้นฐานสำคัญในสหรัฐอเมริกา และสหภาพยุโรปถูกโจมตี ไม่ว่าจะเป็นโรงไฟฟ้า เหมืองแร่ การขนส่ง หากความวุ่นวายเกิดขึ้นจากการหยุดชะงักของการให้บริการ ผู้ที่ถูกวิพากษ์วิจารณ์อาจไม่ใช่รัฐเสมอไป แต่อาจเป็นเอกชนก็ได้ เพราะระบบโครงสร้างพื้นฐานหลายแห่งก็เป็นของเอกชนเอง และอีกเหตุผลหนึ่งคือแนวคิดว่าด้วยปัจเจกชนนิยม ซึ่งเชื่อมั่นในศักยภาพของมนุษย์แต่ละคน แม้ระบบโครงสร้างพื้นฐานที่เป็นที่พึ่งของสาธารณชนจะถูกทำลาย ก็ไม่ทำให้ประชาชนรู้สึกขาดความเชื่อมั่นในตัวรัฐเท่าใดนัก ด้วยเหตุนี้ ระเบียบสังคมของรัฐจึงไม่เสียไป ทว่า ในทางตรงกันข้าม รัฐบาลจีนเป็นเจ้าของระบบโครงสร้างพื้นฐานสำคัญเกือบทั้งหมดภายในประเทศ หากระบบโครงสร้างพื้นฐานสำคัญเสียไป ผู้ที่ตกเป็นเป้าหมายในการวิพากษ์วิจารณ์ก็คือตัวรัฐเอง นอกจากนี้ ด้วยแนวคิดของจีนที่ปลูกฝังให้เชื่อในอำนาจของผู้ปกครองและเห็นแก่ภาพรวมของสังคม หากระบบโครงสร้างพื้นฐานสำคัญถูกทำลาย ภาพรวมที่ประชาชนจีนจะได้เห็นก็คือความเดือดร้อนของบุคคลอื่น และส่งผลเสียต่อความเชื่อมั่นของประชาชนที่มีต่อผู้ปกครองเองในที่สุด ดังนั้นแล้ว สำหรับประเทศจีน ระบบโครงสร้างพื้นฐานสำคัญก็คือปัจจัยหนึ่งที่ทำให้รัฐและผู้ปกครองนั้นอยู่รอดได้

อย่างไรก็ดี การที่รัฐบาลจีนมองว่าระบบโครงสร้างพื้นฐานสำคัญเป็นสิ่งที่สำคัญยิ่งยวดเสมอเทียบเท่าความมั่นคงของประเทศ ทำให้เกิดปัญหาสองประการ ประการแรกคือความยุ่งยากและ ความไม่จำเป็นในเนื้อหาของกฎหมาย ไม่ว่าจะเป็นการตรวจประวัติพนักงานที่เข้ามาทำงานในตำแหน่งสำคัญ หรือการทำสำเนาข้อมูลเผื่อไว้ในกรณีเกิดเหตุร้าย ทั้งที่จริงแล้ว ประวัติอาชญากรรมที่พนักงานผู้นั้นเคยก่ออาจไม่สัมพันธ์กับคุณสมบัติหน้าที่ที่พึงมีในตำแหน่งงานเลยแม้แต่น้อย หรือแม้แต่การทำสำเนาข้อมูลเผื่อไว้นั้น ก็อาจเป็นการ

สิ้นเปลืองโดยใช่เหตุ ประการถัดมาคือปัญหาในเรื่องความซ้ำซ้อนของกฎหมาย ในเมื่อการโจมตีไซเบอร์จัดเป็นอาชญากรรมคอมพิวเตอร์ตามกฎหมายของประเทศจีน กล่าวคือรัฐมีเครื่องมือในการปรามอาชญากรไม่ให้กระทำความผิดอยู่แล้ว เหตุใดถึงต้องมอบภาระหน้าที่ให้กับผู้ดูแลระบบโดยไม่จำเป็นอีก

นอกจากข้อแตกต่างในประเด็นเรื่องสภาพบังคับของการปกป้องระบบโครงสร้างพื้นฐานสำคัญ มีข้อสังเกตเพิ่มเติมคือ การปกป้องระบบโครงสร้างพื้นฐานสำคัญของสหรัฐอเมริกามีลักษณะแยกเป็นแต่ละประเภทไปโดยเฉพาะ และในแต่ละประเภทย่อยจะกล่าวถึงการดูแลข้อมูลและระบบของระบบโครงสร้างพื้นฐานสำคัญอีกทีหนึ่ง ในขณะที่สหภาพยุโรปและประเทศจีนจะเริ่มต้นด้วยประเด็นการดูแลข้อมูลและระบบของระบบโครงสร้างพื้นฐานสำคัญในฐานะข้อมูลและระบบทั้งหมด แล้วให้ปรับใช้กับธุรกิจที่เข้าข่ายเป็นการทั่วไป

4.3.3 การเก็บรวบรวมข้อมูลไว้ภายในท้องที่

กฎหมายสหรัฐอเมริกา

เดิมที สหรัฐอเมริกาไม่เคยมีกฎหมายใดบังคับเกี่ยวกับการเก็บรวบรวมข้อมูลไว้ภายในท้องที่มาก่อน จนกระทั่งในปี ค.ศ. 2019 สมาชิกวุฒิสภาจอร์ช ฮอว์ลีย์ (Josh Hawley) ได้เสนอร่างกฎหมายฉบับหนึ่งขึ้นคือ รัฐบัญญัติความมั่นคงของชาติและการคุ้มครองข้อมูลส่วนบุคคล (National Security and Personal Data Protection Act) ขึ้น[191] การเสนอร่างกฎหมายดังกล่าวคาดว่ามีวัตถุประสงค์เพื่อป้องกันเหตุการณ์ที่ผู้พัฒนาแอพพลิเคชั่นของประเทศจีนที่ทำการเก็บข้อมูลประชาชนในประเทศสหรัฐอเมริกากลับไปที่ประเทศจีนได้อย่างง่ายดายเกินไป อันเป็นผลให้ประเทศจีนมีความได้เปรียบในเชิงเศรษฐกิจมากเกินสมควร[192] โดยกฎหมายฉบับนี้จะบังคับให้บริษัทต่าง ๆ ในสหรัฐอเมริกาต้องไม่ถ่ายโอนข้อมูลของพลเมืองอเมริกาที่เก็บได้ในประเทศไปเก็บไว้ที่ประเทศอื่นที่มีความน่ากังวล อันอาจกล่าวได้ว่า “เสรีในการไหลเวียนของข้อมูลข่าวสารเป็นหลักแต่การเก็บรวบรวมข้อมูลไว้ภายในท้องที่คือข้อยกเว้น”

รัฐบัญญัติความมั่นคงของชาติและการคุ้มครองข้อมูลส่วนบุคคลมีความน่าสนใจคือมาตรการเก็บรวบรวมข้อมูลไว้ภายในท้องที่นี้ไม่ได้บังคับครอบคลุมทุกบริษัท หากแต่ต้องพิจารณาว่าการโอนข้อมูลไปเก็บไว้ที่ประเทศที่หมายนั้นจัดเป็น “ประเทศที่มีความน่ากังวล” (Countries of Concern) หรือไม่ โดยประเทศเหล่านั้นได้แก่ ประเทศจีน ประเทศรัสเซีย และประเทศอื่นตามที่รัฐมนตรีว่าการกระทรวงการต่างประเทศ

---

[191] Fisher, Christine. 2019. "Senate Bill Would Block US Companies From Storing Data In China". Engadget.Com. https://www.engadget.com/2019-11-18-national-security-personal-data-protection-act.html.

[192] Davies, Jamie. 2019. "US Government To Consider Strict Data Localisation Laws". Telecoms. https://telecoms.com/500992/us-government-to-consider-strict-data-localisation-laws/.

เห็นสมควร[193] ซึ่งหากปรากฏว่าการโอนข้อมูลนั้นจะโอนไปเก็บไว้ในประเทศที่มีความน่ากังวล กฎหมายฉบับนี้จะห้ามไม่ให้บริษัทนั้นทำการโอนไป

อย่างไรก็ดี ความในข้างต้นนั้นอาจไม่ใช้บังคับกับบริษัทเทคโนโลยีอันอยู่ในข่าย (Covered technology company) อันหมายถึงบริษัทที่มีการให้บริการออนไลน์เป็นหลัก[194] อาทิ Facebook Twitter หรือ Instagram เนื่องจากว่าธุรกิจประเภทนี้เป็นธุรกิจที่ผู้ใช้มักนำข้อมูลของตนเข้าไปอย่างเป็นกิจวัตรอยู่แล้ว ทำให้ข้อมูลที่บริษัทนี้รวบรวมได้ มีปริมาณมหาศาลและมีความส่วนตัวสูง ต่างกับบริษัทอื่นที่เก็บข้อมูลได้อย่างจำกัด ดังนั้นผู้ประกอบกิจการนี้จึงต้องปฏิบัติตามมาตรการที่เคร่งครัดขึ้นกว่าบริษัททั่วไป โดยการห้ามโอนข้อมูลที่เก็บได้มานั้นไปเก็บไว้ที่ประเทศใด ๆ โดยไม่พิจารณาว่าประเทศนั้นจัดเป็นประเทศที่มีความน่ากังวลหรือไม่ก็ตาม เว้นเสียแต่ว่าประเทศนั้นจะมีข้อตกลงร่วมกันกับสหรัฐอเมริกาโดยเฉพาะเจาะจง[195] ทั้งนี้ การฝ่าฝืนกฎหมายฉบับนี้มีโทษจำคุกสูงสุด 5 ปี[196]

อนึ่ง มีข้อสังเกตคือทั้งประเทศจีนและรัสเซียต่างได้ขึ้นชื่อว่าเป็นประเทศคู่แข่งกับสหรัฐอเมริกามาอย่างช้านาน การที่กฎหมายฉบับนี้ได้ถูกเสนอขึ้นโดยมีจุดมุ่งหมายเป็นการเฉพาะต่อประเทศทั้งสองนี้โดยชัดแจ้ง อาจพิจารณาได้ว่า มูลเหตุของการคุ้มครองข้อมูลส่วนบุคคลเกิดขึ้นเพื่อปิดจุดอ่อนทางเศรษฐกิจ มากกว่าจะเป็นไปเพื่อประโยชน์ของปัจเจกชนโดยแท้จริง แต่หากพิจารณาอีกด้านหนึ่ง การที่จะบังคับให้ทุกบริษัทต้องทำการการเก็บรวบรวมข้อมูลไว้ภายในท้องที่โดยไม่คำนึงว่าจะโอนไปเก็บไว้ในประเทศใดนั้น อาจเป็นการก่ออุปสรรคต่อการไหลเวียนของข้อมูลข่าวสาร และขัดขวางการดำเนินนโยบายเศรษฐกิจแบบเสรีนิยมอันว่าด้วยการรับรู้ข้อมูลของตลาดของผู้ประกอบการก็เป็นได้ ด้วยเหตุนี้ ผู้ร่างกฎหมายจึงเสนอชื่อประเทศเพียง 2 ประเทศที่ต้องเฝ้าระวัง และให้การโอนข้อมูลไปยังประเทศอื่นทำได้โดยปกติ

อย่างไรก็ดี แม้เจตนาของผู้ร่างกฎหมายจะประสงค์ให้ข้อมูลพลเมืองไม่ตกไปอยู่ในมือของชาติคู่แข่งก็ตาม แต่ในทางปฏิบัติก็ยังมีแนวโน้มที่จะหลบหลีกกฎหมายดังกล่าวได้อยู่ ยกตัวอย่างเช่น การตั้งบริษัทลูกในประเทศอื่นนอกจากในประเทศจีนและในรัสเซีย จากนั้นก็ให้บริษัทนั้นเข้าไปประกอบกิจการในสหรัฐอเมริกาและเก็บรวบรวมข้อมูลแทนบริษัทแม่ หลังจากนั้นจึงให้บริษัทลูกนั้นส่งข้อมูลให้กับบริษัทแม่ที่อยู่ในจีนหรือรัสเซียอีกทีหนึ่ง อย่างไรก็ดี ปัจจุบัน กฎหมายฉบับนี้ยังอยู่ในระหว่างการพิจารณาของสมาชิกวุฒิสภา จึงมีแนวโน้มว่ากฎหมายอาจมีการเปลี่ยนแปลงให้เหมาะสมได้ในอนาคต

กฎหมายสหภาพยุโรป

เดิมที สหภาพยุโรปมองว่าการบังคับให้ผู้ประกอบการทำการเก็บรวบรวมข้อมูลไว้ในท้องที่คือการกีดกันทางการค้าอย่างหนึ่ง เนื่องจากว่าเป็นการเพิ่มต้นทุนให้แก่ผู้ประกอบการและขัดขวางเสรีภาพในการ

---

[193] มาตรา 2(2)(A) National Security and Personal Data Protection Act

[194] มาตรา 2(3) National Security and Personal Data Protection Act

[195] มาตรา 3(a)(5) National Security and Personal Data Protection Act

[196] มาตรา 5(b) National Security and Personal Data Protection Act

โอนย้ายข้อมูลข่าวสารระหว่างประเทศสมาชิกด้วยกันเอง อันจะก่อให้เกิดผลกระทบต่อตลาดโดยตรง นอกจากนี้ มาตรการนี้ยังท้าทายปรัชญาพื้นฐานว่าด้วยการรวมตัวกันของประเทศสมาชิกในสหภาพยุโรป เนื่องจากเป็นการสร้างกำแพงข้อมูลข่าวสารระหว่างประเทศขึ้น อย่างไรก็ดี ในยุคแห่งการแข่งขันด้วยข้อมูล หากไม่มีมาตรการการเก็บรวบรวมข้อมูลไว้ภายในท้องที่เกิดขึ้น ข้อมูลของประชาชนในประเทศสมาชิกก็อาจไม่ได้รับความปลอดภัยและถูกนำไปใช้โดยเจ้าของข้อมูลไม่ยินยอมได้ ดังนี้ การออกกฎหมายว่าด้วยการเก็บรวบรวมข้อมูลไว้ภายในท้องที่จึงถูกนำมาพิจารณาอีกครั้ง โดยคงหลักการเดิมว่าประเทศสมาชิกสหภาพยุโรปด้วยกันยังคงสามารถเคลื่อนย้ายข้อมูลไปมาหากันได้อย่างเสรี ในขณะเดียวกัน การเคลื่อนย้ายข้อมูลไปยังประเทศอื่นที่ไม่ใช่ประเทศสมาชิกก็จะมีข้อจำกัดบางประการ เพื่อรับรองสิทธิส่วนตัวของคนในประเทศสมาชิก

กฎหมายสำคัญที่เกี่ยวข้องกับการเก็บรวบรวมข้อมูลไว้ภายในท้องที่ได้แก่ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC หรือ General Data Protection Regulation โดยเป้าหมายของกฎหมายนี้คือการคุ้มครองข้อมูลส่วนบุคคล ซึ่งหมายถึง “ข้อมูลใด ๆ ก็ตามที่สามารถทำให้ทราบถึงบุคคลใดได้โดยเฉพาะเจาะจง ไม่ว่าจะโดยตรงหรือโดยอ้อม เช่น ชื่อ หมายเลขบัตรประจำตัวประชาชน ข้อมูลสถานที่ ตัวตนบนโลกออนไลน์ ตลอดจนรูปลักษณ์ทางกายภาพ อุปนิสัย ภาวะทางจิต อารมณ์ สถานะทางเศรษฐกิจ วัฒนธรรม หรือสภาพทางสังคมของบุคคลนั้น”[197]

กฎหมายฉบับนี้ ไม่ได้ห้ามการโอนย้ายข้อมูลระหว่างประเทศสมาชิกด้วยกัน ทว่าหากการโอนย้ายข้อมูลนั้นจะโอนไปยังประเทศอื่นที่ไม่ใช่ประเทศสมาชิก ผู้ครอบครองข้อมูลจะทำการโอนข้อมูลนั้นไปได้ก็ต่อเมื่อประเทศที่หมายที่ข้อมูลนั้นโอนไปได้มีมาตรการและการบังคับใช้กฎหมายที่เหมาะสมเพื่อบริหารจัดการข้อมูลนั้น ๆ เมื่อมีความรับผิดเกิดขึ้น[198]

เปรียบเทียบกับกฎหมายจีน

การเก็บรวบรวมข้อมูลไว้ภายในท้องที่ ตรงข้ามกับ การปล่อยข้อมูลไหลเวียนเสรี โดยสำหรับสหภาพยุโรปนั้น ระหว่างประเทศสมาชิกด้วยกันเองจะใช้หลักปล่อยข้อมูลไหลเวียนเสรี ทว่า ระหว่างประเทศสมาชิกกับประเทศนอกสมาชิก กฎหมายจะไม่อนุญาตให้ข้อมูลนั้นถูกโอนไปเก็บไว้ยังประเทศปลายทาง เว้นแต่ว่าประเทศนั้นจะมีมาตรการทางกฎหมายที่เพียงพอในการจัดการกับข้อมูลส่วนบุคคล ในขณะที่ประเทศจีน การเก็บรวบรวมข้อมูลไว้ภายในท้องที่ถือเป็นหลักสำคัญของกฎหมายประเทศจีน โดยการโอนข้อมูลไปเก็บยังต่างประเทศจะต้องได้รับอนุญาตจากผู้มีอำนาจก่อนเสมอ และสำหรับสหรัฐอเมริกา โดยอ้างอิงจากร่างกฎหมายซึ่งปัจจุบันยังอยู่ในกระบวนการพิจารณาของวุฒิสภานั้น การโอนข้อมูลไปเก็บไว้ยังที่ใดนั้น ให้

[197] มาตรา 4 (1) General Data Protection Regulation

[198] มาตรา 46 General Data Protection Regulation

พิจารณาว่าผู้โอนข้อมูลไปนั้นเป็นบริษัทประเภทใด หากเป็นบริษัทที่มีส่วนเกี่ยวข้องกับการให้บริการข้อมูลทางอินเทอร์เน็ต การโอนข้อมูลไปเก็บไว้ประเทศอื่นจะทำไม่ได้ กล่าวคือต้องเก็บข้อมูลนั้นไว้ในสหรัฐอเมริกาเท่านั้น เว้นแต่ว่าประเทศที่จะโอนข้อมูลไปนั้นได้มีความตกลงร่วมกันกับสหรัฐอเมริกาแล้ว อีกกรณีหนึ่งคือบริษัทเทคโนโลยีทั่วไปที่ไม่เข้าข่ายบริษัทข้างต้น การโอนข้อมูลสามารถทำได้เสมอ เว้นแต่เป็นการโอนไปเก็บไว้ยังประเทศรัสเซีย จีน หรือประเทศอื่นที่รัฐมนตรีว่าการกระทรวงการต่างประเทศเห็นสมควร

ข้อแตกต่างเหล่านี้แสดงให้เห็นถึงแนวคิดตั้งต้นในการร่างกฎหมายของแต่ละชาติ สำหรับสหภาพยุโรป ประเด็นเรื่องการคุ้มครองสิทธิของประชาชนในข้อมูลส่วนบุคคลมีความสำคัญมากที่สุด โดยจะเห็นได้จากการที่กฎหมายของสหภาพยุโรปจะอนุญาตให้บริษัททำการโอนข้อมูลไปเก็บไว้ ณ ประเทศใดได้ ก็ต่อเมื่อประเทศนั้นมีกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ และในขณะเดียวกัน กฎหมายฉบับนี้ก็ยังไม่ได้ทำลายปรัชญาพื้นฐานว่าด้วยการรวมตัวกันของประเทศสมาชิกในสหภาพ เนื่องจากไม่ได้เป็นการบังคับใช้มาตรการกีดกันทางข้อมูลข่าวสารนี้กับประเทศสมาชิก และยังคงคุณค่าของความเป็นตลาดเสรีของประเทศสมาชิกในกลุ่มสหภาพไว้ได้ โดยข้อมูลข่าวสารต่าง ๆ ก็ยังคงไหลเวียนได้อย่างเสรีอยู่ในประเทศสมาชิกด้วยกัน

สำหรับประเทศจีน ประเด็นเรื่องความมั่นคงของรัฐมีความสำคัญมากที่สุด โดยพิจารณาได้จากการที่ผู้โอนข้อมูลออกไปนอกประเทศจะต้องขออนุญาตเจ้าหน้าที่รัฐก่อนเสมอ กรณีจึงแสดงให้เห็นว่าข้อมูลคือสมบัติของชาติจีน การนำข้อมูลไปเก็บไว้ ณ ต่างประเทศ อาจเป็นการสร้างความได้เปรียบเสียเปรียบในเชิงเศรษฐกิจให้แก่ประเทศจีนได้ เพราะภาครัฐจีนอาจเสียโอกาสที่ตนจะได้ล้วงข้อมูลของบริษัทข้ามชาติเหล่านั้นในประเทศของตนเอง หรือหากข้อมูลที่จะโอนออกไปนั้นเป็นข้อมูลของประเทศจีนเอง ประเทศจีนก็อาจเสียเปรียบให้แก่ต่างชาติเช่นเดียวกัน ด้วยการกระทำเช่นนี้ของประเทศจีนเอง จึงทำให้สหรัฐอเมริกานำบทเรียนที่ได้จากประเทศจีนนี้มาผสมกับแนวคิดเรื่องทุนนิยม และได้เป็นเกิดเป็นร่างกฎหมายใหม่ออกมา จนอาจกล่าวได้ว่าประเด็นเรื่องความหวาดกลัวชาติจีนและแนวคิดเรื่องระบบตลาดแบบทุนนิยมมีอิทธิพลอย่างมากต่อการร่างกฎหมายฉบับนี้ โดยความหวาดกลัวชาติจีนสังเกตได้จากการระบุชื่อประเทศต้องห้ามไม่ให้ถ่ายโอนข้อมูลไปเก็บไว้ ลงในกฎหมายโดยเฉพาะเจาะจง ซึ่งเป็นเหตุให้ประเทศรัสเซียพลอยถูกหางเลขไปด้วย และด้วยความคิดระบบตลาดแบบทุนนิยม ทำให้การร่างกฎหมายนี้ มุ่งเน้นไปที่ประเภทของบริษัทที่จะโอนข้อมูลกว่ามีประเภทใดบ้าง และบริษัทนั้นควรมีข้อจำกัดอย่างไร และมีการวิเคราะห์ไปถึงขั้นว่าบริษัทใดบ้างที่มีโอกาสเข้าถึงข้อมูลได้มาก และมีส่วนสำคัญที่กฎหมายนี้ต้องมาบังคับใช้เป็นพิเศษ ในขณะที่ประเด็นเรื่องการคุ้มครองสิทธิของประชาชนในข้อมูลส่วนบุคคลของสหรัฐอเมริกาอาจต้องปรับปรุงอีกมาก เนื่องจากกฎหมายนี้ไม่ได้ห้ามโดยชัดแจ้งว่าห้ามมิให้ส่งข้อมูลส่วนบุคคลนี้ให้แก่ประเทศที่ไม่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคล ดังเช่นที่สหภาพยุโรปมี นอกจากนี้ การมอบอำนาจในการพิจารณารายชื่อของประเทศต้องห้ามนั้น ยังอยู่ในดุลยพินิจของรัฐมนตรีว่าการกระทรวงการต่างประเทศ มิใช่กระทรวงกลาโหมหรือกระทรวงความมั่นคงแห่งมาตุภูมิสหรัฐซึ่งมีความข้องเกี่ยวกับการดูแลทุกข์สุขของประชาชนโดยตรง ซึ่งหากกล่าวถึงความชำนาญด้านการรักษาความปลอดภัยไซเบอร์ กระทรวงความมั่นคงแห่งมาตุภูมิคือกระทรวงที่เหมาะสมที่สุด เนื่องจากเป็นผู้จัดทำแนวทางในการรักษาความปลอดภัยไซเบอร์ให้แก่อุตสาหกรรมสำคัญต่าง ๆ เอง ดังนั้น จึงอาจกล่าวได้ว่าร่าง

กฎหมายของสหรัฐอเมริกาฉบับนี้เป็นเพียงเครื่องมือที่สหรัฐอเมริกาจะใช้ตอบโต้กับประเทศจีนบนเวทีการเมืองระหว่างประเทศเท่านั้น

4.3.4 การรับรองมาตรฐานความปลอดภัยและการตรวจสอบ

กฎหมายสหรัฐอเมริกา

โดยทั่วไป สหรัฐอเมริกาไม่มีกฎหมายใดบังคับให้ผู้ที่เกี่ยวข้องกับระบบโครงสร้างพื้นฐานสำคัญต้องใช้อุปกรณ์ที่รัฐรับรองว่าได้มาตรฐาน หากแต่เป็นเสรีภาพของผู้ประกอบการว่าจะเลือกใช้อุปกรณ์ใด อย่างไรก็ดี หากผู้ประกอบการต้องการป้องกันกิจการของตนจากการจู่โจมทางไซเบอร์ ผู้ประกอบการสามารถศึกษาได้จากคู่มือหรือแผนการจัดการเฉพาะของหน่วยงานภาครัฐดังนี้

1. กรอบทำงานด้านความมั่นคงปลอดภัยไซเบอร์ของสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (The NIST Cybersecurity Framework) จัดทำโดยสถาบันมาตรฐานและเทคโนโลยีแห่งชาติสหรัฐอเมริกา ซึ่งมีหน่วยงานในสังกัดกระทรวงพาณิชย์ [199]

2. แผนการจัดการเฉพาะ (Sector-Specific Plan) จัดทำโดยหน่วยงานความมั่นคงปลอดภัยของโครงสร้างพื้นฐาน หน่วยงานในสังกัดกระทรวงความมั่นคงแห่งมาตุภูมิ

อย่างไรก็ดี เมื่อต้นปี ค.ศ. 2020 การรับรองมาตรฐานความปลอดภัยและการตรวจสอบภาคบังคับได้ถูกริเริ่มขึ้นโดยกระทรวงกลาโหมสหรัฐอเมริกา หากผู้ประกอบการรายใดประสงค์จะเข้าร่วมการจัดซื้อจัดจ้างหรือรับช่วงต่อสัญญากับกระทรวงกลาโหม ผู้ประกอบการผู้นั้นต้องยินยอมให้หน่วยงานทำการตรวจสอบว่าบริษัทของผู้ประกอบการมีมาตรการรับรองความเสี่ยงภัยไซเบอร์ที่เป็นไปตามที่กำหนดก่อน[200] โดยสถานะการรับรองนั้นคือ Cybersecurity Maturity Model Certification (CMMC) ซึ่งผู้ประกอบการจะต้องมีการจัดวางโครงสร้างในองค์กรที่ดี และมีการใช้อุปกรณ์ซึ่งมีคุณสมบัติตามที่กำหนดไว้ด้วยจึงจะได้รับสถานะรับรอง[201]

กฎหมายสหภาพยุโรป

การรับรองมาตรฐานความปลอดภัยและการตรวจสอบเป็นหนึ่งในองค์ประกอบสำคัญในการส่งเสริมนโยบายตลาดเดียวสหภาพยุโรป (European Single Market) และเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ให้แก่ประเทศสมาชิกไปพร้อม ๆ กัน โดยอุปกรณ์ที่ได้รับการรับรองก็จะสามารถนำไปขายในประเทศสมาชิก

---

[199] National Institute of Standards and Technolog. 2020. "About NIST". NIST. https://www.nist.gov/about-nist.

[200] "Cybersecurity Maturity Model Certification (CMMC) Will Replace NIST 800-171 On Dod Rfis And Rfps In 2020". 2020. Steelcloud. https://www.steelcloud.com/cybersecurity-maturity-model-certification-cmmc.

[201] Tanenbaum, Mitch. 2020. "Why and How The Dod Is Implementing The CMMC". Cmmc-Certification.Com. https://cmmc-certification.com.

อื่นได้โดยง่าย และในขณะเดียวกัน ความมั่นคงปลอดภัยไซเบอร์ก็จะไม่ถูกคุกคามจากอุปกรณ์ที่ไม่มีคุณภาพหรือไม่ปลอดภัย[202]

ในปี ค.ศ. 2019 สหภาพยุโรปได้ออกกฎหมายหนึ่งขึ้น คือ REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) เพื่อเพิ่มบทบาทหน้าที่ให้กับองค์กรเพื่อความมั่นคงปลอดภัยไซเบอร์ (European Union Agency for Cybersecurity) ให้การเป็นตัวกลางระหว่างประเทศสมาชิกในการแบ่งปันข้อมูลข่าวสาร และกรณีนี้ก็ได้รวมไปถึงการแบ่งปันข้อมูลของผลิตภัณฑ์ด้วยว่าอุปกรณ์ใดได้ผ่านการทดสอบแล้ว เพื่อให้ประเทศสมาชิกอื่นรับทราบ และทำให้การนำอุปกรณ์นั้นไปจำหน่ายต่อในประเทศสมาชิกอื่นทำได้สะดวกขึ้น[203] แต่ทั้งนี้ก็ไม่ได้มีโทษแก่ผู้ที่หลีกเลี่ยงไม่นำสินค้าดังกล่าวไปตรวจสอบคุณภาพแต่อย่างใด

เปรียบเทียบกับกฎหมายจีน

ในการรับรองมาตรฐานความปลอดภัย และการตรวจสอบนั้น แต่ละประเทศต่างมีแนวทางที่ไม่เหมือนกัน สำหรับสหรัฐอเมริกา จะมีหน่วยงานรัฐที่ทำหน้าที่ให้การรับรองมาตรฐานความปลอดภัยของอุปกรณ์ต่าง ๆ แต่ทั้งนี้ไม่มีสภาพบังคับ กล่าวคือผู้ประกอบการสามารถเลือกได้ว่าจะใช้อุปกรณ์ที่ผ่านการรับรองหรือไม่ ตามคู่มือที่หน่วยงานรัฐได้จัดทำไว้ สำหรับสหภาพยุโรป จะมีองค์กรระหว่างประเทศสมาชิก ซึ่งมีหน้าที่รับรองมาตรฐานความปลอดภัยของอุปกรณ์ต่าง ๆ เช่นกัน และไม่มีสภาพบังคับ ทว่าหากอุปกรณ์ดังกล่าวผ่านการรับรอง การจำหน่ายสินค้าชิ้นเดียวกันนี้ในประเทศสมาชิกอื่นจะทำได้ง่ายขึ้น ในขณะที่ประเทศจีนเอง กลับบังคับให้ผู้ประกอบธุรกิจในกิจการบางประเภท หรือหน่วยงานรัฐที่เกี่ยวกับความมั่นคง ใช้อุปกรณ์ที่หน่วยงานรัฐของจีนให้การรับรองเท่านั้น โดยหน่วยงานรัฐจีนจะเป็นผู้ตรวจสอบและรับรองมาตรฐานนั้นด้วยตนเอง

สำหรับสหรัฐอเมริกาและสหภาพยุโรปจะเห็นได้ว่าการเลือกใช้อุปกรณ์ใด ไม่ว่าอุปกรณ์นั้นจะผ่านการรับรอง ตรวจสอบหรือไม่ ขึ้นอยู่กับเสรีภาพของผู้ประกอบการ หากมองในด้านหนึ่ง จะเห็นว่ามาตรการดังกล่าวมีข้อดีคือ ในกรณีที่ผู้ประกอบการเห็นว่ากิจการของตนไม่จำเป็นต้องใช้อุปกรณ์ที่มีความปลอดภัยสูงมากนัก ไม่ว่าเพราะกิจการไม่เป็นกลุ่มเสี่ยงที่จะถูกโจมตีก็ดี หรือต้องการจะลดต้นทุนกิจการตนเองก็ดี ผู้ประกอบการสามารถเลือกและตัดสินใจได้เองตามความเหมาะสม แต่หากพิจารณา ก็อาจมีข้อเสียเช่นความ

[202] European Commission. 2020. "The EU Cybersecurity Certification Framework - Shaping Europe'S Digital Future - European Commission". European Commission. https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework.

[203] เรื่องเดียวกัน

ปลอดภัยของข้อมูลผู้ใช้บริการอาจไม่ได้รับการดูแลได้ดีเท่าที่ควร เนื่องจากอุปกรณ์ที่ใช้นั้นไม่ได้มาตรฐาน หรือมีอันตรายอยู่ในตัว

อย่างไรก็ดี สำหรับประเทศจีน การที่หน่วยงานรัฐและเอกชนใช้เพียงแต่อุปกรณ์ที่รัฐรับรองเท่านั้น อาจกลายเป็นผลเสียมากกว่าการใช้อุปกรณ์ที่ใช้นั้นไม่ได้มาตรฐาน หรือมีอันตรายอยู่ในตัวก็ได้ เนื่องจากว่าการที่รัฐจีนกำหนดให้ใช้แต่อุปกรณ์ที่รัฐรับรองจัดว่าเป็นมาตรการการกีดกันทางการค้าประเภทหนึ่ง ซึ่งส่งผลกระทบต่อการแข่งขันของตลาดสินค้าเทคโนโลยีภายในประเทศด้วย ทำให้ผู้ผลิตในจีนขาดแรงกดดันในการทำให้สินค้าของตนพัฒนาได้ดีเท่าสินค้าต่างชาติ จนท้ายที่สุดแล้ว อุปกรณ์ที่รัฐรับรองอาจมีประสิทธิภาพไม่ดีเท่าสินค้าที่อยู่ภายนอกประเทศ นอกจากนี้ การกำหนดให้ผู้ประกอบการหรือหน่วยงานรัฐใช้แต่อุปกรณ์ที่รับรับรอง อาจเป็นการสร้างข้อจำกัดในการเข้าถึงเทคโนโลยีให้แก่คนในชาติตน และทำให้ชาติตนล้าหลังทางเทคโนโลยีได้

4.3.4 การคุ้มครองข้อมูลส่วนบุคคล

กฎหมายสหรัฐอเมริกา

ก่อนปี ค.ศ. 2019 รัฐบาลกลางสหรัฐฯ ได้ออกกฎหมายเพียง 3 ฉบับเท่านั้นที่เกี่ยวข้องกับข้อมูลส่วนบุคคล โดยกฎหมายทั้ง 3 ฉบับนี้ได้แก่ รัฐบัญญัติว่าด้วยการเปลี่ยนแปลงแผนประกันสุขภาพและความรับผิด (Health Insurance Portability and Accountability Act) รัฐบัญญัติว่าด้วยการปฏิรูปธุรกิจการให้บริการทางการเงิน (Financial Services Modernization Act) และ รัฐบัญญัติว่าการบริหารจัดการความปลอดภัยในข้อมูลข่าวสารของรัฐบาลกลาง (Federal Information Security Management Act) ซึ่งต่างใช้คำกว้าง ๆ ว่าผู้ประกอบการหรือหน่วยงานรัฐที่ทำงานในด้านสาธารณสุข การเงิน หรือความมั่นคงต้องรักษาระบบและข้อมูลส่วนตัวให้เหมาะสม แต่ทั้งนี้ก็ไม่ได้มีบทลงโทษใด และเนื่องจากเป็นบทบัญญัติที่มีความหมายกว้างขวาง จึงไม่อาจทราบได้ว่าควรดำเนินการไปในทิศทางใดเพื่อให้บรรลุวัตถุประสงค์นั้น ด้วยเหตุนี้ ในท้ายที่สุด การคุ้มครองข้อมูลส่วนบุคคลจึงไม่ได้รับการสนใจจากผู้ประกอบการหรือหน่วยงานภาครัฐเท่าที่ควร

นอกจากนี้ การล้มเหลวหรือละเมิดในข้อมูลส่วนบุคคลของบริษัท ๆ หนึ่งโดยการนำไปใช้ประโยชน์ต่อหรือนำไปขายต่อก็ดี มักนำไปสู่การพิจารณาโดยคณะกรรมการการค้า (Federal Trade Commission) ว่าเป็นหนึ่งในการกระทำทางการตลาดที่เป็นการหลอกลวง (Deceptive Practices) เท่านั้น โดยบริษัทจะมีความรับผิดตามการกระทำนั้นก็ต่อเมื่อบริษัทนั้นได้ทำผิดสัญญาว่าด้วยความเป็นส่วนตัว หรือไม่ได้จัดเตรียมมาตรการที่เหมาะสม และทำให้เกิดความเสียหายแก่เจ้าของข้อมูล[204]

[204] Chabinsky, Steven. 2019. "ICLG - Data Protection Laws And Regulations - USA Covers Relevant Legislation And Competent Authorities, Territorial Scope, Key Principles, Individual Rights, Registration Formalities, Appointment Of A Data Protection Officer And Of Processors - In 42 Jurisdictions". International Comparative

ทั้งนี้ความรับผิดในการละเมิดข้อมูลส่วนบุคคลอาจเป็นเพียงส่วนเล็ก ๆ ที่สอดแทรกอยู่ในกฎหมายหลาย ๆ ฉบับ เช่น รัฐบัญญัติว่าด้วยการคุ้มครองความเป็นส่วนตัวของผู้ขับขี่ (Driver Privacy Protection Act) ซึ่งระบุให้ชื่อ รูปภาพ หมายเลขบัตรประจำตัวประชาชน หมายเลขประกันสังคม ที่กรมขนส่ง (Department of Motor Vehicles) ได้รวบรวมไว้ได้รับความคุ้มครองตามกฎมหาย และการเปิดเผยรายละเอียดดังข้างต้นโดยปราศจากความยินยอมถือว่าเป็นความผิด หรือรัฐบัญญัติว่าด้วยการปกป้องความเป็นส่วนตัวของเยาวชนบนโลกออนไลน์ (Children's Online Privacy Protection Act) ซึ่งห้ามมิให้ผู้ใดเก็บรวมรวมข้อมูลส่วนตัวของเด็กอายุต่ำกว่า 13 ปี ในรูปแบบออนไลน์ เว้นแต่จะได้รับความยินยอมจากผู้ปกครองก่อน [205]

ความกระจัดกระจายของกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ประกอบกับความไม่ชัดเจนของแนวทางปฏิบัติตดังกล่าวทำให้สรุปได้ว่า ในช่วงก่อนปี ค.ศ. 2019 กฎหมายของสหรัฐอเมริกายังไม่ได้เล็งเห็นถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลอย่างเป็นเฉพาะมากเท่าใดนัก

จนกระทั่งปี ค.ศ. 2019 รัฐบัญญัติความมั่นคงของชาติและการคุ้มครองข้อมูลส่วนบุคคลได้ถูกนำเสนอขึ้น โดยมีลักษณะเป็นการคุ้มครองข้อมูลส่วนบุคคล โดยคำว่าข้อมูลผู้ใช้ (User data) ซึ่งเป็นสิ่งที่ถูกคุ้มครองตามกฎหมายฉบับนี้มีนิยามว่า[206] “ข้อมูลข่าวสารใด ๆ ซึ่งบุคคลใดก็ตามได้รับมาจากการให้บริการเชิงข้อมูล เช่นผ่านทางเว็บไซด์ หรือแอปพลิเคชัน โดยข้อมูลเหล่านั้นอาจทำให้ทราบถึง แสดงถึงความสัมพันธ์ อธิบาย หรือมีส่วนเกี่ยวข้องกับพลเมืองสัญชาติอเมริกาหรือมีถิ่นพำนักอยู่ในสหรัฐอเมริกา อนึ่ง ไม่จำต้องพิจารณาว่าข้อมูลเหล่านั้นได้มาจากตัวเจ้าของข้อมูลเองหรือไม่ ได้มาจากการสังเกตพฤติกรรมของเจ้าของข้อมูลเองหรือไม่ หรือได้ข้อมูลเหล่านั้นมาด้วยวิธีการใด”เมื่อข้อมูลเหล่านั้นตรงตามนิยามของกฎหมาย บริษัทที่ครอบครองข้อมูลนั้นจะมีหน้าที่ตามกฎหมาย

ในกรณีที่บริษัทนั้นเป็นบริษัทเทคโนโลยีอันอยู่ในข่าย (Covered technology company) อันหมายถึงบริษัทที่มีการให้บริการออนไลน์เป็นหลัก บริษัทจะมีหน้าที่ดังต่อไปนี้[207]

1. หน้าที่ในการเก็บข้อมูลเท่าที่จำเป็น (Minimal Collection of Data)

บริษัทต้องไม่เก็บข้อมูลผู้ใช้มากเกินกว่าความจำเป็นในการให้บริการนั้น ๆ

2. หน้าที่ในการไม่นำข้อมูลนั้นไปใช้ประโยชน์ต่อ (Prohibition on Secondary Uses)

Legal Guides International Business Reports. https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa.

[205] เรื่องเดียวกัน.

[206] มาตรา 2(6) National Security and Personal Data Protection Act

[207] มาตรา 3 National Security and Personal Data Protection Act

การไม่นำข้อมูลนั้นไปใช้ประโยชน์ต่อรวมไปถึงการห้ามไม่ให้บริษัทนำข้อมูลนั้นไปใช้ประกอบการวิเคราะห์เพื่อให้การโฆษณานั้นตรงต่อกลุ่มเป้าหมาย หรือแสดงข้อมูลต่อบุคคลที่สามหรือระบุถึงตัวตนของเจ้าของข้อมูลโดยไม่จำเป็น

3. หน้าที่ในการอนุญาตให้เจ้าของข้อมูลดูข้อมูลและลบข้อมูลนั้น (Right to Review and Delete Data)

บริษัทต้องอนุญาตให้เจ้าของข้อมูลดูข้อมูลที่บริษัทนั้นครอบครองอยู่และลบข้อมูลเหล่านั้นอย่างถาวรตามความประสงค์ของเจ้าของข้อมูล โดยไม่จำกัดว่าข้อมูลนั้น บริษัทได้มาโดยวิธีการใด

4. หน้าที่ในการรายงานผล (Reporting Requirement)

ผู้บริหารสูงสุดของบริษัทมีหน้าที่ในการรายงานไปยังหน่วยงานภาครัฐรายปีว่าบริษัทได้ทำตามมาตรการเหล่านี้แล้วอย่างไรบ้าง

ทว่า สำหรับบริษัทเทคโนโลยีทั่วไป ไม่ปรากฏว่ามีหน้าที่ใดในการการคุ้มครองข้อมูลส่วนบุคคล ทั้งนี้ไม่ว่าบริษัทเทคโนโลยีจะจัดเป็นประเภทใด มาตรการการเก็บรวบรวมข้อมูลไว้ในท้องที่ยังเป็นสิ่งที่ต้องปฏิบัติตามอยู่เสมอ

กฎหมายสหภาพยุโรป

กฎหมายสำคัญที่เกี่ยวข้องกับการเก็บรวบรวมข้อมูลไว้ภายในท้องที่ได้แก่ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC หรือ General Data Protection Regulation ซึ่งได้นิยามคำว่าข้อมูลส่วนบุคคล ไว้ว่าหมายถึง “ข้อมูลใด ๆ ก็ตามที่สามารถทำให้ทราบถึงบุคคลใดได้โดยเฉพาะเจาะจง ไม่ว่าจะโดยตรงหรือโดยอ้อม เช่น ชื่อ หมายเลขบัตรประจำตัวประชาชน ข้อมูลสถานที่ ตัวตนบนโลกออนไลน์ ตลอดจนรูปลักษณ์ทางกายภาพ อุปนิสัย ภาวะทางจิต อารมณ์ สถานะทางเศรษฐกิจ วัฒนธรรม หรือสภาพทางสังคมของบุคคลนั้น”[208]

ในการจัดเก็บข้อมูล ผู้รวบรวมข้อมูลจะต้องปฏิบัติตามวิธีการที่กฎหมายกำหนดไว้ เช่นการขอความยินยอมแก่เจ้าของข้อมูลก่อน การจัดให้รูปแบบการขอความยินยอมต้องแยกออกมาจากข้อตกลงการใช้บริการอื่นอย่างชัดเจน หรือการแจ้งให้ทราบถึงสิทธิของเจ้าของข้อมูลในการถอนความยินยอม[209] และนอกจากวิธีการทั่วไปในการขอความยินยอมแล้ว หากปรากฏว่าเจ้าของข้อมูลอายุต่ำกว่า 16 ปี ผู้ปกครองของเจ้าของข้อมูลจะต้องให้ความยินยอมร่วมด้วย[210]

---

[208] มาตรา 4 (1) General Data Protection Regulation

[209] มาตรา 7 General Data Protection Regulation

[210] มาตรา 8 General Data Protection Regulation

ในการคุ้มครองข้อมูล กฎหมายกำหนดให้ผู้ควบคุมมีหน้าที่ต้องใช้มาตรการที่เหมาะสมในการคุ้มครองข้อมูลที่ได้มา[211] และมีการจำกัดบัญญัติรองรับสิทธิของเจ้าของข้อมูลด้วยเช่น สิทธิในการเข้าถึงข้อมูลของตนเอง[212] สิทธิในการแก้ไขข้อมูลของตนเองให้ถูกต้อง[213]สิทธิในการถูกลืม[214] สิทธิในการยับยั้งการประมวลผลข้อมูล[215]

การฝ่าฝืนทั้งในการจัดเก็บข้อมูล การคุ้มครองข้อมูล หรือการละเมิดสิทธิของเจ้าของข้อมูลก็ดี ผู้ฝ่าฝืนจะได้รับโทษปรับตามมาตรา 83 และมาตรา 84 ของกฎหมายฉบับนี้ ซึ่งค่าปรับอาจปรับเป็นจำนวนเงินแน่ชัดหรือเป็นอัตราส่วนร้อยละจากผลประกอบการรายปีของบริษัทนั้นก็ได้ แล้วแต่กรณี

เปรียบเทียบกับกฎหมายจีน

กฎหมายการคุ้มครองข้อมูลส่วนบุคคลของแต่ละประเทศมีลักษณะที่ใกล้เคียงกัน โดยทั้งสหรัฐอเมริกา สหภาพยุโรป และประเทศจีนต่างมีกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่ให้สิทธิผู้ที่เป็นเจ้าของข้อมูลในการตรวจสอบ แก้ไข หรือลบข้อมูลของตนเองได้ รวมถึงหน้าที่ของผู้ควบคุมข้อมูลในการเก็บข้อมูลเท่าที่จำเป็นและการขอความยินยอมต่อเจ้าของข้อมูลก่อนเก็บข้อมูลนั้น

อย่างไรก็ดี แม้ประเทศจีนจะมีกฎหมายเพื่อการคุ้มครองข้อมูลส่วนบุคคล แต่ก็มีบทบัญญัติกฎหมายอื่นซึ่งอาจขัดต่อการคุ้มครองข้อมูลส่วนบุคคลดังนี้

ประการแรก ประเทศจีนมีกฎหมายที่ให้อำนาจเจ้าหน้าที่รัฐในการขอความร่วมมือจากผู้ให้บริการทางเครือข่ายในการสืบสวนอาชญากรรม ซึ่งเจ้าหน้าที่รัฐอาจขอความร่วมมือเมื่อใดก็ได้ และหากผู้ให้บริการทางเครือข่ายไม่ช่วยเหลือ ก็จะมีโทษปรับตามกฎหมายตลอดจนเพิกถอนใบอนุญาต นอกจากนี้ การขอความร่วมมือจากผู้ให้บริการเครือข่ายในการละเมิดสิทธิส่วนบุคคลนี้ยังสามารถทำได้โดยไม่ต้องขอหมายศาล ในขณะที่ในหลาย ๆ ประเทศ หมายศาลเป็นสิ่งจำเป็นในการรวบรวมพยานหลักฐานต่าง ๆ

ประเด็นถัดมา ในการเข้าใช้บริการอินเทอร์เน็ตจะต้องมีการระบุยืนยันตนเองด้วยชื่อจริงเสมอ กฎหมายนี้เป็นแนวบังคับว่า หากไม่ยอมให้ข้อมูลส่วนบุคคลมาก็จะไม่ได้ใช้บริการอินเทอร์เน็ต บทกฎหมายนี้ขัดกับกฎหมาย การคุ้มครองข้อมูลส่วนบุคคลอย่างชัดเจน เนื่องจากเป็นการข่มขู่แกมบังคับให้เจ้าของข้อมูลส่งข้อมูลให้เสียมากกว่า

ประการที่สาม ประเทศจีนมีกฎหมายว่าด้วยการเก็บข้อมูลไว้ภายในท้องที่ เพื่อบังคับให้บริษัทต่างชาติเก็บข้อมูลไว้ภายในอาณาเขตประเทศจีนและทำให้รัฐบาลจีนเองได้ครอบครองข้อมูลนั้นไปด้วย ทั้ง ๆ ที่ข้อมูลนั้นเป็นข้อมูลส่วนบุคคล แต่ก็เป็นที่ทราบกันดีว่า รัฐบาลจีนประสงค์จะให้ข้อมูลนั้นอยู่ในอาณาเขตประเทศตน

---

[211] มาตรา 25 General Data Protection Regulation

[212] มาตรา 15 General Data Protection Regulation

[213] มาตรา 16 General Data Protection Regulation

[214] มาตรา 17 General Data Protection Regulation

[215] มาตรา 18 General Data Protection Regulation

เพื่อที่ตนจะได้ล้วงข้อมูลนั้นมาใช้สร้างความได้เปรียบในเชิงเศรษฐกิจให้กับตนในภายหลัง ด้วยเหตุนี้กฎหมายว่าด้วยการเก็บข้อมูลไว้ภายในท้องที่จึงได้เกิดขึ้น

กรณีศึกษา: กฎหมายการเข้ารหัสข้อมูลของประเทศออสเตรเลีย (Australian Encryption Law)

ร่างกฎหมายได้ผ่านการอนุมัติเป็นกฎหมายในกลางเดือนธันวาคม ค.ศ. 2018 ซึ่งมีชื่ออย่างเป็นทางการว่า Assistance and Access Act 2018 โดยทางการออสเตรเลียให้เหตุผลถึงความจำเป็นของการออกกฎหมายนี้ว่า ทั้งรัฐและผู้ให้บริการทางเทคโนโลยีควรมีการรับผิดชอบร่วมกันในการจัดการดูแลความปลอดภัยของชาวออสเตรเลียที่ใช้เทคโนโลยีและแอปพลิเคชันในชีวิตประจำวัน กฎหมายนี้เป็นการบังคับให้บริษัทผู้ให้บริการเทคโนโลยีคอมพิวเตอร์ยอมให้รัฐ ตำรวจ หรือข้าราชการในองค์การเกี่ยวกับความปลอดภัยเข้าถึงข้อมูลที่เข้ารหัสหรือเป็นความลับของผู้ใช้งานโดยที่ผู้ใช้งานไม่รู้ตัว เพื่อจัดการอาชญากรรม การก่อการร้าย และดูแลความมั่นคงของประเทศ รัฐได้อธิบายว่ากฎหมายนี้มีขึ้นเพื่อแก้ไขการเข้ารหัสแบบ End-to-end เนื่องจากหลายๆ แอปพลิเคชัน เช่น Whatsapp Signal ได้เพิ่มการรักษาความปลอดภัยแบบดังกล่าวให้มีเพียงผู้ส่งและผู้รับเท่านั้นที่สามารถดูข้อมูลได้ โดยที่ผู้ให้บริการหรือคนกลางจะไม่สามารถรับรู้ด้วยไม่ได้เลย ทางการออสเตรเลียชี้ว่านี่คือช่องทางหลักที่อาชญากรและผู้ก่อการร้ายไซเบอร์นิยมใช้ในการก่ออาชญากรรมไซเบอร์[216]

Assistance and Access Act 2018 จะให้อำนาจแก่หน่วยงานของรัฐบาลในการสั่งให้บริษัทเทคโนโลยีสร้างช่องทางพิเศษในการเข้าไปตรวจสอบว่ามีบทสนทนาหรือข้อมูลใดที่เกี่ยวข้องกับการก่อการร้าย สื่อลามกเด็ก การค้ายาเสพติด และการค้ามนุษย์ ซึ่งเป็นการทำลายการเข้ารหัสแบบ End-to-end และเปิดโอกาสให้ผู้ให้บริการสามารถเข้าถึงข้อมูลเหล่านั้นได้

กรณีจึงมีความคล้ายคลึงกับกฎหมายประเทศจีนที่ที่ผู้ให้บริการต้องให้ความช่วยเหลือทางเทคนิคแก่เจ้าหน้าที่รัฐ แต่อย่างไรก็ดี จะพบข้อแตกต่างอยู่ 3 ข้อคือ

ประการแรก ในกฎหมายจีน เจ้าหน้าที่สามารถขอความช่วยเหลือจากผู้ให้บริการโดยไม่ต้องใช้หมายศาลก่อน แต่กฎหมายของออสเตรเลีย การใช้หมายศาลยังคงมีความจำเป็น

ประการที่สอง เหตุผลของเจ้าหน้าที่ในการใช้อำนาจตามกฎหมายจีนมีความยืดหยุ่นและกว้างขวางกว่ามาก คืออ้างเหตุผลด้านความมั่นคงของรัฐ เมื่อเทียบกับกฎหมายของออสเตรเลียที่ระบุชัดเป็นเรื่อง ๆ ไป

[216] Department of Home Affairs. "The Assistance And Access Act 2018". 2020. Homeaffairs.Gov.Au. https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/
data-encryption#:~:text=The%20Australian%20Government%20supports%20cyber,safe%20online%20environment%20for%20Australians.&text=it%20is%20estimated%20that%20by,investigative%20value%20will%20be%20encrypted.

ประการสุดท้าย กฎหมายจีนบังคับแต่แรกให้ผู้ให้บริการสร้างช่องทางพิเศษเพื่อให้รัฐเข้าถึงเป็นการเฉพาะ ในขณะที่กฎหมายออสเตรเลียเพียงบังคับให้ผู้ให้บริการสร้างช่องทางพิเศษไว้เตรียมพร้อม แต่มิได้สร้างไว้ให้แก่รัฐโดยตรง หากแต่สร้างเผื่อไว้ในกรณีที่เจ้าหน้าที่รัฐได้มีการร้องขอ โดยหากเปรียบเทียบการสร้างช่องทางพิเศษนี้กับการสร้างกุญแจบ้าน ในมุมของกฎหมายจีน ผู้ให้บริการต้องสร้างกุญแจสำหรับเข้าบ้านและมอบให้กับรัฐไปทันที ในขณะที่ในมุมของกฎหมายออสเตรเลีย ผู้ให้บริการเพียงต้องสร้างกุญแจสำหรับเข้าบ้านไว้เท่านั้น และจะมอบให้แก่รัฐได้ก็ต่อเมื่อมีหมายศาล

จากกฎหมายฉบับนี้ ฝ่ายที่สนับสนุนมองว่า กฎหมายบังคับให้ภาคเอกชนต้องร่วมมือกับกับรัฐ โดยมีเงื่อนไขที่สมเหตุสมผลตามกฎหมาย เช่น ต้องมีหมายศาลอนุญาตให้เข้ารหัส หรือการเข้ารหัสจะช่วยในกระบวนการสืบสวนได้จริง หาได้ให้อำนาจรัฐอย่างไม่มีขีดจำกัดดังเช่นกฎหมายของจีน ซึ่งเพียงมีข้อสงสัยรัฐก็สามารถอ้างเป็นเหตุเพื่อเข้าถึงข้อมูลได้หรือให้ Backdoor กับรัฐตั้งแต่เริ่มแรก มุมมองดังกล่าวเห็นว่า ทางการออสเตรเลียต้องการแก้ไขปัญหาในกรณีที่เกิดเหตุการณ์ที่คล้ายกับเหตุการณ์ San Bernaedino ที่สหรัฐอเมริกา ซึ่ง FBI ได้ iPhone ผู้ต้องหามาแต่ติดรหัสผ่าน เมื่อ FBI ขอเข้าถึงข้อมูลจากแอปเปิล แอปเปิลปฏิเสธที่จะให้ FBI เข้ารหัสโทรศัพท์ของผู้ต้องหาเนื่องจากเหตุผลเรื่องการเคารพความเป็นส่วนตัวของลูกค้า อย่างไรก็ดี ในคดีนั้น ทาง FBI ก็เข้าถึงข้อมูลได้โดยใช้แฮกเกอร์ โดยทางการออสเตรเลียมีความมุ่งหมายจะทำให้การเข้ารหัสข้อมูลชัดเจนและถูกรองรับทำโดยอำนาจที่ถูกต้องเมื่อมีเหตุจำเป็น[217]

ในทางกลับกัน บริษัท แอปเปิล กูเกิล ไมโครซอฟต์ เฟซบุ๊ก และผู้คัดค้านกฎหมายนี้รายอื่นๆ ต่างเห็นว่ากฎหมายไม่ได้ให้ความสำคัญต่อความปลอดภัยของข้อมูล สิทธิมนุษยชน และความเป็นส่วนตัวของผู้ใช้ การให้อำนาจการเข้าถึงของรัฐที่มากเกินไปเป็นการยากที่จะควบคุมรัฐในทางปฏิบัติ บริษัทแอปเปิลแสดงจุดยืนที่ชัดเจนต่อกฎหมายฉบับนี้ว่า กฎหมายนี้จะทำให้ความปลอดภัยในการใช้งานผลิตภัณฑ์แอปเปิลของชาวออสเตรเลียลดลง อีกทั้งการละเมิดความปลอดภัยของคนส่วนมากเพื่อจะตรวจสอบหรือสอบสวนผู้กระทำผิดส่วนน้อยนั้นเป็นการได้ไม่คุ้มเสียและไม่ได้สัดส่วน[218]

[217] Zwart, Alexandra De. 2019. "Australia: Assistance And Access Act, December 2018 – Uncertainty Created By New Rushed-In Data Encryption Laws". Privacy Matters. https://blogs.dlapiper.com/privacymatters/australia-assistance-and-access-act-december-2018-holy-grail-of-uncertainty-created-by-new-rushed-in-data-encryption-laws/.

[218] Statt, Nick. 2018. "Apple Argues Stronger Encryption Will Thwart Criminals In Letter To Australian Government". The Verge. https://www.theverge.com/2018/10/12/17971444/apple-iphone-stronger-encryption-letter-australian-assistance-and-access-bill-2018.

กรณีศึกษา: หน่วยงานสากลที่เกี่ยวข้องกับการกำกับดูแลไซเบอร์สเปซ

ประชาคมอินเตอร์เน็ต (Internet Society) [219]

ประชาคมอินเทอร์เน็ต เป็นองค์กรที่มีวัตถุประสงค์สนับสนุนการสร้างมาตรฐานที่เกี่ยวข้องกับอินเตอร์เน็ต โดยเริ่มจัดตั้งขึ้นในสหรัฐอเมริกาตั้งแต่ปี ค.ศ. 1992 และยกระดับเป็นองค์กรสากล ปัจจุบันมีสำนักงานใหญ่อยู่ที่กรุงเจนีวา ประเทศสวิสเซอร์แลนด์และในรัฐเวอร์จิเนีย ประเทศสหรัฐอเมริกา

การทำงานของประชาคมอินเตอร์เน็ตในแต่ละปีจะมีแผนงานและจุดเน้นที่แตกต่างกันไป ในปี ค.ศ. 2019 จะเน้นไปที่ 4 มิติหลักได้แก่ **หนึ่ง** การสร้างความเชื่อมั่นในการใช้อินเทอร์เน็ต: สนับสนุนโครงการของหน่วยงานอื่น ๆ เพื่อทำให้อินเทอร์เน็ตปลอดภัย และผู้ใช้งานใช้งานโดยปราศจากความกังวลเรื่องความปลอดภัยของข้อมูล **สอง** การเชื่อมทั้งโลกเข้าด้วยกัน: ทำให้ทุกๆ ที่บนโลกมีโครงสร้างพื้นฐาน เทคโนโลยีที่เท่าทัน เปิดโอกาสให้ทุกคนได้ใช้อินเทอร์เน็ต **สาม** พัฒนาความปลอดภัยในทางเทคนิค: เป็นตัวกลางเชื่อมหน่วยงานเกี่ยวกับความปลอดภัยด้านโครงสร้างพื้นฐานอินเทอร์เน็ตให้ร่วมมือกัน เพื่อทำให้อินเทอร์เน็ตปลอดภัยในแง่ระบบเช่น มาตรฐาน TLS--Transport Layer Security, Deploy360 Program, MANRS-Manually Agreed Norms for Routing Security Campaign และ **สี่** พยากรณ์อนาคตของอินเทอร์เน็ต: ศึกษาผลกระทบของอินเทอร์เน็ตตลอด 30 ปีทีผ่านมา และคาดคะเนมาตรการในการดูแล รวมทั้งทิศทางการพัฒนาของอินเทอร์เน็ต

ทั้งนี้ ประชาคมอินเตอร์เน็ตทำงานเป็น NGOs ได้รับเงินสนับสนุนจากสมาชิกและผู้บริจาค ทั้งหมดทำภายใต้วิสัยทัศน์ The Internet is for Everyone เพื่อให้อินเทอร์เน็ตเข้าถึงได้โดยทุกคนและใช้ให้เกิดประโยชน์สูงสุดกับมวลมนุษยชาติ

ที่ประชุมว่าด้วยธรรมาภิบาลด้านอินเทอร์เน็ต (Internet Governance Forum) [220]

ที่ประชุมว่าด้วยธรรมาภิบาลด้านอินเทอร์เน็ต เป็นการประชุมเพื่อการจัดการกำกับดูแลอินเทอร์เน็ตในด้านข้อกำหนดและนโยบาย มีตัวแทนทั้งจากภาครัฐและเอกชนเข้าร่วมประชุมและแสดงความเห็น การประชุมนี้ริเริ่มโดยองค์การสหประชาชาติในปี ค.ศ. 2006 มีการประชุมปีละครั้ง โดยการประชุมนี้มีลักษณะเป็นการแลกเปลี่ยน รับฟังความคิดเห็นที่หลากหลาย มากกว่าจะเป็นการตัดสินหรือแทรกแซงควบคุมโดย

[219] Internet Society. 2020. "About Internet Society | Internet Society". Internet Society. https://www.internetsociety.org/about-internet-society/.

[220] Internet Governance Forum. 2020. "About The IGF". https://www.intgovforum.org/multilingual/tags/about.

องค์การสหประชาชาติ สำหรับในปี ค.ศ. 2019 การประชุมจัดขึ้นที่ประเทศเยอรมนี ในวันที่ 25-29 พฤศจิกายน ในหัวข้อ One World. One Net. One Vision.

Paris Call for Trust and Security 2018 [221]

Paris Call for Trust and Security (in Cyberspace) 2018 หรือ Paris Call เกิดจากการประชุม IGF ในปี ค.ศ. 2018 ที่กรุงปารีส ประเทศฝรั่งเศส เรียกได้ว่าเป็นการประกาศหลักการข้อกำหนดทั่วไปเกี่ยวกับความปลอดภัยบนไซเบอร์สเปซ กล่าวคือ เกี่ยวกับหน้าที่ของรัฐ การนำกฎหมายระหว่างประเทศมาประยุกต์ใช้บนไซเบอร์สเปซ ความรับผิดของผู้ให้บริการอินเทอร์เน็ต การดูแลเหยื่ออาชญากรรมไซเบอร์ และความร่วมมือระดับนานาชาติบนไซเบอร์สเปซ เป็นต้น

Paris Call เน้นย้ำถึงความเสี่ยงที่อาจเกิดจากความมั่นคงปลอดภัยทางไซเบอร์ที่อาจส่งผลร้ายต่ออินเทอร์เน็ต และการบล็อกควบคุมข้อมูลออนไลน์ที่อาจขัดกับหลักการปกครองในประเทศที่อยู่ภายใต้การปกครองระบอบประชาธิปไตย อีกทั้งยังกล่าวถึงภาระความรับผิดชอบของบริษัทใหญ่เกี่ยวกับอินเทอร์เน็ตและคอมพิวเตอร์ ความปลอดภัยของผลิตภัณฑ์ดิจิทัล และการร่วมมือระหว่างรัฐกับบริษัทเหล่านี้

อย่างไรก็ดี สหรัฐอเมริกา จีน และรัสเซียไม่ลงนามใน Paris Call ต่างกับอีกกว่า 50 ประเทศสมาชิกที่ลงนาม ส่วนบริษัทเทคโนโลยียักษ์ใหญ่อย่างไมโครซอฟต์ กูเกิล และเฟซบุ๊คลงนาม แต่แอปเปิล อะเมซอนและทุกบริษัทของจีนรวมถึง BAT ปฏิเสธการลงนามใน Paris Call

[221] Paris Call. 2020. "Paris Call For Trust And Security In Cyberspace". Pariscall.International. https://pariscall.international/en/.

บทที่ 5

ศึกษาเปรียบเทียบแนวทางการรักษาความปลอดภัยทางไซเบอร์ของประเทศไทย

ในบทนี้ จะวิเคราะห์แนวทางการรักษาความปลอดภัยทางไซเบอร์ของประเทศไทย ซึ่งปรากฏในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พระราชบัญญัติความมั่นคงปลอดภัยทางไซเบอร์พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล โดยจำแนกตามหัวข้อต่างๆ ได้แก่ หน้าที่ตามกฎหมายของผู้ให้บริการทางเครือข่าย การปกป้องระบบโครงสร้างพื้นฐานสำคัญ การเก็บรวบรวมข้อมูลไว้ภายในท้องที่ การรับรองมาตรฐานความปลอดภัยและการตรวจสอบ รวมทั้งให้ข้อสังเกตเปรียบเทียบกับแนวทางของประเทศจีน สหรัฐอเมริกา และสหภาพยุโรป

5.1 หน้าที่ตามกฎหมายของผู้ให้บริการทางเครือข่าย

มาตรา 3 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้ให้นิยามคำว่าผู้ให้บริการไว้ว่า หมายถึงบุคคล 2 ประเภท

ประเภทแรกได้แก่ บุคคลที่ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่นโดยผ่านทางระบบคอมพิวเตอร์ ไม่ว่าจะเป็นการให้บริการด้วยตนเองหรือให้บริการในนามของบุคคลอื่น

ประเภทที่สองได้แก่ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์ เพื่อประโยชน์ของบุคคลอื่น[222] โดยผู้ที่เป็นผู้ให้บริการมีหน้าที่ตามกฎหมายดังต่อไปนี้

[222] มาตรา 3 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

1. ไม่สนับสนุนหรือยินยอมให้มีการกระทำความผิดตามมาตรา 14[223] ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน มิฉะนั้นต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา 14[224]

2. ให้ความช่วยเหลือแก่พนักงานเจ้าหน้าที่ที่มีอำนาจในการส่งมอบข้อมูลดังต่อไปนี้เพื่อประโยชน์ในการสืบสอนหรือสอบสวน[225]

1.) ข้อมูลจราจรทางคอมพิวเตอร์เกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์

2.) ข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บหรือที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการเอง

ทั้งนี้ เจ้าพนักงานที่มีอำนาจในการสืบสวนหรือสอบสวน หากต้องการเรียกข้อมูลข้างต้นจะต้องมีคำสั่งศาลก่อน[226] เว้นเสียแต่ว่าจะปรากฏเหตุผลพิเศษคือ 1.) มีเหตุอันควรเชื่อได้ว่า มีการกระทำความผิดตามพระราชบัญญัตินี้ และ 2.) การขอข้อมูลดังกล่าวเป็นไปเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด และหาตัวผู้กระทำความผิด และ 3.) การขอข้อมูลนั้นมีความจำเป็น หากปรากฏเหตุพิเศษนี้ครบทั้งสามข้อ เจ้าพนักงานที่มีอำนาจอาจสั่งให้ผู้ให้บริการส่งมอบข้อมูลแก่ตนได้ทันที โดยมิต้องได้รับอนุญาตจากศาลก่อน[227]

3. ผู้ให้บริการอาจมีหน้าที่ต้องระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ หากปรากฏว่าข้อมูลคอมพิวเตอร์นั้นมีเนื้อหาที่อาจกระทบกระเทือนต่อความมั่นคงของประเทศ ตามที่กำหนดไว้ในภาคสอง

---

[223] มาตรา 15 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 บัญญัติไว้ว่า “ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

(1) นำเข้าสู่ระบบคอมพิวเตอร์ ซึ่งข้อมูลคอมพิวเตอร์ปลอม ไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน

(2) นำเข้าสู่ระบบคอมพิวเตอร์ ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

(3) นำเข้าสู่ระบบคอมพิวเตอร์ ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร หรือความผิดเกี่ยวกับการก่อการร้าย ตามประมวลกฎหมายอาญา

(4) นำเข้าสู่ระบบคอมพิวเตอร์ ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามก และข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

(5) เผยแพร่ หรือส่งต่อ ซึ่งข้อมูลคอมพิวเตอร์ โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม (1) (2) (3) หรือ (4)

[224] มาตรา 15 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

[225] มาตรา 18 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

[226] มาตรา 19 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

[227] มาตรา 18 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

ลักษณะ 1[228] หรือลักษณะ 1/1[229] แห่งประมวลกฎหมายอาญา หรือที่มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน และพนักงานเจ้าหน้าที่ ซึ่งได้รับความเห็นชอบจากรัฐมนตรีแล้ว อาจยื่นคำร้องพร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจ ขอให้มีคำสั่งระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้นได้ และภายหลังจากที่ศาลมีคำสั่งให้ระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้นแล้ว ผู้ให้บริการต้องระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้น หากได้รับคำสั่งจากเจ้าหน้าที่[230]

4. ผู้ให้บริการมีหน้าที่ต้องเก็บข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ หรืออาจเกินกว่านั้นก็ได้ หากได้รับคำสั่งจากพนักงานเจ้าหน้าที่ แต่ทั้งนี้ระยะเวลาดังกล่าวต้องไม่เกิน 1 ปี โดยข้อมูลที่ผู้ให้บริการต้องเก็บนั้นต้องเพียงพอเพื่อให้สามารถระบุตัวผู้ใช้บริการ โดยให้เก็บตั้งแต่วันที่เข้าใช้บริการ และสามารถกำจัดออกได้ หลังจากที่ผ่านพ้นวันสิ้นสุดการให้บริการไปแล้วเป็นเวลา 90 วัน[231]

ในปี พ.ศ. 2560 ได้มีการแก้ไขพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 โดยใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 ทำให้หน้าที่ของผู้ให้บริการเปลี่ยนไปจากเดิมบ้าง ดังต่อไปนี้

1. จากเดิมที่ผู้ให้บริการต้องไม่สนับสนุนหรือยินยอมให้มีการกระทำความผิดตามมาตรา 14 ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน มิฉะนั้นต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา 14 ได้เปลี่ยนเป็นผู้ให้บริการต้องไม่ให้ความร่วมมือ ยินยอม หรือรู้เห็นเป็นใจให้มีการกระทำความผิด มิฉะนั้นต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา 14 ด้วย[232]

2. จากเดิมที่ผู้ให้บริการต้องส่งมอบข้อมูลให้แก่พนักงานเจ้าหน้าที่ก็ต่อเมื่อมีเหตุผลพิเศษเท่านั้นคือ 1.) มีเหตุอันควรเชื่อได้ว่า มีการกระทำความผิดตามพระราชบัญญัตินี้ และ 2.) การขอข้อมูลดังกล่าวเป็นไปเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด และหาตัวผู้กระทำความผิด และ 3.) การขอข้อมูลนั้นมีความจำเป็น ได้เปลี่ยนเป็นว่า องค์ประกอบของเหตุผลพิเศษในข้อ 1.) นอกจากการเชื่อว่ามีเหตุอัน

---

[228] ฐานความผิดที่ถูกระบุไว้ในภาคสอง ลักษณะ 1 แห่งประมวลกฎหมายอาญา ชื่อว่า ความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร และประกอบด้วย 4 หมวดย่อยภายใน ได้แก่ หมวด1 ความผิดต่อองค์พระมหากษัตริย์ พระราชินี รัชทายาท และผู้สำเร็จราชการแทนพระองค์ (มาตรา 107-112) หมวด2 ความผิดต่อความมั่งคงของรัฐ ภายในราชอาณาจักร (มาตรา 113-118) หมวด3 ความผิดต่อความมั่นคงของรัฐ ภายนอกราชอาณาจักร (มาตรา 119-129) และ หมวด4 ความผิดต่อสัมพันธไมตรี กับต่างประเทศ (มาตรา 130-135)

[229] ฐานความผิดที่ถูกระบุไว้ในภาคสอง ลักษณะ 1/1 แห่งประมวลกฎหมายอาญา ชื่อว่า ความผิดเกี่ยวกับการก่อการร้าย (มาตรา 135/1-135/4)

[230] มาตรา 20 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

[231] มาตรา 26 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

[232] มาตรา 9 พระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

ควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้แล้วนั้น หากพนักงานเจ้าหน้าที่ได้รับคำร้องขอจากพนักงานสอบสวน ก็สามารถเอาเหตุนี้มาแทนองค์ประกอบดังกล่าวได้เช่นกัน[233]

3. จากเดิมที่ผู้ให้บริการต้องระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ หากปรากฏว่าข้อมูลคอมพิวเตอร์นั้นมีเนื้อหาที่อาจกระทบกระเทือนต่อความมั่นคงของประเทศ ตามที่กำหนดไว้ในภาคสองลักษณะ 1 หรือลักษณะ 1/1 แห่งประมวลกฎหมายอาญา ได้มีการเพิ่มหมวดความผิดอีกสองหมวดเข้ามาด้วย คือ[234]

1.) ข้อมูลคอมพิวเตอร์ที่เป็นความผิดตามกฎหมายนี้

2.) ข้อมูลคอมพิวเตอร์ที่เป็นความผิดอาญาตามกฎหมายเกี่ยวกับทรัพย์สินทางปัญญาหรือกฎหมายอื่นซึ่งข้อมูลคอมพิวเตอร์นั้นมีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชนและเจ้าหน้าที่ตามกฎหมายนั้นหรือพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญาได้ร้องขอ

ดังนั้นแล้ว หากพนักงานเจ้าหน้าที่ ซึ่งได้รับความเห็นชอบจากรัฐมนตรีแล้ว ยื่นคำร้องและแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจ ขอให้มีคำสั่งระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ประเภทนั้นๆ แล้ว ผู้ให้บริการก็ต้องระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้นด้วย หากได้รับคำสั่งจากเจ้าหน้าที่[235]

4. จากเดิมที่ผู้ให้บริการมีหน้าที่ต้องเก็บข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าระยะเวลาที่กฎหมายกำหนดไว้นั้น เว้นแต่พนักงานเจ้าหน้าที่จะสั่งให้เก็บเกินกว่าระยะเวลาที่กฎหมายกำหนด แต่ทั้งนี้ระยะเวลาที่เจ้าหน้าที่สั่งต้องไม่เกิน 1 ปี ทว่าสำหรับกฎหมายใหม่ ได้มีการแก้ไขให้เจ้าพนักงานสามารถสั่งให้ผู้ให้บริการเก็บข้อมูลไว้ได้ยาวนานที่สุดคือ 2 ปี[236]

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เป็นกฎหมายฉบับแรกที่กำหนดหน้าที่ให้แก่ผู้ให้บริการทางเครือข่าย โดยหน้าที่สำคัญของผู้ให้บริการทางเครือข่ายไม่ใช่การรักษาเสถียรภาพของระบบที่ตนให้บริการให้สามารถทำงานต่อไปได้ แต่เป็นหน้าที่การช่วยเหลือรัฐในการป้องปรามการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กฎหมายฉบับนี้ได้เอาผิดแก่ผู้ให้บริการที่สนับสนุนหรือยินยอมให้มีการกระทำความผิดตามกฎหมายฉบับนี้ ให้ความช่วยเหลือแก่พนักงานเจ้าหน้าที่ในการสืบสวนสอบสวนอาชญากรรม ระงับการเผยแพร่ข้อมูลที่ต้องห้ามตามกฎหมายนี้ รวมถึงการเก็บข้อมูลการเข้าสู่ระบบคอมพิวเตอร์ของผู้ใช้บริการไว้เป็นระยะเวลาอย่างน้อย 90 วัน จะเห็นได้ว่าไม่มีมาตราใดหรือกฎหมายอื่นใดที่กล่าวถึงหน้าที่ของผู้ให้บริการในการเสริมสร้างระบบการรักษาความปลอดภัยของตน แม้เมื่อมีการแก้ไข

---

[233] มาตรา 13 พระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

[234] มาตรา 14 พระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

[235] เรื่องเดียวกัน.

[236] มาตรา 17 พระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

กฎหมายฉบับนี้อีกครั้งโดยพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 ผู้ให้บริการก็ยังคงมีหน้าที่เพียงช่วยรัฐในการปราบปรามอาชญากรรมแต่เพียงเท่านั้น

หากสังเกตกฎหมายของสหภาพยุโรปและประเทศจีนเกี่ยวกับหน้าที่ตามกฎหมายของผู้ให้บริการทางเครือข่าย จะพบว่าสหภาพยุโรปไม่ได้มองว่าหน้าที่ของผู้ให้บริการเครือข่ายคือการช่วยรัฐปราบปรามความผิดเกี่ยวกับคอมพิวเตอร์แต่อย่างใด หากแต่หน้าที่ของผู้ให้บริการเครือข่ายคือการจัดให้มีมาตรการที่เหมาะสมในการบริหารจัดการความเสี่ยงไซเบอร์ ในขณะที่ประเทศจีนกลับกำหนดให้หน้าที่ของผู้ให้บริการเครือข่ายเป็นไปได้ทั้งสองประการคือช่วยรัฐในการปราบปรามอาชญากรรมคอมพิวเตอร์ และกำหนดหน้าที่ให้ผู้ให้บริการในการจัดทำมาตรการป้องกันความเสี่ยงไซเบอร์ที่เหมาะสมไปพร้อมๆ กันด้วย ในขณะที่กฎหมายของสหรัฐอเมริกานั้น ไม่ปรากฏว่าได้กำหนดหน้าที่ใดๆ แก่ผู้ให้บริการ

5.2 การปกป้องระบบโครงสร้างพื้นฐานสำคัญ

คำว่า “โครงสร้างพื้นฐานสำคัญ” ในเชิงความหมายของความมั่นคงปลอดภัยไซเบอร์นี้ ได้ถูกบัญญัติอยู่ในพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 โดยมาตรา 3 ได้นิยามให้คำว่า “โครงสร้างพื้นฐานสำคัญทางสารสนเทศ” หมายความว่า “คอมพิวเตอร์หรือระบบคอมพิวเตอร์ ซึ่งหน่วยงานของรัฐหรือหน่วยงานเอกชนใช้ในกิจการของตนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของรัฐ ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ” หน่วยงานของรัฐหรือ หน่วยงานเอกชนใดที่ได้ให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จะถูกเรียกว่า “หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ”

ในมาตรา 48 ของกฎหมายนี้ก็ได้เน้นย้ำให้เห็นถึงความสำคัญของโครงสร้างพื้นฐานสำคัญทางสารสนเทศขึ้นมาอีกว่า “โครงสร้างพื้นฐานสำคัญทางสารสนเทศเป็นกิจการที่มีความสำคัญต่อความมั่นคงของรัฐ ความมั่นคงทางทหาร ความมั่นคงทางเศรษฐกิจ และความสงบเรียบร้อยภายในประเทศ...” และได้ยกตัวอย่างสิ่งที่เข้าข่ายว่าเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศว่าอาจมีได้หลายด้านดังต่อไปนี้ [237]

1. ด้านความมั่นคงของรัฐ
2. ด้านบริการภาครัฐที่สำคัญ
3. ด้านการเงินการธนาคาร
4. ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม
5. ด้านการขนส่งและโลจิสติกส์

[237] มาตรา 49 พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

6. ด้านพลังงานและสาธารณูปโภค

7. ด้านสาธารณสุข

8. ด้านอื่นตามที่คณะกรรมการประกาศกำหนดเพิ่มเติม

เพื่อให้การรักษาความปลอดภัยไซเบอร์ในโครงสร้างพื้นฐานสำคัญเป็นไปอย่างมีประสิทธิภาพ กฎหมายนี้จึงได้จัดตั้งให้มี 3 หน่วยงานเกิดขึ้น เพื่อทำหน้าที่แยกคนละส่วนกัน ได้แก่ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ คณะกรรมการการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ และสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

สำหรับผู้มีอำนาจหน้าที่ในการกำหนดนโยบายต่างๆ ที่มีผลมากที่สุดต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ให้แก่โครงสร้างพื้นฐานสำคัญตามกฎหมายนี้ได้แก่ “คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ”[238] ซึ่งมีอำนาจหน้าที่ที่เกี่ยวกับการรักษาโครงสร้างพื้นฐานสำคัญ ดังนี้

1. กำหนดนโยบายการบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ[239]

2. ส่งเสริมการรับรองมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ[240]

3. กำหนดมาตรการและแนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของพนักงานเจ้าหน้าที่ เจ้าหน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ[241]

4. มอบหมายการควบคุมและกำกับดูแล รวมถึงการออกข้อกำหนด วัตถุประสงค์ หน้าที่และอำนาจและกรอบการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ[242]

นอกจากคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ซึ่งมีบทบาทในการกำหนดนโยบายต่างๆ ที่มีผลต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ให้แก่โครงสร้างพื้นฐานสำคัญแล้ว กฎหมายนี้ยังจัดตั้ง “คณะกรรมการการกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์” เพิ่มขึ้นมาอีกด้วย [243] ซึ่งมีอำนาจหน้าที่แยกต่างหากจากคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ดังนี้

---

[238] มาตรา 5 พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

[239] มาตรา 8 (2) พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

[240] มาตรา 8 (4) พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

[241] มาตรา 8 (5) พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

[242] มาตรา 8 (8) พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

[243] มาตรา 12 พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

1. กำหนดประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อันเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ [244]

2. กำหนดหน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน้าที่ของหน่วยงานควบคุมหรือกำกับดูแล โดยอย่างน้อยต้องกำหนดหน้าที่ให้หน่วยงานควบคุมหรือกำกับดูแลต้องกำหนดมาตรฐานที่เหมาะสมเพื่อรับมือกับภัยคุกคามทางไซเบอร์ของแต่ละหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

สำหรับหน่วยงานสุดท้ายที่ถูกจัดตั้งตามกฎหมายฉบับนี้ ได้แก่ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ[245] ซึ่งมีหน้าที่ให้ความร่วมมือหรือช่วยเหลือในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยเฉพาะภัยคุกคามทางไซเบอร์ที่กระทบหรือเกิดแก่โครงสร้างพื้นฐานสำคัญ ทางสารสนเทศ[246]

เมื่อพิจารณาทั้ง 3 หน่วยงานนี้แล้ว จะพบว่า หน่วยงานที่มีบทบาทมากที่สุด ได้แก่ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ซึ่งมีอำนาจในการกำหนด จัดทำนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ให้แก่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนำไปปฏิบัติตาม[247] ในขณะที่หน่วยงานที่มีหน้าที่รับนโยบายนั้นไปปฏิบัติตาม และให้การสนับสนุน หรือความช่วยเหลือในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่กระทบหรือเกิดแก่โครงสร้างพื้นฐานสำคัญทางสารสนเทศ ได้แก่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ[248]

นอกจากนี้ กฎหมายดังกล่าวยังมอบหน้าที่ให้แก่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้วยว่าต้องจัดให้มีมาตรฐานขั้นต่ำเรื่องความมั่นคงปลอดภัยไซเบอร์ของตนเอง และหากหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้นไม่ปฏิบัติตาม หน่วยงานที่กำกับดูแลรายงานปัญหาดังกล่าวต่อคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และคณะกรรมการก็จะแจ้งให้แก่ผู้บริหารระดับสูงสุดของหน่วยงานเพื่อใช้อำนาจในทางบริหาร สั่งการไปยังหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้น เพื่อให้ดำเนินการแก้ไขจนได้มาตรฐานโดยเร็ว โดยไม่จำกัดว่าโครงสร้างพื้นฐานนั้นจะเป็นหน่วยงานของรัฐหรือของ

[244] มาตรา 13 (4) พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

[245] มาตรา 20 พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

[246] มาตรา 22 (8) พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

[247] มาตรา 43 พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

[248] มาตรา 43 พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

เอกชน[249] และยังมีหน้าที่ในการจัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ทั้งโดยผู้ตรวจสอบภายในหรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละหนึ่งครั้ง[250]

ในกรณีที่มีภัยคุกคามทางไซเบอร์เกิดขึ้นต่อโครงสร้างพื้นฐานสำคัญ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ก็มีหน้าที่จะต้องรายงานหน่วยงานที่ควบคุมหรือกำกับดูแลตนโดยเร็ว เพื่อให้หน่วยงานนั้นทำหน้าที่สนับสนุนและให้ความช่วยเหลือต่อไป[251] โดยหากหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศใดไม่ปฏิบัติตามโดยไม่มีเหตุอันควรจะมีโทษปรับไม่เกิน 200,000 บาท[252]

ภัยคุกคามทางไซเบอร์ซึ่งอาจเกิดขึ้นต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศสามารถแบ่งได้ 3 ระดับดังนี้[253]

1. ภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง หมายถึง ภัยคุกคามทางไซเบอร์ที่มีความเสี่ยง อย่างมีนัยสำคัญถึงระดับที่ทำให้ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศด้อยประสิทธิภาพลง

2. ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง หมายถึง ภัยคุกคามที่มีลักษณะการเพิ่มขึ้นอย่างมีนัยสำคัญของการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์ โดยมุ่งหมาย เพื่อโจมตีโครงสร้างพื้นฐานสำคัญของประเทศและการโจมตีดังกล่าวมีผลทำให้ โครงสร้างสำคัญทางสารสนเทศที่เกี่ยวข้องกับการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศ ความมั่นคงของรัฐ ความสัมพันธ์ระหว่างประเทศ การป้องกันประเทศ เศรษฐกิจ การสาธารณสุข ความปลอดภัยสาธารณะ หรือความสงบเรียบร้อยของประชาชนเสียหาย จนไม่สามารถทำงานหรือ ให้บริการได้

3. ภัยคุกคามทางไซเบอร์ในระดับวิกฤติ หมายถึง ภัยคุกคามทางไซเบอร์ในระดับวิกฤติที่มีลักษณะเป็นภัยคุกคามทางไซเบอร์ที่เกิดจากการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ในระดับที่สูงขึ้นกว่าภัยคุกคามทางไซเบอร์ในระดับร้ายแรง โดยส่งผลกระทบรุนแรงต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศในลักษณะที่เป็นวงกว้าง จนทำให้การทำงานของหน่วยงานรัฐหรือการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศที่ให้กับประชาชนล้มเหลวทั้งระบบ จนรัฐไม่สามารถควบคุมการทำงานส่วนกลางของระบบคอมพิวเตอร์ของรัฐได้ หรือการใช้มาตรการเยียวยาตามปกติในการแก้ไขปัญหาภัยคุกคามไม่สามารถแก้ไขปัญหาได้และมีความเสี่ยงที่จะลุกลามไปยังโครงสร้างพื้นฐานสำคัญอื่นๆ ของประเทศ ซึ่งอาจมีผลทำให้บุคคลจำนวนมากเสียชีวิตหรือระบบคอมพิวเตอร์ คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์จำนวนมากถูกทำลายเป็นวงกว้างในระดับประเทศ

---

[249] มาตรา 53 พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

[250] มาตรา 54 พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

[251] มาตรา 57 และ 58 พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

[252] มาตรา 73 พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

[253] มาตรา 60 พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

หากปรากฏว่าภัยคุกคามทางไซเบอร์ที่เกิดขึ้นต่อระบบโครงสร้างพื้นฐานเป็นภัยคุกคามไซเบอร์ในระดับร้ายแรง หรือในระดับวิกฤติ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติจะมีอำนาจหน้าที่เพิ่มขึ้นตามกฎหมายฉบับนี้ ทั้งนี้ อำนาจบางประการอาจต้องใช้คำสั่งศาลก่อนจึงจะสามารถใช้อำนาจตามกฎหมายนั้นได้

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เป็นหัวใจหลักของการการปกป้องระบบโครงสร้างพื้นฐานสำคัญของประเทศไทย ซึ่งบังคับให้หน่วยงานไม่ว่าจะภาครัฐหรือเอกชนที่มีภารกิจหรือกิจการเกี่ยวข้องกับระบบโครงสร้างพื้นฐานสำคัญของประเทศมีหน้าที่ต้องจัดให้มีมาตรฐานขั้นต่ำในการบริหารจัดการภยันตรายที่จะเกิดแก่ระบบโครงสร้างพื้นฐาน และจะให้มีการตรวจสอบรายปี ซึ่งหากไม่ปฏิบัติตามหน่วยงานที่มีหน้าที่กำกับดูแลก็สามารถทำการร้องเรียนแก่ผู้ที่มีอำนาจสูงสุดของหน่วยงานนั้น เพื่อสั่งให้แก้ไขโดยเร็วก็ได้ แต่ก็ไม่ได้มีโทษอาญาแต่อย่างใด หากไม่ปฏิบัติตามคำสั่งนั้น

กฎหมายนี้จะมีสภาพบังคับ 2 กรณี คือ ประการแรก เมื่อเกิดภัยคุกคามทางไซเบอร์ต่อโครงสร้างพื้นฐานสำคัญ และหน่วยงานโครงสร้างพื้นฐานสำคัญละเลยไม่รายงานหน่วยงานที่ควบคุมหรือกำกับดูแล โดยไม่มีเหตุอันควร จึงจะมีโทษปรับ ประการถัดมาคือ หากเกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรงขึ้น แต่หน่วยงานโครงสร้างพื้นฐานกลับไม่ได้ให้ความร่วมมือ หรือปรับปรุงแก้ไขมาตรฐานความปลอดภัย จึงจะมีโทษปรับและโทษจำคุก

หากเปรียบเทียบเรื่องการคุ้มครองระบบโครงสร้างพื้นฐานของประเทศไทยกับประเทศจีน สหรัฐอเมริกา สหภาพยุโรป จะพบว่ากฎหมายเกี่ยวกับการกำหนดให้มีมาตรฐานขั้นต่ำในการบริหารจัดการความเสี่ยงที่อาจเกิดต่อระบบโครงสร้างพื้นฐานของไทยมีลักษณะคล้ายกับแนวทางของสหรัฐอเมริกาและสหภาพยุโรป กล่าวคือไม่มีสภาพบังคับหรือโทษอาญาแต่อย่างใด หากหน่วยงานใดไม่ได้จัดให้มีขึ้น และมีหน่วยงานรัฐเป็นผู้ออกแนวทางหรือคู่มือให้เอกชนนำไปปรับใช้หรือปฏิบัติตาม อย่างไรก็ดี หากปรากฏว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้นต่อระบบโครงสร้างพื้นฐานสำคัญและไม่มีการแจ้งสถานการณ์ที่เกิดขึ้นต่อหน่วยงานรัฐ หรือในกรณีที่มีภัยคุกคามทางไซเบอร์เกิดขึ้นต่อระบบโครงสร้างพื้นฐานสำคัญในระดับร้ายแรง และผู้มีอำนาจตามกฎหมายนี้ได้สั่งให้แก้ไขมาตรฐานความปลอดภัย แต่หน่วยงานนั้นกลับละเลย กรณีทั้งสองนี้จึงจะมีโทษอาญาเช่นเดียวกับกฎหมายของจีน

5.3 การเก็บรวบรวมข้อมูลไว้ภายในท้องที่

กฎหมายที่กล่าวถึง การเก็บรวบรวมข้อมูลไว้ภายในท้องที่ถูกบัญญัติไว้ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยข้อมูลที่จะถูกคุ้มครองตามกฎหมายฉบับนี้ได้แก่ ข้อมูลส่วนบุคคล ซึ่ง

กฎหมายฉบับนี้ได้ให้นิยามว่าเป็น “ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ”[254]

การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศได้ถูกกำหนดไว้ว่าจะทำได้ก็ต่อเมื่อประเทศปลายทางที่ข้อมูลโอนไปนั้นมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ อย่างไรก็ดี หลักนี้อาจถูกยกเว้นได้หากปรากฏเหตุตามกฎหมายดังต่อไปนี้คือ[255]

1. เป็นการปฏิบัติตามกฎหมาย

2. ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลโดยได้แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอของประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลแล้ว

3. เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น

4. เป็นการกระทำตามสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับบุคคลหรือนิติบุคคลอื่น เพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

5. เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของเจ้าของข้อมูลส่วนบุคคล หรือบุคคลอื่น เมื่อเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมในขณะนั้นได้

6. เป็นการจำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะที่สำคัญ

ทั้งนี้ หากผู้ควบคุมข้อมูลใดไม่ปฏิบัติตาม ก็จะได้รับปรับ หรือจำคุก แล้วแต่กรณี[256]

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศได้ถูกกำหนดไว้ว่าจะทำได้ก็ต่อเมื่อประเทศปลายทางที่ข้อมูลโอนไปนั้นมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ หลักการนี้ก็เป็นหลักการเดียวกันกับกฎหมายของสหภาพยุโรป ทว่า กฎหมายไทยมีความพิเศษอยู่คือ การโอนข้อมูลส่วนบุคคลไปยังประเทศที่ไม่มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอก็อาจทำได้เช่นกัน หากเข้าเหตุยกเว้นตามที่กฎหมายกำหนดไว้[257] ซึ่งไม่ปรากฏว่ากฎหมายของสหรัฐอเมริกา สหภาพยุโรป หรือประเทศจีนจะมีเหตุยกเว้นเหล่านี้แต่อย่างใด

---

[254] มาตรา 6 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[255] มาตรา 28 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[256] โปรดดูมาตรา 79 83 และ 84 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[257] เหตุเหล่านั้นได้แก่

1. เป็นการปฏิบัติตามกฎหมาย

2. ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลโดยได้แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอของประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลแล้ว

5.4 การรับรองมาตรฐานความปลอดภัยและการตรวจสอบ

ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ได้กำหนดให้“หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ” ซึ่งหมายถึงหน่วยงานของรัฐหรือหน่วยงานเอกชนใดที่ได้ให้บริการโครงสร้างพื้นฐานสำคัญมีหน้าที่ในการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยประมวลแนวทางดังกล่าวนั้นต้องประกอบด้วยแผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยผู้ตรวจประเมิน ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปีละหนึ่งครั้ง[258] ทว่า ถึงแม้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะเป็นผู้จัดทำประมวลแนวทางปฏิบัติเพื่อใช้ตรวจสอบตนเองนั้นเอง แต่เนื้อหาดังกล่าวก็ต้องสอดคล้องกับข้อกำหนดขั้นต่ำที่คณะกรรมการการกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ได้กำหนดไว้ด้วย[259] ซึ่งในปัจจุบัน ยังไม่มีมาตรฐานขั้นต่ำกำหนดไว้

นอกจากนี้ หากปรากฏว่าประมวลแนวทางของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศไม่ได้มาตรฐาน คณะกรรมการการกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ก็จะมีอำนาจในการสั่งให้ผู้มีอำนาจหรือผู้บริหารจัดการแก้ไขให้เป็นมาตรฐานโดยเร็ว[260] ทว่า ไม่ปรากฏว่าหากไม่ปฏิบัติตามแล้วจะมีโทษอาญาแต่อย่างใดหากไม่ปฏิบัติตาม เว้นแต่จะปรากฏในภายหลังว่าเกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรงแล้วหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศก็ไม่ได้ให้ความร่วมมือ หรือปรับปรุงแก้ไขให้ถูกต้อง จึงจะมีโทษปรับและโทษจำคุก[261]

อนึ่ง สำหรับเรื่องการรับรองว่าการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศใดได้มาตรฐานหรือไม่นั้น กฎหมายก็ให้อำนาจหน้าที่แก่คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติในการเป็นผู้รับรอง[262]

---

3. เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือ เพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น

4. เป็นการกระทำตามสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับบุคคลหรือนิติบุคคลอื่น เพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

5. เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของเจ้าของข้อมูลส่วนบุคคล หรือบุคคลอื่น เมื่อเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมในขณะนั้นได้

6. เป็นการจำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะที่สำคัญ

[258] มาตรา 44 พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

[259] มาตรา 13 (4) พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

[260] มาตรา 53 พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

[261] มาตรา 75 และ 76 พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

[262] มาตรา 9 (4) พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ได้กำหนดให้หน่วยงานที่มีกิจการหรือภารกิจเกี่ยวกับระบบโครงสร้างพื้นฐานสำคัญเท่านั้นที่ต้องจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และจัดทำประเมินปีละหนึ่งครั้ง โดยคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเป็นผู้มีอำนาจหน้าที่ในการรับรองมาตรฐาน อย่างไรก็ดี มีข้อสังเกตสองประการคือ ประการที่หนึ่ง การไม่จัดทำมาตรฐานดังกล่าวไม่มีโทษอาญาแต่อย่างใด จนกว่าจะเกิดภัยคุกคามไซเบอร์ระดับร้ายแรงขึ้นและผู้มีอำนาจได้สั่งให้แก้ไข ประการถัดมา กฎหมายฉบับนี้ ได้พูดถึงหน้าที่ของคณะกรรมการในการกำหนดมาตรฐานและตรวจสอบความปลอดภัยไซเบอร์ของตัวระบบแต่เพียงเท่านั้น แต่ไม่ได้กล่าวถึงตัวอุปกรณ์ที่ใช้ในกิจการนั้นๆ แต่อย่างใด

สำหรับกฎหมายของสหรัฐอเมริกาและสหภาพยุโรป หน่วยงานของรัฐนอกจากจะมีบริการรับรองมาตรฐานความปลอดภัยและการตรวจสอบรักษาความปลอดภัยให้แล้ว พันธกิจของหน่วยงานนั้นๆ ยังรวมไปถึงการตรวจสอบและรับรองมาตรฐานของอุปกรณ์ที่ใช้ในกิจการงานนั้นๆ ด้วย โดยไม่จำกัดว่าระบบรักษาความปลอดภัยหรืออุปกรณ์นั้นจะใช้ในระบบโครงสร้างพื้นฐานสำคัญหรือไม่ แต่กฎหมายไม่มีสภาพบังคับหากใช้สิ่งที่ไม่ได้ผ่านการรับรองมาตรฐาน ในทางตรงกันข้าม ประเทศจีนกลับบังคับให้ระบบรักษาความปลอดภัยทุกระบบและอุปกรณ์ทุกชิ้น ไม่ว่าจะใช้ในกิจการใด ต้องผ่านการรับรองจากรัฐก่อนเสมอ ดังนั้นอาจสรุปได้ว่ากฎหมายเรื่องการรับรองมาตรฐานความปลอดภัยและการตรวจสอบของประเทศไทยมีความคล้ายคลึงกับกฎหมายของสหรัฐอเมริกาและสหภาพยุโรปมากกว่า แต่ยังมีความแตกต่างกันบ้างในเรื่องขอบเขตงานว่าจะรวมไปถึงการตรวจสอบตัวอุปกรณ์ด้วยหรือไม่

5.5 การคุ้มครองข้อมูลส่วนบุคคล

จากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 คำว่าข้อมูลส่วนบุคคล หมายถึง “ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ”[263] และมีบุคคลอีกสองประเภทซึ่งมีส่วนเกี่ยวข้องกับข้อมูลส่วนบุคคลได้แก่ “ผู้ควบคุมข้อมูลส่วนบุคคล” ซึ่งได้แก่ บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจ เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล[264] และ “ผู้ประมวลผลข้อมูลส่วนบุคคล” ซึ่งได้แก่ บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล[265]

---

[263] มาตรา 6 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[264] เรื่องเดียวกัน.

[265] เรื่องเดียวกัน.

เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลเกิดขึ้นได้ กฎหมายได้บัญญัติหน้าที่ให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล ดังต่อไปนี้

1. ผู้ควบคุมข้อมูลส่วนบุคคลจะกระทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไม่ได้ หากเจ้าของข้อมูลส่วนบุคคลไม่ได้ให้ความยินยอมไว้ก่อนหรือในขณะนั้น[266] โดยการขอความยินยอมต้องทำโดยชัดแจ้ง เป็นหนังสือหรือทำโดยผ่านระบบอิเล็กทรอนิกส์[267] โดยการขอความยินยอมนั้น ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งไปยังเจ้าของข้อมูลส่วนบุคคลด้วยว่าจะทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นไปเพื่อวัตถุประสงค์ใด ด้วยภาษาที่อ่านง่ายและชัดเจน ทั้งนี้การขอความยินยอมนั้นจะต้องแยกออกมาจากข้อความอื่น ๆ ด้วย[268]

อนึ่ง ผู้ควบคุมข้อมูลส่วนบุคคลอาจทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลได้ แม้ปราศจากความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ถ้าหากกฎหมายนี้หรือกฎหมายอื่นกำหนดให้ทำได้[269]

2. ในการเข้าทำสัญญาหรือให้บริการใดๆ ผู้ควบคุมข้อมูลส่วนบุคคลต้องไม่ขอความยินยอมเพื่อเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ไม่มีความจำเป็นในการเข้าทำสัญญาหรือการให้บริการนั้น ๆ[270]

3. ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลจะขอความยินยอมเจ้าของข้อมูลส่วนบุคคลในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล หากปรากฏว่าเจ้าของข้อมูลเป็นผู้ไร้ความสามารถในการทำนิติกรรมตามกฎหมาย การขอความยินยอมอาจต้องปฏิบัติตามหลักเกณฑ์ ดังต่อไปนี้

1.) เจ้าของข้อมูลส่วนบุคคลเป็นผู้เยาว์ที่มีอายุตั้งแต่สิบปีขึ้นไป หากปรากฏว่าการให้ความยินยอมของผู้เยาว์นั้นไม่เกี่ยวข้องกับการใดๆ ซึ่งผู้เยาว์อาจให้ความยินยอมได้โดยลำพังได้ตามที่บัญญัติไว้ในมาตรา 22[271] มาตรา 23[272] หรือมาตรา 24[273] แห่งประมวลกฎหมายแพ่งและพาณิชย์ และผู้เยาว์ประสงค์จะให้ความยินยอมในการดังกล่าว ก็จะต้องได้รับความยินยอมจากผู้ใช้อำนาจปกครอง[274]

---

[266] มาตรา 19 วรรคหนึ่ง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[267] มาตรา 19 วรรคสอง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[268] มาตรา 19 วรรคสาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[269] มาตรา 19 วรรคหนึ่ง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[270] มาตรา 19 วรรคสี่ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[271] มาตรา 22 ประมวลกฎหมายแพ่งและพาณิชย์ “ผู้เยาว์อาจทำการใด ๆ ได้ทั้งสิ้น หากเป็นเพียงเพื่อจะได้ไปซึ่งสิทธิอันใดอันหนึ่ง หรือเป็นการเพื่อให้หลุดพ้นจากหน้าที่อันใดอันหนึ่ง”

[272] มาตรา 23 ประมวลกฎหมายแพ่งและพาณิชย์ “ผู้เยาว์อาจทำการใด ๆ ได้ทั้งสิ้น ซึ่งเป็นการต้องทำเองเฉพาะตัว”

[273] มาตรา 24 ประมวลกฎหมายแพ่งและพาณิชย์ “ผู้เยาว์อาจทำการใด ๆ ได้ทั้งสิ้น ซึ่งเป็นการสมแก่ฐานานุรูปแห่งตนและเป็นการอันจำเป็นในการดำรงชีพตามสมควร”

[274] มาตรา 20 (1) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

2.) เจ้าของข้อมูลส่วนบุคคลเป็นผู้เยาว์อายุต่ำกว่าสิบปี คนไร้ความสามารถ หรือคนเสมือนไร้ความสามารถ ผู้ควบคุมข้อมูลต้องขอความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์ ผู้อนุบาลที่มีอำนาจกระทำการแทนคนไร้ความสามารถ หรือผู้พิทักษ์ที่มีอำนาจกระทำการแทนคนเสมือนไร้ความสามารถเท่านั้น ไม่สามารถขอกับเจ้าของข้อมูลส่วนบุคคลนั้นได้เองโดยตรง[275]

4. ผู้ควบคุมข้อมูลส่วนบุคคลต้องทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ได้แจ้งเจ้าของข้อมูลส่วนบุคคลไว้ก่อนหรือในขณะที่เก็บรวบรวม อนึ่ง หากผู้ควบคุมข้อมูลส่วนบุคคลจะทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนอกขอบวัตถุประสงค์ที่ได้แจ้งเจ้าของข้อมูลส่วนบุคคลนั้น ผู้ควบคุมข้อมูลส่วนบุคคลจะทำได้ก็ต่อเมื่อตรงตามเงื่อนไขข้อใดข้อหนึ่งดังนี้[276]

1.) ผู้ควบคุมข้อมูลส่วนบุคคลได้แจ้งวัตถุประสงค์ใหม่แก่เจ้าของข้อมูล และได้รับความยินยอมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลแล้ว

2.) กฎหมายนี้หรือกฎหมายอื่นกำหนดให้ทำได้

ประเด็นที่น่าสนใจสำหรับการวิเคราะห์กฎหมายฉบับนี้ คือหลักการที่ว่าผู้ควบคุมข้อมูลส่วนบุคคลจะกระทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไม่ได้โดยปราศจากความยินยอมของเจ้าของข้อมูลส่วนบุคคล ซึ่งมีข้อยกเว้นว่าอาจทำการข้างต้นได้ หากมีกฎหมายนี้หรือกฎหมายอื่นให้อำนาจไว้ โดยจากที่พบได้คือพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้บัญญัติถึงสิทธิและวิธีการเก็บข้อมูลส่วนบุคคลไว้ไม่ต่างจากกฎหมายของสหภาพยุโรปมากนัก ซึ่งอาจทำให้เข้าใจได้ว่าประเทศไทยต้องการให้เกิดการไหลเวียนเสรีทางข้อมูลระหว่างสหภาพยุโรปและไทย เนื่องจากตามกฎหมายของสหภาพยุโรปแล้ว หากประเทศปลายทางที่โอนข้อมูลไปนั้นมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่ด้อยกว่าสหภาพยุโรป การโอนข้อมูลส่วนบุคคลไปมาหากันอาจจะทำไม่ได้เลย และกลายเป็นอุปสรรคสำหรับภาคธุรกิจ

อย่างไรก็ดี แม้ประเทศไทยจะมีกฎหมายคุ้มครองข้อมูลส่วนบุคคลแล้วก็ตาม แต่ก็มีกฎหมายหลายฉบับที่เป็นข้อยกเว้นของกฎหมายฉบับนี้ด้วย เช่น พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 หรือพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ที่มอบอำนาจให้ฝ่ายบริหารสามารถขอให้ผู้ให้บริการทางเครือข่ายส่งมอบข้อมูลที่ตนเองต้องการมาได้ หากเป็นไปเพื่อยับยั้งความผิดเกี่ยวกับคอมพิวเตอร์ ความผิดเกี่ยวกับความมั่นคง หรือความผิดอื่นๆ โดยผู้ให้บริการต้องส่งมอบข้อมูลระบุตัวตนผู้ที่เข้าสู่ระบบคอมพิวเตอร์ไปให้ ซึ่งแท้จริงแล้ว ข้อมูลนั้นก็คือข้อมูลส่วนบุคคลนั่นเอง หรือตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ที่มอบอำนาจให้ ได้แก่ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติในการเข้าถึงข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูล

[275] มาตรา 20 (2) มาตรา 20 วรรคสามและสี่ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[276] มาตรา 21 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

อื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทำสำเนา หรือสกัดคัดกรองข้อมูลสารสนเทศหรือโปรแกรมคอมพิวเตอร์ ซึ่งมีเหตุอันควรเชื่อได้ว่าเกี่ยวข้อง ดังนั้นข้อมูลส่วนบุคคลก็อาจมีความเสี่ยงที่จะถูกคุกคามได้เช่นกัน

ด้วยเหตุนี้ ถึงแม้ว่าประเทศไทยจะจัดให้มีพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เพื่อให้มาตรฐานการคุ้มครองข้อมูลส่วนบุคคลในประเทศสอดคล้องกับกฎหมายของสหภาพยุโรปแล้วก็ตาม อย่างไรก็ดี ด้วยความที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีข้อยกเว้นเป็นกฎหมายอื่นหลายฉบับ โดยเฉพาะอย่างยิ่งที่เป็นกฎหมายที่อ้างเหตุผลด้านความมั่นคงและให้อำนาจฝ่ายบริหารได้โดยปราศจากการใช้คำสั่งศาล กรณีจึงเป็นที่น่าสงสัยว่าพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลจะใช้ได้อย่างมีประสิทธิภาพและตรงตามมาตรฐานขั้นต่ำตามที่กฎหมายของสหภาพยุโรปกำหนดไว้หรือไม่

5.6 ถอดบทเรียนสำหรับการกำกับดูแลเศรษฐกิจดิจิทัลในยุคไทยแลนด์ 4.0

5.6.1 บทเรียนด้านกฎหมาย

จากการศึกษาเปรียบเทียบข้างต้น สามารถสรุปว่าในแต่ละประเด็น ประเทศไทยเลือกเดินตามโมเดลกฎหมายประเทศใด ดังนี้

หัวข้อ	ประเทศไทยใช้โมเดลกฎหมายประเทศใด
หน้าที่ตามกฎหมายของผู้ให้บริการทางเครือข่าย	**โมเดลจีน** โดยหน้าที่สำคัญของผู้ให้บริการทางเครือข่ายเป็นหน้าที่การช่วยเหลือรัฐในการป้องปรามการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ส่วนนี้ไม่มีในกฎหมายสหภาพยุโรปและกฎหมายสหรัฐอเมริกา) อย่างไรก็ตาม ในกฎหมายไทย ไม่มีมาตราใดหรือกฎหมายอื่นใดที่กล่าวถึงหน้าที่ของผู้ให้บริการในการเสริมสร้างระบบการรักษาความปลอดภัยของตน ซึ่งเป็นส่วนที่มีทั้งในกฎหมายจีนและกฎหมายของสหภาพยุโรป
การปกป้องระบบโครงสร้างพื้นฐานสำคัญ	**โมเดลสหรัฐอเมริกาและโมเดลสหภาพยุโรป** โดยกฎหมายเกี่ยวกับการกำหนดให้มีมาตรฐานขั้นต่ำในการบริหารจัดการความเสี่ยงที่อาจเกิดต่อระบบโครงสร้างพื้นฐานของไทยไม่มีสภาพบังคับหรือโทษอาญาแต่อย่างใด หากหน่วยงานใดไม่ได้จัดให้มีขึ้นและมีหน่วยงานรัฐเป็นผู้ออกแนวทางหรือคู่มือให้เอกชนนำไปปรับใช้หรือปฏิบัติตาม **โมเดลจีน** กฎหมายไทยกำหนดโทษอาญาเช่นเดียวกับกฎหมายของจีนเฉพาะในสองกรณี ได้แก่ หากปรากฏว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้นต่อระบบโครงสร้างพื้นฐานสำคัญและไม่มีการแจ้งสถานการณ์ที่เกิดขึ้นต่อหน่วยงานรัฐ หรือในกรณีที่มีภัยคุกคามทางไซเบอร์เกิดขึ้นต่อระบบโครงสร้างพื้นฐานสำคัญในระดับร้ายแรง และผู้มีอำนาจตามกฎหมายนี้ได้สั่งให้แก้ไขมาตรฐานความปลอดภัย

หัวข้อ	ประเทศไทยใช้โมเดลกฎหมายประเทศใด
การเก็บรวบรวมข้อมูลไว้ภายในท้องที่	**โมเดลสหภาพยุโรป** ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศได้ถูกกำหนดไว้ว่าจะทำได้ก็ต่อเมื่อประเทศปลายทางที่ข้อมูลโอนไปนั้นมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ อย่างไรก็ตาม กฎหมายไทยมีความพิเศษอยู่คือ การโอนข้อมูลส่วนบุคคลไปยังประเทศที่ไม่มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอก็อาจทำได้เช่นกัน หากเข้าเหตุยกเว้นตามที่กฎหมายกำหนดไว้ ซึ่งไม่ปรากฏว่ากฎหมายของสหรัฐอเมริกา สหภาพยุโรป หรือประเทศจีนจะมีเหตุยกเว้นเหล่านี้แต่อย่างใด
การรับรองมาตรฐานความปลอดภัยและการตรวจสอบ	**โมเดลสหรัฐอเมริกาและโมเดลสหภาพยุโรป** หน่วยงานของรัฐนอกจากจะมีบริการรับรองมาตรฐานความปลอดภัยและการตรวจสอบรักษาความปลอดภัยให้แล้ว พันธกิจของหน่วยงานนั้นๆ ยังรวมไปถึงการตรวจสอบและรับรองมาตรฐานของอุปกรณ์ที่ใช้ในกิจการงานนั้นๆ ด้วย โดยไม่จำกัดว่าระบบรักษาความปลอดภัยหรืออุปกรณ์นั้นจะใช้ในระบบโครงสร้างพื้นฐานสำคัญหรือไม่ แต่กฎหมายไม่มีสภาพบังคับหากใช้สิ่งที่ไม่ได้ผ่านการรับรองมาตรฐาน อย่างไรก็ตาม กฎหมายไทยมีความแตกต่างกันในเรื่องขอบเขตงานว่าจะรวมไปถึงการตรวจสอบตัวอุปกรณ์ด้วยหรือไม่
การคุ้มครองข้อมูลส่วนบุคคล	**โมเดลสหภาพยุโรป** พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลในประเทศสอดคล้องกับกฎหมายของสหภาพยุโรป **โมเดลจีน** พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีข้อยกเว้นเป็นกฎหมายอื่นหลายฉบับ

หัวข้อ	ประเทศไทยใช้โมเดลกฎหมายประเทศใด
	โดยเฉพาะอย่างยิ่งที่เป็นกฎหมายที่อ้างเหตุผลด้านความมั่นคงและให้อำนาจฝ่ายบริหารได้โดยปราศจากการใช้คำสั่งศาล

หากสรุปในภาพกว้าง จะเห็นว่า แนวคิดด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของสหรัฐอเมริกา อยู่ที่การรักษาโครงสร้างพื้นฐานอินเทอร์เน็ต ในขณะที่แนวคิดด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของจีนอยู่ที่การรักษาความมั่นคงของรัฐ ส่วนแนวคิดด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของยุโรปมุ่งไปที่การคุ้มครองดูแลผู้ใช้งาน โดยเน้นความปลอดภัยและการรักษาข้อมูลส่วนบุคคล จากการศึกษา เห็นได้ชัดเจนว่า โมเดลกฎหมายจีนเริ่มมีอิทธิพลต่อการบัญญัติกฎหมายของประเทศไทยในการกำกับดูแลเศรษฐกิจดิจิทัลในยุคไทยแลนด์ 4.0 ถึงแม้ว่าในทางรูปแบบและเนื้อหาของกฎหมายส่วนใหญ่ จะมีความพยายามยึดตามโมเดลของสหภาพยุโรปและสหรัฐอเมริกา แต่ก็มีการสอดแทรกเนื้อหาหรือลักษณะเด่นของโมเดลจีนด้วย อาทิ ในประเด็นหน้าที่ทางกฎหมายของผู้ให้บริการทางเครือข่าย ซึ่งมีลักษณะคล้ายกฎหมายจีน การปกป้องระบบโครงสร้างพื้นฐานสำคัญ ซึ่งมีการกำหนดโทษอาญาในสองกรณี รวมทั้งการคุ้มครองข้อมูลส่วนบุคคล ซึ่งแม้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะบัญญัติมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลในประเทศสอดคล้องกับกฎหมายของสหภาพยุโรป แต่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ก็มีข้อยกเว้นเป็นกฎหมายอื่นหลายฉบับ โดยเฉพาะอย่างยิ่งที่เป็นกฎหมายที่อ้างเหตุผลด้านความมั่นคงและให้อำนาจฝ่ายบริหารได้โดยปราศจากการใช้คำสั่งศาล

ขณะเดียวกัน ก็มีข้อสังเกตที่น่าสนใจว่า ในประเทศตะวันตกเอง ก็เริ่มมีกระแสการเดินตามโมเดลจีนบ้างเช่นกัน เนื่องจากความกังวลเรื่องภัยคุกคามต่อความมั่นคง การแข่งขันทางเทคโนโลยีระหว่างมหาอำนาจและความปลอดภัยทางไซเบอร์ ดังนั้น เส้นการแบ่งแยกที่ชัดเจนระหว่างสำนัก Cyber Paternalism ตามแนวจีน กับสำนัก Cyber Commons ตามแนวตะวันตก อาจไม่สามารถแบ่งได้ชัดเจนดังเช่นในอดีต โดยจะมีความซับซ้อนมากขึ้นตามแต่ละประเด็นกฎหมาย รวมทั้งจะมีแนวโน้มเป็นเรื่องของระดับการที่รัฐเข้ามากำกับดูแลไซเบอร์สเปซมากกว่าเรื่องว่ารัฐจะเข้ามากำกับหรือไม่ ตัวอย่างที่ชัดเจน เช่น กฎหมายการเข้ารหัสข้อมูลของประเทศออสเตรเลีย ซึ่งบังคับให้บริษัทผู้ให้บริการเทคโนโลยีคอมพิวเตอร์ยอมให้รัฐ ตำรวจ หรือข้าราชการในองค์การเกี่ยวกับความปลอดภัยเข้าถึงข้อมูลที่เข้ารหัสหรือเป็นความลับของผู้ใช้งานโดยที่ผู้ใช้งานไม่รู้ตัว เพื่อจัดการอาชญากรรม การก่อการร้าย และดูแลความมั่นคงของประเทศ หรือเช่นร่างกฎหมายรัฐบัญญัติความมั่นคงของชาติและการคุ้มครองข้อมูลส่วนบุคคล (National Security and Personal Data Protection Act) ของสหรัฐอเมริกา ซึ่งจะบังคับให้บริษัทต่าง ๆ ในสหรัฐอเมริกาต้องไม่ถ่ายโอนข้อมูลของพลเมืองอเมริกาที่เก็บได้ในประเทศไปเก็บไว้ที่ประเทศอื่นที่มีความน่ากังวล เช่น จีนหรือรัสเซีย อย่างไรก็ตาม จะเห็นว่าสหภาพยุโรป

ยังมีความชัดเจนในเรื่องอุดมการณ์ตามแนวทางของสำนัก Cyber Commons และมีมาตรฐานที่สูงกว่าสหรัฐอเมริกาในเรื่องการคุ้มครองข้อมูลส่วนบุคคลและการสร้างหลักประกันให้ไซเบอร์สเปซเป็นโลกเสรี

บทเรียนด้านกฎหมายที่สำคัญ คือ ในการวางแนวทางการกำกับดูแลเศรษฐกิจดิจิทัลในยุคไทยแลนด์ 4.0 จะต้องก้าวข้ามกรอบคิดว่าจะเลือกแบบสำนัก Cyber Paternalism ตามแนวจีน หรือสำนัก Cyber Commons ตามแนวตะวันตก แต่จะต้องพิจารณาถึงการสร้างสมดุลระหว่าง 2 แนวคิด ผ่านการออกแบบกลไกที่เหมาะสม และการออกแบบเกณฑ์หรือมาตรฐานที่จำกัดการใช้ดุลยพินิจของรัฐเกินสมควร ตัวอย่างเช่น ในกฎหมายการเข้ารหัสของออสเตรเลียนั้น เจ้าหน้าที่สามารถขอความช่วยเหลือจากผู้ให้บริการโดยต้องมีหมายศาล มีเกณฑ์ระบุชัดถึงเหตุผลของเจ้าหน้าที่ในการใช้อำนาจตามกฎหมาย และในทางเทคนิค เพียงบังคับให้ผู้ให้บริการสร้างช่องทางพิเศษไว้เตรียมพร้อม ซึ่งแตกต่างจากแนวทางของจีนที่ขาดกลไกในการจำกัดการใช้ดุลยพินิจของรัฐ เป็นที่น่าเสียดายว่า ในกฎหมายของไทยในส่วนที่คล้ายกับโมเดลจีน มักขาดการออกแบบกลไกหรือเกณฑ์ที่ชัดเจน แต่มักอาศัยการให้ดุลยพินิจแก่เจ้าหน้าที่รัฐด้วยภาษากฎหมายที่กำกวมและเปิดให้มีการตีความเพื่อใช้ดุลยพินิจได้อย่างกว้างขวาง ตัวอย่างเช่น ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งมีข้อยกเว้นเป็นกฎหมายที่อ้างเหตุผลด้านความมั่นคงและให้อำนาจฝ่ายบริหารได้โดยปราศจากการใช้คำสั่งศาล

5.6.2 บทเรียนด้านภูมิรัฐศาสตร์การเมืองและเทคโนโลยีระหว่างประเทศ และนัยยะต่อคนไทย 4.0

การศึกษากฎหมายความปลอดภัยทางไซเบอร์ของจีน สะท้อนแนวคิดที่เป็นเอกลักษณ์ของจีนเกี่ยวกับระบบการเมือง ระบบเศรษฐกิจ และความมุ่งมั่นที่จะกำกับดูแลเทคโนโลยีอินเตอร์เน็ตและไซเบอร์สเปซ โดยมองว่ามีความเชื่อมโยงโดยตรงกับความมั่นคงของรัฐจีน แนวคิดเหล่านี้สะท้อนภาพความเป็นจริงเกี่ยวกับภูมิรัฐศาสตร์การเมืองและเทคโนโลยีระหว่างประเทศในปัจจุบัน

จอร์จ โซรอส พ่อมดการเงินโลกได้กล่าวในงานเลี้ยงอาหารค่ำในการประชุม World Economic Forum ที่ดาวอส เมื่อเดือนมกราคม ค.ศ. 2019 ว่า นี่เป็นครั้งแรกในประวัติศาสตร์โลกที่มีเผด็จการที่มีเทคโลยีสมัยใหม่ในการควบคุมจัดการสังคมได้ในระดับสูง ด้วยการปรับใช้เทคโนโลยีไม่ว่าจะเป็นปัญญาประดิษฐ์ (AI) หรือ Big Data ซึ่งมีพื้นฐานคือโลกไซเบอร์สเปซ ทำให้พรรคคอมมิวนิสต์จีนมีเครื่องมือใหม่ในการควบคุมจัดการสังคม [277] จนนักวิเคราะห์หลายคนมองว่า พรรคคอมมิวนิสต์จีนกลายเป็นสถาบันการเมืองที่มั่นคงแข็งแรงที่สุดแห่งหนึ่งของโลก และมีกลไกที่รัดกุมในการควบคุมการใช้ไซเบอร์สเปซและเทคโนโลยียุคใหม่ที่เชื่อมโยงกับอินเตอร์เน็ตในการส่งเสริมระบบการปกครองและระบบเศรษฐกิจของจีนเอง [278]

[277] Soros, George. 2019. " Remarks delivered at the World Economic Forum". https://www.georgesoros.com/2019/01/24/remarks-delivered-at-the-world-economic-forum-2/.

[278] Larson, Christina. 2018. "Who need democracy when you have data". MIT Technology Review.

เทคโนโลยียุค 4.0 ไม่ว่าจะเป็น ปัญญาประดิษฐ์ (AI), Big Data, หรือสัญญาณ 5G ซึ่งในปัจจุบันจีนได้พัฒนาเทคโนโลยีเหล่านี้ขึ้นมาอย่างรวดเร็ว การแข่งขันระหว่างสหรัฐฯ กับจีนในเทคโนโลยีเหล่านี้ แตกต่างจากการแข่งขันระหว่างสหรัฐฯ กับสหภาพโซเวียตในเรื่องเทคโนโลยีอวกาศและเทคโนโลยีการทหารในอดีต เพราะเทคโนโลยีอวกาศและเทคโนโลยีการทหารนั้นไม่เกี่ยวกับชีวิตประจำวันของคนหมู่มาก แต่เทคโนโลยีสมัยใหม่ในยุค 4.0 นี้ ทุกคนใช้กันในชีวิตประจำวัน ดังที่วันนี้เรามีสมาร์ทโฟนกันคนละเครื่อง และอีกไม่นานก็จะถึงยุคที่ข้าวของเครื่องใช้ทุกอย่าง ไม่ว่าจะเป็นตู้เย็น โทรทัศน์ ลำโพง สามารถพูดคุยกับเราและเชื่อมต่อกับอินเทอร์เน็ตได้

การที่จีนกำลังก้าวขึ้นมาเทียบชั้นสหรัฐฯ ในเทคโนโลยีเหล่านี้ จึงมีมิติด้านความมั่นคงและเป็นภัยคุกคาม เพราะเกี่ยวข้องกับความปลอดภัยของข้อมูล และด้วยความเชื่อที่ว่า ใครที่เป็นเจ้าของแพลตฟอร์มต่างๆ ในอนาคต ย่อมเป็นมหาอำนาจทั้งในทางการเมืองและเศรษฐกิจ ซึ่งเดิมฝั่งตะวันตกได้แก่ยุโรปและสหรัฐฯ เป็นผู้นำในเชิงตลาดอุปกรณ์โครงข่ายและเครื่องรับส่งสัญญาณ 4G และแพลตฟอร์มบนอินเทอร์เน็ตไม่ว่าจะเป็น Google, Facebook, Amazon รวมทั้งแพลตฟอร์มที่เป็นฮาร์ดแวร์ ซอฟต์แวร์และอุปกรณ์เครื่องใช้ต่างๆ เช่น Apple, Microsoft แต่ในปัจจุบัน จีนเป็นชาติเดียวที่ขึ้นมาแข่งขันในแพลตฟอร์มบนอินเทอร์เน็ตเต็มตัว รวมทั้งยังมีแนวทางการกำกับดูแลไซเบอร์สเปซตามสำนักคิด Cyber Paternalism เพื่อเอื้อกับการส่งเสริมระบบการเมืองและระบบเศรษฐกิจของจีน ซึ่งแตกต่างจากแนวคิด Cyber Commons ดั้งเดิมของตะวันตก

สาเหตุที่จีนเป็นชาติเดียวที่ขึ้นมาแข่งขันในแพลตฟอร์มบนอินเตอร์เน็ตเต็มตัว แม้จะอยู่ในสำนักคิด Cyber Paternalism เนื่องด้วยปัจจัยด้านเศรษฐกิจการเมืองที่พิเศษของจีน อาทิ ระบบเศรษฐกิจที่มีเอกลักษณ์ของจีนที่รัฐมียุทธศาสตร์อินเตอร์เน็ตที่ชัดเจน การวางแผนสร้างระบบ Great Firewall ของจีนตั้งแต่เริ่มแรกที่ทำให้สามารถควบคุมอินเตอร์เน็ต รวมทั้งการใช้ประโยชน์จากตลาดขนาดใหญ่ และพลังสร้างสรรค์ของผู้ประกอบการแพลตฟอร์มบนอินเตอร์เน็ตของจีน ในขณะที่เมื่อมองย้อนกลับมาที่ไทย ซึ่งรับแนวความคิดสากลในเรื่องอินเตอร์เน็ต และไม่มีระบบ Great Firewall ตั้งแต่เริ่มต้น หากแต่มีแนวคิดต้องการที่จะรักษาและควบคุมอินเตอร์เน็ตตามโมเดลจีนในระยะหลัง ผลคือยากที่จะบังคับใช้กฎหมายได้ตามวัตถุประสงค์ดังเช่นในจีน ดังนั้น แม้ว่าไทยจะพยายามเดินตามโมเดลจีนในการกำกับดูแลความมั่นคงปลอดภัยทางไซเบอร์ แต่เนื่องจากไทยเองขาดปัจจัยด้านเศรษฐกิจการเมืองอื่นที่จีนมี ทำให้ไทยไม่มีศักยภาพที่จะแข่งขันในแพลตฟอร์มบนอินเตอร์เน็ตอย่างที่จีนทำได้

เบื้องหลังแพลตฟอร์มไซเบอร์สเปซของจีนก็คือ รัฐจีน ซึ่งสะท้อนอารยธรรม ระบบ ความคิดความเชื่อที่แตกต่างจากตะวันตก ถึงแม้ว่าหลายบริษัทข้างต้นจะเป็นบริษัทเอกชนจีน แต่กฎหมายความปลอดภัยทางไซเบอร์ของจีนบัญญัติไว้ชัดเจนว่าบริษัทเอกชนจีนต้องให้ความร่วมมือกับรัฐในเรื่องความมั่นคง รวมทั้งปัญหาที่ว่า บริษัทเทคโนโลยีจีนเหล่านี้ก้าวขึ้นมาได้ขนาดนี้ย่อมเป็นเพราะการช่วยเหลือ อุดหนุน และส่งเสริมจากรัฐบาลจีนทั้งในเรื่องแหล่งเงินทุนและการปิดกั้นต่างชาติผ่านกลไกกฎหมาย

คนไทย 4.0 จึงกำลังเผชิญกับโลกภูมิรัฐศาสตร์การเมืองและเทคโนโลยีระหว่างประเทศที่มีความซับซ้อน และแตกต่างจากโลกเดิมที่มีความเห็นร่วมกัน (Consensus) เกี่ยวกับไซเบอร์สเปซที่ค่อนข้างชัดเจนสำหรับคนไทย 4.0 ซึ่งต่อไปในทุกมิติของชีวิตย่อมมีความเกี่ยวข้องกับเทคโนโลยีอินเตอร์เน็ตอย่างหลีกเลี่ยงไม่ได้ ควรตระหนักว่าการเชื่อมโยงกับไซเบอร์สเปซมีมิติด้านความมั่นคงของรัฐเสมอ คำถามใหญ่ต่อไปก็คือ เราจะเป็นส่วนหนึ่งของแพลตฟอร์มสหรัฐฯ หรือจีน และไม่ว่าในประเด็นไหนหรือเทคโนโลยีใด เราจะกลายเป็นส่วนหนึ่งของแพลตฟอร์มของใครก็ตาม คำถามสำคัญถัดมาก็คือ เราจะแสวงหาแนวทางการกำกับดูแลที่เหมาะสมอย่างไร เพื่อประกันความปลอดภัยทางไซเบอร์และความมั่นคงของชาติ โดยสร้างสมดุลทั้งคุณค่าในเรื่องความมั่นคงของรัฐและคุณค่าเสรีนิยม

บรรณานุกรม

Allen-Ebrahimian, Bethany. 2015. "The 'Chilling Effect' Of China's New Cybersecurity Regime". Foreign Policy. https://foreignpolicy.com/2015/07/10/china-new-cybersecurity-law-internet-security/.

An, Bai Jie. 2017. "Xi's Guidance Focuses Push on Internet". Chinadaily. https://www.chinadaily.com.cn/china/2017-04/20/content_29003244.htm.

Auchard, Eric, and Tom Käckenhoff. 2016. "Thyssenkrupp Secrets Stolen In 'Massive' Cyber Attack". U.S. Reuters. https://www.reuters.com/article/us-thyssenkrupp-cyber/thyssenkrupp-secrets-stolen-in-massive-cyber-attack-idUSKBN13X0VW.

Australian Associated Press, "Chinese Cyber-Attack Launched on WA Government". 2020. 9NEWS. https://www.9news.com.au/national/chinese-cyberattack-blamed-for-hack-on-wa-government/f1de86d4-67a6-498e-a95d-3624727a6856#close.

Balke, Liudmyla. 2018. "China'S New Cybersecurity Law and U.S.-China Cybersecurity Issues". Santa Clara Law Review 58 (1): 141.

Battaglio, Stephen. 2020. "Celebrity Law Firm Won't Pay Ransom to Hackers Claiming to Have 'Dirty Laundry' On Trump". Los Angeles Times. https://www.latimes.com/entertainment-arts/business/story/2020-05-18/hackers-demand-42-million-to-keep-from-leaking-law-firms-stolen-data-on-president-trump.

Blinderman, Eric, and Myra Din. 2017. "Hidden by Sovereign Shadows: Improving the Domestic Framework for Deterring State-Sponsored Cybercrime". Vanderbilt Journal of Transnational Law 50: 889, 896-897.

Calfee, Bailey. 2020. "Bella Thorne Posted Her Own Nudes After Blackmail Threats". Nylon. https://www.nylon.com/bella-thorne-nudes-hacker-blackmail.

Carte, William A., and Daniel G. Sofio. 2017. "Cybersecurity Legislation And Critical Infrastructure Vulnerabilities". Foundations of Homeland Security, 223-224.

Chabinsky, Steven. 2019. "ICLG - Data Protection Laws and Regulations - USA Covers Relevant Legislation and Competent Authorities, Territorial Scope, Key Principles, Individual Rights, Registration Formalities, Appointment of A Data Protection Officer and Of

Processors - In 42 Jurisdictions". International Comparative Legal Guides International Business Reports. https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa.

Chander, Anupam, and Uyên P. Lê. 2015. "Data Nationalism". Emory Law Journal 64: 677, 680.

Chang, Amy. 2014. "Warring State: China's Cybersecurity Strategy". Center for A New American Security. https://www.cnas.org/publications/reports/warring-state-chinas-cybersecurity-strategy.

Cheng, Ron. 2016. "China Passes Long-Awaited Cyber Security Law". FORBES. https://www.forbes.com/sites/roncheng/2016/11/09/china -passes-long-awaited-cyber-security-law/#5924ea3f24d2.

Cloutier, Christopher T. 2012. "Casting A Wide Net: China's Encryption Restrictions". Worldecr. https://research.umbc.edu/files/2014/10/11-11WorldECRCloutierCohen.pdf.

Cohen, Bret, Britanie Hall, and Charlie Wood. 2017. "Data Localization Laws and Their Impact on Privacy, Data Security and The Global Economy". ANTITRUST 32 (1): 107,109.

Condron, Sean M. 2007. "Getting It Right: Protecting American Critical Infrastructure In Cyberspace". Harvard Journal of Law & Technology 20 (2): 407.

Daniel C. K. Chow. 2013. "How China Uses International Trade to Promote Its View of Human Rights." George Washington International Law Review 45. no. 4: 681-726.

Davies, Jamie. 2019. "US Government to Consider Strict Data Localisation Laws". Telecoms. https://telecoms.com/500992/us-government-to-consider-strict-data-localisation-laws/.

Department of Home Affairs. "The Assistance and Access Act 2018". 2020. Homeaffairs.Gov.Au. https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/data-encryption#:~:text=The%20Australian%20Government%20supports%20cyber,safe%20online%20environment%20for%20Australians.&text=it%20is%20estimated%20that%20by,investigative%20value%20will%20be%20encrypted.

Department of Homeland Security. 2020. "ABOUT CISA". Cisa.Gov. https://www.cisa.gov/about-cisa.

Department of Homeland Security. 2020. "Critical Infrastructure Sectors". Cisa.Gov. https://www.cisa.gov/critical-infrastructure-sectors.

Department of Homeland Security. 2020. "Critical Infrastructure Security". Cisa.Gov. https://www.dhs.gov/topic/critical-infrastructure-security.

Department of Homeland Security. 2020. "Infrastructure Security Division | CISA". Cisa.Gov. https://www.cisa.gov/infrastructure-security-division.

Eichensehr, Kristen. 2015. "The Cyber-Law of Nations". Georgetown Law Journal, 317, 346.

Engleman, Eric. 2011. "SOPA Bill Petition Collects 7 Million Signatures, According to Google". Washington Post. https://web.archive.org/web/20120120082947/http://www.washingtonpost.com/business/google-says-7-million-signed-petition-against-anti-piracy-bills/2012/01/19/gIQAJ2MiBQ_story.html?tid=pm_business_pop.

Ernst, Dieter, and Barry J. Naughton. 2008. "China's Emergent Political Economy Insights from The IT Industry". SSRN Electronic Journal, 39-59. doi:10.2139/ssrn.2742927.

European Commission. 2020. "The EU Cybersecurity Certification Framework - Shaping Europe’S Digital Future - European Commission". European Commission. https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework.

Ewen MacAskill. 2013. "NSA Files Decoded: Edward Snowden's Surveillance Revelations Explained". The Guardian.https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded.

Fisher, Christine. 2019. "Senate Bill Would Block US Companies from Storing Data in China". Engadget.Com. https://www.engadget.com/2019-11-18-national-security-personal-data-protection-act.html.

Fourkas, Vassilys. 2004. "WhatIs‘Cyberspace’?". Researchgate. https://www.researchgate.net/publication/328928631_What_is_'cyberspace'.

Funk, Matthew. 2015. "Tragedy of The Commons: Snowden'S Reformation and The Balkanization of The Internet". Syracuse Journal of Science and Technology Law 31: 49-52.

Gao, Charlotte. 2017. "China Fines Its Top 3 Internet Giants for Violating Cybersecurity Law". The Diplomat. https://thediplomat.com/2017/09/china-fines-its-top-3-internet-giants-for-violating-cybersecurity-law/.

Gierow, Hauke Johannes. 2015. "Cyber Security in China: Internet Security, Protectionism and Competitiveness: New Challenges to Western Businesses". China Moniter. https://www.merics.org/sites/default/files/2019-08/150407_MERICS%20China%20Monitor%2022_en.pdf.

Greenfield, Heather. 2017. "CCIA Highlights to Trump Administration Trade Barriers in China's Cybersecurity Law". Computer and Communications Industry Association: CCIA. https://www.ccianet.org/2017/06/ccia-highlights-to-trump-administration-trade-barriers-in-chinas-cybersecurity-law/.

Ho, Alexander. 2014. "Why China Is A Nightmare for American Internet Companies". TIME. https://time.com/10178/why-china-is-a-nightmare-for-american-internet-companies/.

Hoffmann, Richard. 2017. "Update: China Releases New Draft Regulations regarding Cyber Security of Online Services and Products". Ecovis BEIJING. http://www.ecovis-beijing.com/enfblog-en/articles/810-update-china.

Horwitz, Josh. 2017. "A Key Question at The Heart of China's Cybersecurity Law: Where Should Data Live?". Quartz. https://qz.com/999613/a-key-question-at-the-heart-of-chinas-cybersecurity-law-where-should-data-live/.

Iasiello, Emilio. 2017. "China's Cyber Initiatives Counter International Pressure". Journal of Strategic Security 10 (1): 9. doi:10.5038/1944-0472.10.1.1548.

Information Office of the State Council the People's Republic of China. 2010. "Govt. White Papers - The Internet in China". 2010. China.Org.Cn. http://www.china.org.cn/government/whitepaper/2010-06/08/content_20208007.htm.

Internet Governance Forum. 2020. "About The IGF". https://www.intgovforum.org/multilingual/tags/about.

Internet Society. 2020. "About Internet Society | Internet Society". Internet Society. https://www.internetsociety.org/about-internet-society/.

itnews. 2016. "China's New Cyber Security Laws Will 'Lock Out' Businesses". Nextmedia. https://www.itnews.com.au/news/chinas-new-cyber-security-laws-will-lock-out-businesses-440929.

Jacob Quinn. 2017. "A Peek Over the Great Firewall: A Breakdown of China'S New Cybersecurity Law". SMU Science & Technology Law Review 2 (20): 408-411.

Jiang, Min. 2010. "Authoritarian Informationalism: China's Approach to Internet Sovereignty". SAIS Review of International Affairs 30 (2): 71.

Jing, Catherine, and Amy Yin. 2018. "New Regulations on Cybersecurity: Release of Draft Regulations on The Cybersecurity Multi-Level Protection Scheme". Reedsmith. https://www.reedsmith.com/en/perspectives/2018/08/new-regulations-on-cyber-security.

Johnson, David R., and David G. Post. 1996. "Law and Borders - The Rise of Law in Cyberspace". Stanford Law Review 48: 1367, 1394.

Justia U.S. Supreme Court. "United States V. United States Dist. Ct., 407 U.S. 297 (1972)". 1972. Justia Law. https://supreme.justia.com/cases/federal/us/407/297/.

Kelley, Katherine W. 2017. "China's Cybersecurity Law Goes into Effect June 1, 2017—Are You Ready?". National Association of Corporate Directors. https://blog.nacdonline.org/posts/chinas-cybersecurity-law-goes-into-effect-june-1-2017-are-you-ready.

Larson, Christina. 2018. "Who need democracy when you have data". MIT Technology Review.

Law Library of Congress. "H.R.3261 - 112Th Congress (2011-2012): Stop Online Piracy Act". 2012. CONGRESS.GOV. https://www.congress.gov/bill/112th-congress/house-bill/3261.

Lee, Jyh-An, and Ching-Yi Liu. 2012. "Forbidden City Enclosed by The Great Firewall". Minnesota Journal of Law, Science, And Technology 13 (1): 148-150.

Lee, Jyh-An. 2014. "The Red Storm in Uncharted Waters: China and International Cyber Security". University of Missouri-Kansas City Law Review 8 (4): 951, 953.

Li, Pei. 2018. "Shanghai Temporarily Closes Marriott Website in China After Questionnaire Gaffe". U.S. Reuters. https://www.reuters.com/article/us-china-marriott/shanghai-temporarily-closes-marriott-website-in-china-after-questionnaire-gaffe-idUSKBN1F00UT.

Lindsay, Jon R. 2015. "The Impact of China on Cybersecurity: Fiction and Friction". International Security 39 (3): 7, 13.

McKune, Sarah. 2015. "Analysis of International Code of Conduct". The Citizen Lab. https://citizenlab.ca/2015/09/international-code-of-conduct/.

Miles, Tom. 2017. "U.S. Asks China Not to Enforce Cyber Security Law". REUTERS. http://www.reuters.com/article/us-usa-china-cyber-trade/u-s-asks-china-not-to-enforce-cyber-security-law-idUSKCNC11D1.

Moore, Stephen. 2014. "Cyber Attacks and The Beginnings of An International Cyber Treaty". North California Journal of International Law and Commercial Regulation 39 (1): 223, 253.

National Institute of Standards and Technolog. 2020. "About NIST". NIST. https://www.nist.gov/about-nist.

Parasol, Max. 2018. "The Impact of China's 2016 Cyber Security Law on Foreign Technology Firms, And on China's Big Data and Smart City Dreams". Computer Law & Security Review 34 (1): 67.

Paris Call. 2020. "Paris Call for Trust and Security in Cyberspace". Pariscall.International. https://pariscall.international/en/.

Polityuk, Pavel, Oleg Vukmanovic, and Stephen Jewkes. 2017. "Ukraine's Power Outage Was A Cyber Attack: Ukrenergo". U.S. Routers. https://www.reuters.com/article/us-ukraine-cyber-attack-energy/ukraines-power-outage-was-a-cyber-attack-ukrenergo-idUSKBN1521BA.

Reuters. "China Takes Another Step Toward Controversial Cybersecurity Law". 2016. Fortune. https://fortune.com/2016/06/27/china-moves-toward-adopting-cybersecurity-law/.

Reuters. 2017. "China's Tough Cybersecurity Law to Come into Force This Week". South China Morning Post. http://www.scmp.com/news/china/policies-politics/article/2096094/chinas-tough-cybersecurity-law-come-force-week.

Ruan, Lotus. 2016. "What Does China's New Cybersecurity Law Mean for Chinese Internet Companies?". The Diplomat. https://thediplomat.com/2016/11/what-does-chinas-new-cybersecurity-law-mean-for-chinese-internet-companies/.

Sacks, Samm. 2017. "China'S Cybersecurity Law Takes Effect: What to Expect". Lawfare. https://www.lawfareblog.com/chinas-cybersecurity-law-takes-effect-what-expect.

Sargsyan, Tatevik. 2016. "Data Localization and The Role of Infrastructure for Surveillance, Privacy, And Security". International Journal of Communication 10: 2221, 2225-2226.

Savelyev, Alexander. 2016. "Russia's New Personal Data Localization Regulations: A Step Forward or A Self-Imposed Sanction?". Computer Law & Security Review 32 (1): 128, 140.

Selby, John. 2017. "Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, Or Both?". International Journal of Law and Information Technology 25 (3): 213, 231. doi:10.1093/ijlit/eax010.

Shackelford, Scott J. 2013. "Toward Cyber Peace: Managing Cyber Attacks Through Polycentric Governance". SSRN Electronic Journal 62 (5): 1281-1282.

Shackelford, Scott J., Andrew A. Proia, Brenton Martell and Amanda N. Craig. 2014. "Toward a Global Cybersecurity Standard of Care? Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices.": 305, 311.

Shackelford, Scott, and Amanda Craig. "Beyond the New "Digital Divide": Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cyber-Security": 119, 121, 144, 164-165.

Shackelford, Scott, Scott Russell, and Andreas Kuehn. 2016. "Unpacking the International Law on Cybersecurity Due Diligence: Lessons from The Public and Private Sectors". Chicago Journal of International Law 17 (1): 1, 25.

Shackelford, Scott, Scott Russell, and Jeffrey Haut. 2015. "Bottoms Up: A Comparison of Voluntary Cybersecurity Frameworks". Kelley School of Business Research Paper 16 (2): 217, 223.

Shah, Reema. 2015. "Law Enforcement and Data Privacy: A Forward-Looking Approach". Yale Law Journal 125 (2): 543, 548.

Soros, George. 2019. " Remarks delivered at the World Economic Forum". https://www.georgesoros.com/2019/01/24/remarks-delivered-at-the-world-economic-forum-2/.

Statt, Nick. 2018. "Apple Argues Stronger Encryption Will Thwart Criminals in Letter to Australian Government". The Verge. https://www.theverge.com/2018/10/12/17971444/apple-iphone-stronger-encryption-letter-australian-assistance-and-access-bill-2018.

Tanenbaum, Mitch. 2020. "Why and How the Dod Is Implementing The CMMC". Cmmc-Certification.Com. https://cmmc-certification.com.

Valentino-DeVries, Jennifer, and Danny Yadron. 2015. "Cataloging the World's Cyberforces". The Wall Street Journal. https://www.wsj.com/articles/cataloging-the-worlds-cyberforces-1444610710.

Woolf, Nicky. 2016. "Ddos Attack That Disrupted Internet Was Largest of Its Kind in History, Experts Say". The Guardian. https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet.

Xia, Sara. 2017. "China Cybersecurity and Data Protection Laws: Change Is Coming". China Law Blog. https://www.chinalawblog.com/2017/05/china-cybersecurity-and-data-protection-laws-change-is-coming.html.

Yu, Liang. 2016. "China Focus: XI Calls for Developing China into World Science and Technology Leader". XINHUANET. http://www.xinhuanet.com/english/2016-04/19/c_135293965.htm.

Zwart, Alexandra De. 2019. "Australia: Assistance and Access Act, December 2018 – Uncertainty Created by New Rushed-In Data Encryption Laws". Privacy Matters. https://blogs.dlapiper.com/privacymatters/australia-assistance-and-access-act-

december-2018-holy-grail-of-uncertainty-created-by-new-rushed-in-data-encryption-laws/.

保定网警巡查执法. 2020. "公安机关“净网 2019”网络安全相关典型案例". Baidu. https://baijiahao.baidu.com/s?id=1655167701544954540.

南通网警巡查执法. 2020. "国家安全教育日丨网络安全 人人有责". Baidu. https://baijiahao.baidu.com/s?id=1664003149856685134.

大河网. 2019. "违反网络安全法这个企业被罚了". 大河网. http://newpaper.dahe.cn/jrab/html/2019-10/14/content_374468.html.

娄底网警巡查执法. 2019. "「净网 2019」网络安全行政执法十大类典型案例". Baidu. https://baijiahao.baidu.com/s?id=1649618195170303205.

季, 雨. 2020. "违规进行人脸采集，江苏宿迁一健身中心被罚！". 腾讯网. https://xw.qq.com/cmsid/20200509A0AOJZ00.

韩, 帅南. 2020. "昆明西山网警 “一案双查” 构筑网络安全屏障". 中国新闻网. http://www.yn.chinanews.com/news/2020/0430/56680.html.

ภาคผนวก

การเสวนาเพื่อรับฟังความคิดเห็นและเผยแพร่ผลการศึกษา

จัดเมื่อวันอาทิตย์ที่ 6 สิงหาคม พ.ศ. 2563 ในการนำเสนอผลการศึกษาของแผนงานคนไทย 4.0 ในงานมหกรรมวิจัยแห่งชาติ ณ โรงแรมเซ็นทราราแกรนด์ และบางกอกคอนเวนชันเซ็นเตอร์ กรุงเทพฯ

บทความเผยแพร่ทางสื่อ หนังสือพิมพ์หรือสื่อออนไลน์ชั้นนำ ครั้งที่ 1

จีนกับกฎหมายความปลอดภัยทางไซเบอร์

สื่อสิ่งพิมพ์: หนังสือพิมพ์กรุงเทพธุรกิจ ฉบับวันที่ 16 กรกฎาคม 2563

สื่อออนไลน์: https://www.bangkokbiznews.com/blog/detail/650679

กฎหมายความปลอดภัยทางไซเบอร์ของจีนเป็นรากฐานของการกำกับดูแลความปลอดภัยของข้อมูลและความปลอดภัยทางไซเบอร์ในยุคเศรษฐกิจดิจิทัล

คำถามที่น่าสนใจคือกฎหมายดังกล่าวต่างจากแนวคิดการกำกับดูแลความปลอดภัยทางไซเบอร์ของโลกตะวันตกอย่างไร?

ผมได้ดำเนินโครงการศึกษากฎหมายความปลอดภัยทางไซเบอร์กับการกำกับดูแลเศรษฐกิจดิจิทัลของประเทศจีน เพื่อถอดบทเรียนสำหรับเศรษฐกิจดิจิทัลในยุคไทยแลนด์ 4.0 ภายใต้แผนงานบูรณาการยุทธศาสตร์เป้าหมาย (Spearhead) ด้านสังคม คนไทย 4.0 สนับสนุนโดยสำนักงานการวิจัยแห่งชาติ จากการศึกษาพบว่ากฎหมายความปลอดภัยทางไซเบอร์ของจีนสะท้อนให้เห็นถึงความพยายามของรัฐบาลจีนในการอ้างอำนาจอธิปไตยบนโลกอินเทอร์เน็ตอย่างเด่นชัด

ในขณะที่แนวคิดตะวันตกแต่เดิมมองว่าไซเบอร์สเปซเป็นโลกเสรี แต่จีนกลับมองว่าไซเบอร์สเปซต้องอยู่ในความควบคุมของรัฐ ด้วยการมอบอำนาจให้รัฐบาลในการระบุและควบคุมพฤติกรรมต่างๆ บนโลกออนไลน์ที่ไม่เหมาะสม

การทำความเข้าใจกฎหมายความปลอดภัยทางไซเบอร์ของจีนจึงควรพิจารณาผ่านมุมมองพิเศษของจีนขอบเขตของความปลอดภัยทางไซเบอร์ของจีนกว้างขวางกว่าของชาติตะวันตก ในขณะที่ชาติตะวันตกเน้นเรื่องความปลอดภัยของระบบและโครงสร้างพื้นฐานเป็นสำคัญ ในประเทศจีน ความปลอดภัยทางไซเบอร์มีความหมายกว้าง โดยรวมถึงการรักษาเสถียรภาพทางการเมืองและสังคมด้วย

ภายใต้การบังคับใช้ของกฎหมายความปลอดภัยทางไซเบอร์ของจีน ผู้ให้บริการทางโครงข่ายซึ่งประกอบกิจการอันเกี่ยวข้องกับระบบโครงสร้างพื้นฐานสำคัญจะถูกบังคับให้มีส่วนร่วมในการปกป้องความมั่นคงของรัฐด้วย

จีนยังมีมาตรการบังคับให้บริษัทเทคโนโลยีต้องเก็บรวบรวมข้อมูลในท้องที่ ซึ่งทำให้ผู้ประกอบธุรกิจได้รับความเสี่ยงจากการถูกสอดแนมโดยรัฐบาลท้องที่ และถึงแม้ว่ากฎหมายจะมีบทบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล แต่กฎหมายความปลอดภัยทางไซเบอร์ก็ยังให้อำนาจรัฐบาลในการเข้าถึงข้อมูลเหล่านั้น อันย่อมนำไปสู่การรั่วไหลของข้อมูลอยู่นั่นเอง

นี่จึงเป็นสาเหตุที่เราเห็นกระแสการตั้งข้อกังวลเกี่ยวกับบริษัทเทคโนโลยีจีนและการใช้เทคโนโลยีจีน ไม่ว่าจะเป็นกรณีของ Tiktok หรือ Huawei โดยนักวิจารณ์ฝั่งตะวันตกมักอ้างถึงกฎหมายความปลอดภัยทางไซเบอร์ของจีนที่สะท้อนความเป็นไปได้ที่รัฐจีนจะทำการแทรกแซงเพื่อเข้าถึงข้อมูล โดยอ้างเหตุผลด้านความมั่นคง

อย่างไรก็ตาม ในวงวิชาการในปัจจุบัน มีข้อชวนสังเกตว่าในประเทศตะวันตกเอง กลับเริ่มมีกระแสหันมาเดินตามโมเดลจีนบ้างเช่นกัน เนื่องจากโลกตะวันตกเองก็เริ่มกังวลเรื่องภัยคุกคามต่อความมั่นคง การแข่งขันทางเทคโนโลยีกับฝ่ายจีน และมองประเด็นเหล่านี้ผ่านกรอบคิดเรื่องความปลอดภัยทางไซเบอร์

ตัวอย่างที่ชัดเจน เช่น กฎหมายการเข้ารหัสข้อมูลของประเทศออสเตรเลีย ซึ่งบังคับให้บริษัทผู้ให้บริการเทคโนโลยีคอมพิวเตอร์ยอมให้รัฐ ตำรวจ หรือข้าราชการในองค์การเกี่ยวกับความปลอดภัยเข้าถึงข้อมูลที่เข้ารหัสหรือเป็นความลับของผู้ใช้งานโดยที่ผู้ใช้งานไม่รู้ตัว เพื่อจัดการอาชญากรรม การก่อการร้าย และดูแลความมั่นคงของประเทศ

หรือเช่นร่างกฎหมายรัฐบัญญัติความมั่นคงของชาติและการคุ้มครองข้อมูลส่วนบุคคล (National Security and Personal Data Protection Act) ของสหรัฐ ซึ่งจะบังคับให้บริษัทต่างๆ ในสหรัฐต้องไม่ถ่ายโอนข้อมูลของพลเมืองอเมริกันที่เก็บได้ในประเทศไปเก็บไว้ที่ประเทศอื่นที่มีความน่ากังวล เช่น จีนหรือรัสเซีย

บทเรียนด้านกฎหมายที่สำคัญสำหรับประเทศไทยก็คือ ในการวางแนวทางการกำกับดูแลเศรษฐกิจดิจิทัลในยุคไทยแลนด์ 4.0 มีความจำเป็นจะต้องพิจารณาถึงการสร้างสมดุลระหว่าง 2 แนวคิด ได้แก่ แนวคิดเสรีนิยมกับแนวคิดที่ให้ความสำคัญกับความมั่นคง ผ่านการวางกลไกทางกฎหมายที่เหมาะสม โดยต้องออกแบบเกณฑ์หรือมาตรฐานที่จำกัดการใช้ดุลยพินิจของรัฐเกินสมควร

ในกฎหมายของไทยในบางเรื่อง ยังขาดการออกแบบกลไกหรือเกณฑ์ที่ชัดเจน แต่มักอาศัยการให้ดุลยพินิจแก่เจ้าหน้าที่รัฐด้วยภาษากฎหมายที่กำกวมและเปิดให้มีการตีความเพื่อใช้ดุลยพินิจได้อย่างกว้างขวาง ตัวอย่างเช่นในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ซึ่งมีข้อยกเว้นเป็นกฎหมายที่อ้างเหตุผลด้านความมั่นคงและให้อำนาจฝ่ายบริหารได้โดยปราศจากการใช้คำสั่งศาล

ขณะที่ในตัวอย่างกฎหมายการเข้ารหัสของออสเตรเลียนั้น เจ้าหน้าที่สามารถขอความช่วยเหลือจากผู้ให้บริการโดยต้องมีหมายศาล มีเกณฑ์ชัดเจนระบุถึงเหตุผลของเจ้าหน้าที่ในการใช้อำนาจตามกฎหมาย และในทางเทคนิคก็เพียงบังคับให้ผู้ให้บริการสร้างช่องทางพิเศษไว้เตรียมพร้อม ซึ่งแตกต่างจากแนวทางของจีนที่ขาดกลไกในการจำกัดการใช้ดุลยพินิจของรัฐ

ดังนั้น ในโลกไซเบอร์ของคนไทย 4.0 หลักคิดเรื่องการกำกับดูแลความปลอดภัยทางไซเบอร์ต้องอาศัยการสร้างสมดุลทั้งคุณค่าในเรื่องความมั่นคงของรัฐและคุณค่าเสรีนิยมไปพร้อมกัน

บทความเผยแพร่ทางสื่อ หนังสือพิมพ์หรือสื่อออนไลน์ชั้นนำ ครั้งที่ 2

ความปลอดภัยทางไซเบอร์กับโมเดลจีน

สื่อสิ่งพิมพ์: หนังสือพิมพ์กรุงเทพธุรกิจ ฉบับวันที่ 3 ธันวาคม 2563

สื่อออนไลน์: https://www.bangkokbiznews.com/blog/detail/651603

กฎหมายความปลอดภัยทางไซเบอร์ของจีน สะท้อนแนวคิดที่เป็นเอกลักษณ์เกี่ยวกับระบบการเมือง เศรษฐกิจและความมุ่งมั่นที่จะกำกับดูแลเทคโนโลยีอินเตอเน็ต

หากเราศึกษากฎหมายความปลอดภัยทางไซเบอร์ของจีน จะพบว่าสะท้อนแนวคิดที่เป็นเอกลักษณ์ของจีนเกี่ยวกับระบบการเมือง ระบบเศรษฐกิจ และความมุ่งมั่นที่จะกำกับดูแลเทคโนโลยีอินเตอร์เน็ตและไซเบอร์สเปซแบบจีน ซึ่งแตกต่างจากโมเดลเสรีนิยมในฝั่งตะวันตก

คำถามคือ โมเดลจีนเป็นตัวอย่างให้กับโมเดลไทยได้หรือไม่ คำตอบที่ชัดเจนคือ ไม่ได้ เพราะบริบทเศรษฐกิจการเมืองและระบบโครงสร้างพื้นฐานอินเตอร์เน็ตที่แตกต่างกัน นี่เป็นผลสรุปจากโครงการศึกษากฎหมายความปลอดภัยทางไซเบอร์กับการกำกับดูแลเศรษฐกิจดิจิทัลของประเทศจีน เพื่อถอดบทเรียนสำหรับเศรษฐกิจดิจิทัลในยุคไทยแลนด์ 4.0 ภายใต้แผนงานบูรณาการยุทธศาสตร์เป้าหมาย (Spearhead) ด้านสังคมคนไทย 4.0 สนับสนุนโดยสำนักงานการวิจัยแห่งชาติ

ในมุมมองของจีน การกำกับดูแลเทคโนโลยีอินเตอร์เน็ตและไซเบอร์สเปซมีความเชื่อมโยงโดยตรงกับความมั่นคงของรัฐจีน แนวคิดนี้ยังสะท้อนภาพความเป็นจริงเกี่ยวกับภูมิรัฐศาสตร์การเมืองและเทคโนโลยีระหว่างประเทศในปัจจุบัน

จอร์จ โซรอส พ่อมดการเงินโลกได้เคยกล่าวในงานเลี้ยงอาหารค่ำในการประชุม World Economic Forum ที่ดาวอส เมื่อเดือนมกราคม ค.ศ. 2019 ว่า จีนเป็นเผด็จการที่มีเทคโลยีสมัยใหม่ในการควบคุมจัดการสังคมได้ในระดับสูง ด้วยการปรับใช้เทคโนโลยีไม่ว่าจะเป็นปัญญาประดิษฐ์ (AI) หรือ Big Data ซึ่งมีพื้นฐานคือโลกไซเบอร์สเปซ ทำให้พรรคคอมมิวนิสต์จีนมีเครื่องมือใหม่ในการควบคุมจัดการสังคม

จนนักวิเคราะห์หลายคนมองว่า พรรคคอมมิวนิสต์จีนกลายเป็นสถาบันการเมืองที่มั่นคงแข็งแรงที่สุดแห่งหนึ่งของโลก และมีกลไกที่รัดกุมในการควบคุมการใช้ไซเบอร์สเปซและเทคโนโลยียุคใหม่ที่เชื่อมโยงกับอินเตอร์เน็ตในการส่งเสริมระบบการปกครองและระบบเศรษฐกิจของจีนเอง

เทคโนโลยียุค 4.0 ไม่ว่าจะเป็น ปัญญาประดิษฐ์ (AI), Big Data, หรือสัญญาณ 5G ซึ่งในปัจจุบันจีนได้พัฒนาเทคโนโลยีเหล่านี้ขึ้นมาอย่างรวดเร็ว การแข่งขันระหว่างสหรัฐฯ กับจีนในเทคโนโลยีเหล่านี้ แตกต่างจากการแข่งขันระหว่างสหรัฐฯ กับสหภาพโซเวียตในเรื่องเทคโนโลยีอวกาศและเทคโนโลยีการทหารในอดีต

นั่นก็เพราะเทคโนโลยีอวกาศและเทคโนโลยีการทหารไม่เกี่ยวกับชีวิตประจำวันของคนหมู่มาก แต่เทคโนโลยีสมัยใหม่ในยุค 4.0 นี้ ทุกคนใช้กันในชีวิตประจำวัน ดังที่วันนี้เรามีสมาร์ทโฟนกันคนละเครื่อง และอีกไม่นานก็จะถึงยุคที่ข้าวของเครื่องใช้ทุกอย่าง ไม่ว่าจะเป็นตู้เย็น โทรทัศน์ ลำโพง สามารถพูดคุยกับเราและเชื่อมต่อกับอินเทอร์เน็ตได้

การที่จีนกำลังก้าวขึ้นมาเทียบชั้นสหรัฐฯ ในเทคโนโลยีเหล่านี้ จึงมีมิติด้านความมั่นคงและเป็นภัยคุกคาม เพราะเกี่ยวข้องกับความปลอดภัยของข้อมูล และด้วยความเชื่อที่ว่า ใครที่เป็นเจ้าของแพลตฟอร์มต่างๆ ในอนาคต ย่อมเป็นมหาอำนาจทั้งในทางการเมืองและเศรษฐกิจ ซึ่งเดิมฝั่งตะวันตกได้แก่ยุโรปและสหรัฐฯ เป็นผู้นำในเชิงตลาดอุปกรณ์โครงข่ายและเครื่องรับส่งสัญญาณ 4G และแพลตฟอร์มบนอินเทอร์เน็ตไม่ว่าจะเป็น Google, Facebook, Amazon รวมทั้งแพลตฟอร์มที่เป็นฮาร์ดแวร์ ซอฟต์แวร์และอุปกรณ์เครื่องใช้ต่างๆ เช่น Apple, Microsoft

แต่ในปัจจุบัน จีนเป็นชาติเดียวที่ขึ้นมาแข่งขันในแพลตฟอร์มบนอินเทอร์เน็ตเต็มตัว รวมทั้งยังมีแนวทางการกำกับดูแลไซเบอร์สเปซตามแนวคิดการกำกับดูแลอย่างรัดกุม เพื่อเอื้อกับการส่งเสริมระบบการเมืองและระบบเศรษฐกิจของจีน ซึ่งแตกต่างจากแนวคิดเสรีนิยมของตะวันตกที่มองว่าไซเบอร์สเปซเป็นพื้นที่เสรี

สาเหตุที่จีนเป็นชาติเดียวที่ขึ้นมาแข่งขันในแพลตฟอร์มบนอินเตอร์เน็ตเต็มตัว แม้จะไม่ได้เดินตามแนวทางเสรีนิยมดังแนวทางของตะวันตก เนื่องด้วยปัจจัยด้านเศรษฐกิจการเมืองที่พิเศษของจีน อาทิ ระบบเศรษฐกิจที่มีเอกลักษณ์ของจีนที่รัฐมียุทธศาสตร์อินเตอร์เน็ตที่ชัดเจน การวางแผนสร้างระบบ Great Firewall ของจีนตั้งแต่เริ่มแรกที่ทำให้สามารถควบคุมอินเตอร์เน็ต รวมทั้งการใช้ประโยชน์จากตลาดขนาดใหญ่ และพลังสร้างสรรค์ของผู้ประกอบการแพลตฟอร์มบนอินเตอร์เน็ตของจีน

ในขณะที่เมื่อมองย้อนกลับมาที่ไทย ซึ่งรับแนวความคิดสากลในเรื่องอินเตอร์เน็ตตั้งแต่เริ่มแรก และไม่มีระบบ Great Firewall มาตั้งแต่เริ่มต้น หากต่อมาโมเดลไทยมีแนวคิดต้องการที่จะรักษาและควบคุมอินเตอร์เน็ตตามโมเดลจีน ผลคือยากที่จะบังคับใช้กฎหมายได้ตามวัตถุประสงค์ทางการเมืองและเศรษฐกิจดังเช่นในจีน

เบื้องหลังแพลตฟอร์มไซเบอร์สเปซของจีนก็คือ รัฐจีน ซึ่งสะท้อนระบบ ความคิดความเชื่อที่แตกต่างจากตะวันตก ถึงแม้ว่าหลายบริษัทด้านเทคโนโลยีของจีนจะเป็นบริษัทเอกชนจีน แต่กฎหมายความปลอดภัยทางไซเบอร์ของจีนบัญญัติไว้ชัดเจนว่าบริษัทเอกชนจีนต้องให้ความร่วมมือกับรัฐในเรื่องความมั่นคง รวมทั้งปัญหาที่ว่า บริษัทเทคโนโลยีจีนเหล่านี้ก้าวขึ้นมาได้ขนาดนี้ย่อมเป็นเพราะการช่วยเหลือ อุดหนุน และส่งเสริมจากรัฐบาลจีนทั้งในเรื่องแหล่งเงินทุนและการปิดกั้นต่างชาติผ่านกลไกกฎหมาย

คนไทย 4.0 จึงกำลังเผชิญกับโลกภูมิรัฐศาสตร์การเมืองและเทคโนโลยีระหว่างประเทศที่มีความซับซ้อน และแตกต่างจากโลกเดิมที่มีความเห็นร่วมกันเกี่ยวกับไซเบอร์สเปซที่ค่อนข้างชัดเจน สำหรับคน

ไทย 4.0 ซึ่งต่อไปในทุกมิติของชีวิตย่อมมีความเกี่ยวข้องกับเทคโนโลยีอินเตอร์เน็ตอย่างหลีกเลี่ยงไม่ได้ ควรตระหนักว่าการเชื่อมโยงกับไซเบอร์สเปซมีมิติด้านความมั่นคงของรัฐเสมอ

คำถามใหญ่ต่อไปก็คือ เราจะเป็นส่วนหนึ่งของแพลตฟอร์มสหรัฐฯ หรือจีน และไม่ว่าในประเด็นไหนหรือเทคโนโลยีใด เราจะกลายเป็นส่วนหนึ่งของแพลตฟอร์มของใครก็ตาม คำถามสำคัญถัดมาก็คือ เราจะแสวงหาแนวทางการกำกับดูแลที่เหมาะสมอย่างไร เพื่อประกันความปลอดภัยทางไซเบอร์และความมั่นคงของชาติ โดยสร้างสมดุลทั้งคุณค่าในเรื่องความมั่นคงของรัฐและคุณค่าเสรีนิยม

ร่างบทความวิชาการเผยแพร่ในวารสารวิชาการในประเทศไทยที่มีคุณภาพ

กฎหมายความปลอดภัยทางไซเบอร์ของประเทศจีน: ศึกษาเปรียบเทียบกฎหมายของสหรัฐอเมริกา สหภาพยุโรป และไทย

ดร.อาร์ม ตั้งนิรันดร

1. บทนำ

เศรษฐกิจดิจิทัลของจีนมีการพัฒนาอย่างรวดเร็ว จนจีนนับเป็นผู้นำด้านเศรษฐกิจดิจิทัลในระดับโลก โดยกฎหมายความปลอดภัยทางไซเบอร์ของจีน (Cybersecurity Law 2017) เป็นกฎหมายหลักที่เป็นรากฐานของการกำกับดูแลความปลอดภัยของข้อมูลและความปลอดภัยทางไซเบอร์ในยุคเศรษฐกิจดิจิทัล กฎหมายดังกล่าวได้ผ่านการพิจารณาจากสภาประชาชนแห่งชาติในวันที่ 7 พฤศจิกายน ค.ศ. 2016 และเริ่มมีผลบังคับใช้ตั้งแต่วันที่ 1 มิถุนายน ค.ศ. 2017 เป็นต้นมา

กฎหมายความปลอดภัยทางไซเบอร์ของจีนสะท้อนให้เห็นถึงความพยายามของรัฐบาลจีนในการอ้างอำนาจอธิปไตยบนโลกอินเทอร์เน็ต ประเทศจีนมีความต้องการจัดการดูแลไซเบอร์เสปซด้วยตัวเอง ด้วยการมอบอำนาจให้รัฐบาลในการระบุและควบคุมพฤติกรรมต่างๆ บนโลกออนไลน์ที่ไม่เหมาะสม การทำความเข้าใจในกฎหมายความปลอดภัยทางไซเบอร์ของจีนควรพิจารณาผ่านมุมมองพิเศษของประเทศจีนที่มีต่อความปลอดภัยทางไซเบอร์ ซึ่งมีความหมายกว้างขวางกว่าของชาติตะวันตก ในประเทศจีน ความปลอดภัยทางไซเบอร์จะเกิดขึ้นได้ก็ด้วยการควบคุมเนื้อหาบนอินเทอร์เน็ต เพื่อรักษาไว้ซึ่งความเสถียรภาพทางการเมืองและสังคม นอกจากนี้ การปฏิบัติต่อข้อมูลส่วนบุคคลในกฎหมายฉบับนี้สะท้อนให้เห็นถึงมุมมองของประเทศจีนในด้านสิทธิมนุษยชน สิทธิมนุษยชนได้รับการรับรองตามกฎหมาย ทว่าก็สามารถถูกละเมิดโดยอำนาจรัฐได้

บทความนี้จะเริ่มจากการอภิปรายเกี่ยวกับสำนักคิดสองสำนักที่เกี่ยวกับการดำกับดูแลไซเบอร์สเปซ

2. สำนักคิดที่เกี่ยวกับการกำกับดูแลไซเบอร์สเปซ

คำถามสำคัญคือรัฐควรจะเข้ามามีบทบาทอย่างไรในการกำกับดูแลไซเบอร์สเปซ รัฐควรแทรกแซงธุรกิจของเอกชนหรือไม่ เพื่อให้แน่ใจว่าข้อมูลที่เอกชนรวบรวมจากประชาชนได้รับการคุ้มครองที่เหมาะสม หรือรัฐควรป้องกันไม่ให้มีการเข้าถึงบางส่วนของอินเตอร์เน็ต เพื่อป้องกันไม่ให้ประชาชนเข้าไปตกอยู่ในภาวะเสี่ยงที่ข้อมูลส่วนตัวจะถูกลักลอบ ปัจจุบัน ในประเด็นเหล่านี้ มีสองสำนักคิดที่แตกต่างกันอย่างสุดขั้ว[279] โดย

[279] Shackelford, Scott J. 2013. "Toward Cyber Peace: Managing Cyber Attacks Through Polycentric Governance". SSRN Electronic Journal 62 (5): 1281-1282.

ประเทศจีนมีแนวคิดสอดคล้องกับสำนัก Cyber Paternalism แตกต่างจากฝั่งตะวันตก ซึ่งมีแนวคิดสอดคล้องกับสำนัก Cyber Commons

2.1 สำนัก Cyber Paternalism

ขั้วปรัชญาของสำนักคิดแรกชื่อว่า “Cyber Paternalism” หรือเรียกว่า “Data Nationalism” หรือ “Internet Sovereignty”[280] เป็นแนวคิดที่ว่าด้วยการขยายอำนาจของรัฐเข้าไปในไซเบอร์สเปซ และควบคุมการเคลื่อนไหวของข้อมูลซึ่งบันทึกไว้ในหน่วยของประเทศทั้งขาเข้าและขาออก[281] ภายใต้แนวคิดนี้ เขตอำนาจบังคับใช้กฎหมายย่อมครอบคลุมไปถึงสื่อต่างๆ ในโลกความเป็นจริง และเพื่อให้การขยายขอบเขตอำนาจบังคับใช้กฎหมายเป็นไปอย่างมีประสิทธิภาพมากที่สุด ข้อมูลต่างๆ ที่เก็บรวบรวมได้ภายในประเทศควรถูกบังคับให้นำมาเก็บไว้ในแหล่งเก็บข้อมูลของประเทศด้วย โดยขั้นตอนดังกล่าวเรียกว่า data localization[282] นอกจากนี้แล้ว แนวคิดนี้ยังสนับสนุนการอ้างเขตอำนาจบังคับใช้กฎหมายเหนือประชากรส่วนใหญ่บนโลกอินเตอร์เน็ต โดยไม่สนใจว่าข้อมูลเหล่านั้นเก็บไว้ที่ใด หากโดเมนนั้นได้เข้ามาในเขตอำนาจแล้ว ก็ย่อมตกอยู่ใต้การกำกับควบคุมนั้นด้วย[283]

2.2 สำนัก Cyber Commons

ขั้วปรัชญาของสำนักคิดขั้วตรงข้ามมีชื่อว่า “Cyber Commons” หากพิจารณาในด้านคำศัพท์ จะพบว่า Commons หมายถึง ที่ดินหรือทรัพยากรที่เป็นของชุมชนและมีลักษณะเป็นทรัพย์สินร่วมกัน มิใช่ของผู้ใดผู้หนึ่ง กล่าวคือเป็นทรัพย์สินสาธารณะ การมองว่าไซเบอร์สเปซเป็นทรัพย์สินสาธารณะ เช่นเดียวกันกับน้ำ อากาศ หรือพื้นที่ในอวกาศ เท่ากับเป็นการปฏิเสธไม่ให้ผู้ใช้งานหน่วยหนึ่งหน่วยใดมีอำนาจเหนือกว่ากันในการใช้ทรัพยากรนั้น สำนัก Cyber Commons มีความเชื่อว่าขอบเขตอำนาจบังคับใช้กฎหมายแยกกันต่างหากกับไซเบอร์สเปซ ขอบเขตอำนาจบังคับใช้กฎหมายจะใช้บังคับได้มากน้อยเพียงใด ย่อมขึ้นกับว่าใครเป็นผู้บริหารจัดการโดเมนของเว็บไซต์นั้นๆ มิใช่ขึ้นอยู่กับว่าแหล่งข้อมูลนั้นจะถูกเก็บไว้ ณ ที่ใด[284] มาตรการรักษาความปลอดภัยของโดเมนควรถูกควบคุมอยู่แล้วโดยมาตรฐานอุตสาหกรรม ซึ่งเป็นระดับความระมัดระวัง

---

[280] Shackelford, Scott J. "Toward Cyber Peace: Managing Cyber Attacks Through Polycentric Governance": 1283.

[281] Chander, Anupam. 2015. "Data Nationalism". Emory Law Journal 64 (3): 680.

[282] Chander, Anupam. "Data Nationalism": 680-681.

[283] Johnson, David R., and David G. Post. 1996. "Law And Borders - The Rise Of Law In Cyberspace". Stanford Law Review 48: 1367, 1394.

[284] Johnson, David R., and David G. Post. 1996. "Law And Borders - The Rise Of Law In Cyberspace": 1378, 1380.

ตามกฎหมายที่ใช้ในการอ้างถึงเมื่อเกิดกรณีพิพาทระหว่างบริษัทผู้ให้บริการกับคู่กรณี[285] มาตรฐานเช่นว่านี้คือผลของการร่วมมือกันระหว่างภาครัฐและเอกชน องค์กรธุรกิจ นักกฎหมาย และนักวิชาการเพื่อสร้างความมั่นคงให้กับโลกไซเบอร์[286] ซึ่งบุคคลเหล่านี้ต่างก็เป็นผู้มีส่วนได้เสียกับการปกครองบนโลกอินเตอร์เน็ต

3. โครงสร้างกฎหมายความปลอดภัยทางไซเบอร์ของประเทศจีน

เนื่องด้วยการพัฒนาเทคโนโลยีดิจิตัลอย่างรวดเร็วในและการเชื่อมต่อระหว่างเครือข่ายในประเทศจีนเป็นส่วนสำคัญที่ทำให้ความปลอดภัยทางไซเบอร์กลายเป็นวาระระดับชาติ กฎหมายความปลอดภัยทางไซเบอร์ถูกร่างขึ้นโดยอาศัยแนวคิด “อธิปไตยไซเบอร์” ตามแนวคิดของสำนัก Cyber Paternalism ซึ่งเป็นส่วนสำคัญในการกำหนดนโยบายและระเบียบของอินเตอร์เน็ตในประเทศจีน โดยมีวัตถุประสงค์เพื่อเป็นหลักสำคัญในการปกป้องความมั่นคงของจีน

โครงสร้างเนื้อหาของกฎหมายความปลอดภัยทางไซเบอร์ สามารถสรุปได้โดยสังเขป ดังนี้

ในหมวดแรกของกฎหมายใหม่ระบุถึงเจตนารมณ์ของกฎหมาย และกล่าวถึงหน่วยงานซึ่งมีหน้าที่รับผิดชอบต่อกฎหมายฉบับนี้[287] โดยหนึ่งในเจตนารมณ์นั้นรวมไปถึงการเผยแพร่ “แก่นคุณค่าของสังคมนิยม”[288] และสร้างความรับผิดชอบให้แก่หน่วยงานต่างๆ ของรัฐในการวางแผน ทำงานร่วมกัน กำกับดูแล และบริหารจัดการความมั่นคงของเครือข่าย[289] มาตราดังกล่าวยังกำหนดหน้าที่ของเอกชนและองค์กรต่างๆ ให้รายงานการกระทำต่างๆ ที่เป็นภัยต่อความมั่นคงบนอินเตอร์เน็ต ในขณะที่รัฐเองก็มีหน้าที่ต้องตอบกลับอย่างทันท่วงที[290] นอกจากนี้ ยังมีมาตรการที่ใช้บังคับ “องค์กรอุตสาหกรรมต่างๆ ที่เกี่ยวข้องกับเครือข่าย” ให้เสริมสร้างระบบการรักษาความปลอดภัยของพวกเขา โดยไม่จำเป็นต้องรายงานให้ทางการทราบถึงวิธีการที่ทำให้บรรลุวัตถุประสงค์ดังกล่าว[291] และในมาตรา 12 บังคับให้ทั้งบุคคลและองค์กรทั้งหมดงดเว้นการกระทำใดๆ ที่อาจส่งผลเสียต่อนโยบายสังคมนิยมของชาติ[292]

---

[285] Shackelford, Scott J., Andrew A. Proia, Brenton Martell and Amanda N. Craig. 2014. “Toward a Global Cybersecurity Standard of Care? Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices.”: 305, 311.

[286] Eichensehr, Kristen. 2015. "The Cyber-Law Of Nations". *Georgetown Law Journal*, 317, 346.

[287] 《中华人民共和国网络安全法》第 1 章

[288] 《中华人民共和国网络安全法》第 6 章

[289] 《中华人民共和国网络安全法》第 8 章

[290] 《中华人民共和国网络安全法》第 12 章

[291] 《中华人民共和国网络安全法》第 11 条

[292] 《中华人民共和国网络安全法》第 12 条

ในหมวดที่ 2 ของกฎหมายนี้สร้างแนวทางพื้นฐานว่ารัฐบาลควรจะทำอย่างไรเพื่อเสริมสร้างความปลอดภัยไซเบอร์[293] โดยมีการบังคับให้หน่วยงานรัฐทุกระดับ ตั้งแต่คณะรัฐมนตรีจนไปถึงเทศบาลในเขตปกครองตนเองจัดทำแผนการต่างๆ ที่เกี่ยวข้อง[294] นอกจากนี้ รัฐยังให้การสนับสนุนด้านต่างๆ ที่เกี่ยวกับการเสริมสร้างความปลอดภัยไซเบอร์ด้วย ยกตัวอย่างเช่น การให้การสนับสนุนนวัตกรรมเทคโนโลยีที่เกี่ยวข้องกับความมั่นคง การสนับสนุนการศึกษาเกี่ยวกับความปลอดภัยไซเบอร์ในการศึกษาระดับมหาวิทยาลัยหรือการศึกษาระดับวิชาชีพขั้นสูง ซึ่งรวมไปถึงการปลูกฝังในความตระหนักรู้เกี่ยวกับความปลอดภัยไซเบอร์ด้วย[295]

ในหมวดที่ 3 เป็นบทที่ใช้บังคับแก่ผู้ให้บริการเครือข่ายที่ให้บริการบนอินเตอร์เน็ต หรือผู้ให้บริการ[296] โดยกฎหมายได้บัญญัติถึงหน้าที่ทั่วไปที่ผู้ให้บริการต้องดำเนินการ[297] พร้อมทั้งหน้าที่พิเศษสำหรับการจัดการ “ระบบข้อมูลที่มีความอ่อนไหว” ซึ่งเกี่ยวข้องกับระบบโครงสร้างพื้นฐาน[298] โดยบังคับให้ผู้ให้บริการต้องเก็บข้อมูลตัวตนของบุคคลผู้ใช้งานที่แท้จริงไว้[299] และปฏิบัติตามคำสั่งที่หน่วยงานรัฐจะบังคับใช้แก่อุตสาหกรรมตนด้วย[300] ระบบโครงสร้างพื้นฐานประกอบด้วยระบบพลังงาน ระบบการบริหารจัดการน้ำ และเรื่องการธุรกรรม แต่สำหรับกฎหมายนี้ ระบบโครงสร้างพื้นฐานอาจรวมไปถึงสิ่งอื่นๆ ซึ่งเมื่อเกิดการรั่วไหลของข้อมูล ณ ส่วนนั้นแล้ว “อาจเป็นอันตรายต่อความมั่นคงของชาติ สวัสดิการแห่งรัฐ ความเป็นอยู่ของประชาชน หรือประโยชน์สาธารณะ” [301] นอกจากนี้ รัฐบาลยังสนับสนุนให้ผู้ให้บริการที่ไม่ใช่ระบบโครงสร้างพื้นฐานให้มามีหน้าที่ตามกฎหมายเช่นเดียวกันกับผู้ให้บริการเครือข่ายที่เกี่ยวข้องกับระบบโครงสร้างพื้นฐานสำคัญด้วย[302] กรณีนี้เป็นประเด็นที่สำคัญมาก เนื่องจากว่า ผู้ให้บริการเครือข่ายที่เกี่ยวข้องกับระบบโครงสร้างพื้นฐานสำคัญต้องยินยอมให้หน่วยงานของรัฐที่เกี่ยวข้องตรวจสอบเสมอ เมื่อพวกเขาต้องการซื้อผลิตภัณฑ์หรือบริการที่ เกี่ยวกับเครือข่ายซึ่ง “อาจกระทบต่อความปลอดภัยของพวกเขา” [303] ผู้ให้บริการเครือข่ายที่เกี่ยวข้องกับระบบโครงสร้างพื้นฐานสำคัญต้องเก็บข้อมูลที่ได้มาจากการสะสมหรือผลิตขึ้นไว้ภายในอาณาเขตของประเทศ และในกรณีที่มีความต้องการนำข้อมูลเหล่านั้นไปแสดง ณ ต่างประเทศ ข้อมูลเหล่านี้ต้องผ่านการประเมินด้านความปลอดภัยจากรัฐบาล[304] นอกจากนี้ ผู้ให้บริการเครือข่ายที่เกี่ยวข้องกับระบบโครงสร้างพื้นฐานสำคัญต้องยอมอยู่ภายใต้การกำกับดูแลของรัฐและทำการส่งเนื้อหาต่าง ๆ ที่มีความอ่อนไหวให้แก่รัฐบาล[305]

---

[293] 《中华人民共和国网络安全法》第 2 章
[294] 《中华人民共和国网络安全法》第 16 条
[295] 《中华人民共和国网络安全法》第 20 条
[296] 《中华人民共和国网络安全法》第 76 条
[297] 《中华人民共和国网络安全法》第 21 条
[298] 《中华人民共和国网络安全法》第 34 条
[299] 《中华人民共和国网络安全法》第 24 条
[300] 《中华人民共和国网络安全法》第 32 条
[301] เรื่องเดียวกัน.
[302] เรื่องเดียวกัน.
[303] 《中华人民共和国网络安全法》第 35 条
[304] 《中华人民共和国网络安全法》第 37 条
[305] 《中华人民共和国网络安全法》第 39 条

ในหมวดที่ 4 กล่าวถึงมาตรฐานของผู้ให้บริการทั่วไป[306] โดยมาตราส่วนใหญ่ในบทนี้กล่าวถึงข้อพึงปฏิบัติต่างๆ ที่ผู้ให้บริการต้องดำเนินการ เช่น ข้อมูลใดจะถูกเก็บสะสมได้บ้าง[307] ซึ่งเกี่ยวข้องกับการที่บุคคลจะถูกบังคับให้แสดงตัวตนที่แท้จริงทุกครั้งที่มีการเชื่อมถึงอินเตอร์เน็ต การจดทะเบียนโดเมน หรือเข้าถึงบริการข้อมูลสาธารณะ[308] และมีมาตราหนึ่งที่บังคับผู้ให้บริการต้องเฝ้าระวังการเผยแพร่เนื้อหาของผู้ใช้งานที่มีลักษณะต้องห้ามตามระเบียบของฝ่ายบริหารหรือกฎหมายอื่นอีกด้วย[309] กฎหมายฉบับนี้กำหนดให้ผู้ให้บริการมีหน้าที่ทั้งเป็นผู้เซ็นเซอร์แทนหน่วยงานรัฐและยังเป็นหูเป็นตาให้รัฐบาลในการสอดส่องดูแล ซึ่งสังเกตได้จากการที่กฎหมายนี้ให้ผู้ให้บริการรายงานความพยายามในการเผยแพร่ข้อมูลที่ไม่เหมาะสมนี้ไปให้ “หน่วยงานรัฐที่เกี่ยวข้อง”[310] ทั้งนี้ ผู้ให้บริการต้องอยู่ภายใต้การบริหารจัดการและการกำกับดูแลของรัฐ[311]

ในหมวดที่ 5 กล่าวถึงวิธีการที่หน่วยงานต่างๆ ของรัฐจะกำกับดูแลความปลอดภัยไซเบอร์ พร้อมทั้งกำหนดว่าหน่วยงานใดบ้างของรัฐที่มีหน้าที่ในการเตรียมพร้อมรับมือกับสถานการณ์อันเสี่ยงต่อความมั่นคง[312] มาตราสุดท้ายในหมวดนี้น่าสนใจเป็นอย่างยิ่ง เนื่องจากให้อำนาจคณะรัฐมนตรี พร้อมทั้งรัฐบาลในระดับอื่นซึ่งได้รับอนุญาตจากคณะรัฐมนตรี ในการบังคับใช้มาตรการชั่วคราวเพื่อควบคุมระบบเครือข่ายในกรณีที่เกิดสถานการณ์ฉุกเฉิน หรืออุบัติเหตุต่างๆ จากผลิตภัณฑ์ได้ [313] ในขณะที่มาตรการอื่นๆ คือการระงับการเข้าถึงอย่างตรงไปตรงมา[314]

หมวดที่ 6 ได้กล่าวถึงความรับผิดทางกฎหมายของผู้ให้บริการที่ฝ่าฝืนหรือไม่ปฏิบัติมาตรการในกฎหมายนี้[315] เป็นที่น่าสนใจว่ารัฐบาลได้มุ่งจะเอาผิดแก่ตัวบุคคลและบังคับให้จ่ายค่าปรับ แทนที่จะเป็นการนำโทษปรับนั้นไปใช้กับองค์กรธุรกิจซึ่งใหญ่กว่า[316] และมีอีกสองมาตราที่กล่าวถึงการเซ็นเซอร์ของรัฐ โดยผู้ผู้ให้บริการที่ล้มเหลวในการเซ็นเซอร์เนื้อหาที่ต้องห้ามนั้นจะถูกปรับและระงับการอนุญาตการให้บริการ[317] นอกจากนี้ ในมาตรา 70 ยังขยายขอบเขตของเนื้อหาต้องห้าม ด้วยการอ้างถึงมาตรา 12 (มาตราที่บังคับว่าห้ามมิให้ผู้ใดใช้อินเตอร์เน็ตเพื่อทำลาย “แก่นคุณค่าแห่งสังคมนิยม) [318]

กฎหมายความปลอดภัยทางไซเบอร์ ค.ศ. 2017 กำหนดหน้าที่และบทลงโทษไว้อย่างชัดเจน ขณะเดียวกันก็ยังมีอีกหลายส่วนที่เว้นว่างไว้ให้หน่วยงานของรัฐที่เกี่ยวข้องไปบัญญัติเพิ่มเองได้ จะเห็นได้ว่า

---

[306] 《中华人民共和国网络安全法》第 4 章
[307] 《中华人民共和国网络安全法》第 40-45 条
[308] 《中华人民共和国网络安全法》第 24 条
[309] 《中华人民共和国网络安全法》第 47 条
[310] 《中华人民共和国网络安全法》第 47 条
[311] 《中华人民共和国网络安全法》第 50 条
[312] 《中华人民共和国网络安全法》第 5 章
[313] 《中华人民共和国网络安全法》第 58 条
[314] เรื่องเดียวกัน.
[315] 《中华人民共和国网络安全法》第 6 章
[316] 《中华人民共和国网络安全法》第 60 条
[317] 《中华人民共和国网络安全法》第 68-69 条
[318] 《中华人民共和国网络安全法》第 70 条

ประเทศจีนมีความพยายามที่จะดึงให้ผู้ให้บริการมาเป็นส่วนของของระบบเซ็นเซอร์ของตัวเอง เสมือนหนึ่งผู้ให้บริการนั้นเป็นแขนขาให้กับทางการ[319] จึงมีนักวิเคราะห์บางคนมองว่ากฎหมายฉบับนี้เป็นมากกว่าการต้องการคุ้มครองรักษาข้อมูล แต่หากเป็นการที่รัฐพยายามจะปิดหูปิดตาประชาชน[320] และการอ้างเรื่องความปลอดภัยไซเบอร์แสดงให้เห็นถึงความเชื่อในสำนัก Cyber Paternalism โดยอ้างว่าทำไปเพื่อคุ้มครองความปลอดภัยในไซเบอร์สเปซ[321]

4. ประเด็นกฎหมายความปลอดภัยทางไซเบอร์ของจีน: ศึกษาเปรียบเทียบกับกฎหมายที่เกี่ยวข้องของประเทศสหรัฐอเมริกา สหภาพยุโรป และประเทศไทย

4.1 หน้าที่ตามกฎหมายของผู้ให้บริการทางเครือข่าย

1) กฎหมายจีน

กลุ่มเป้าหมายของกฎหมายความมั่นคงไซเบอร์ใช้บังคับแก่บุคคลที่เป็นตัวกลางในการสื่อสารบนโลกอินเทอร์เน็ต เช่น หน่วยงานที่ให้บริการเชื่อมต่อเข้ากับเครือข่าย (ISP) เสิร์ชเอนจิน และ ผู้ให้บริการสื่อออนไลน์ต่างๆ บุคคลที่เป็นตัวกลางเหล่านี้ โดยเฉพาะอย่างยิ่งหน่วยงานที่ให้บริการเชื่อมต่อเข้ากับเครือข่าย (ISP) มีส่วนสำคัญยิ่งในการบล็อกและเซ็นเซอร์เนื้อหาต่างๆ บนเว็บไซต์ของต่างประเทศที่ไม่พึงประสงค์[322]

นอกจากนี้ กฎหมายนี้ยังสร้างหน้าที่ตามกฎหมายมากมายให้กับกลุ่มเป้าหมายเหล่านั้น ไม่ว่าจะเป็นผู้ให้บริการทางเครือข่ายทั่วไป ผู้ให้บริการข้อมูลโครงสร้างพื้นฐานที่มีความอ่อนไหวสูง หรือแม้กระทั่งผู้ผลิตสินค้าหรือบริการที่เกี่ยวข้องกับเครือข่าย ตัวอย่างเช่น กฎหมายความปลอดภัยทางไซเบอร์ มาตรา 25 บังคับให้ผู้ให้บริการพัฒนามาตรการฉุกเฉินเพื่อรับมือกับความเสี่ยงและภยันตรายที่อาจเกิดขึ้น เช่น ช่องโหว่ของระบบ ไวรัส หรือการโจมตีทางไซเบอร์ รวมถึงหน้าที่ในการรายงานเหตุการณ์ต่างๆ ที่เกิดขึ้นให้แก่เจ้าหน้าที่ทราบ หรือ มาตรา 38 บังคับให้ผู้ให้บริการข้อมูลโครงสร้างพื้นฐานที่มีความอ่อนไหวสูงต้องทำการประเมินผลและพัฒนามาตรการเฝ้าระวังของตนเอง หรือ มาตรา 22 ซึ่งบังคับให้ผู้ผลิตสินค้าหรือบริการที่เกี่ยวข้องกับเครือข่ายปฏิบัติตามมาตรฐานของชาติ ห้ามการใช้โปรแกรมที่มีวัตถุประสงค์ชั่วร้าย และหากมีช่องโหว่เกิดขึ้น ผู้ผลิตจะต้องแจ้งให้ผู้ใช้งานและหน่วยงานที่เกี่ยวข้องทราบทันทีและดำเนินการแก้ไขโดยเร็ว

---

[319] 《中华人民共和国网络安全法》第 50 条

[320] Allen-Ebrahimian, Bethany. 2015. "The 'Chilling Effect' Of China's New Cybersecurity Regime". Foreign Policy. https://foreignpolicy.com/2015/07/10/china-new-cybersecurity-law-internet-security/.

[321] Shackelford, Scott, and Amanda Craig. "Beyond the New "Digital Divide": Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cyber-Security": 121.

[322] Lee, Jyh-An, and Ching-Yi Liu. 2012. "Forbidden City Enclosed by The Great Firewall". Minnesota Journal of Law, Science, And Technology 13 (1): 148-150.

กฎหมายได้ให้นิยามคำว่า “ผู้ให้บริการทางเครือข่าย” หรือผู้ให้บริการ ว่าคือ เจ้าของโครงข่าย ผู้บริการโครงข่าย และผู้ให้บริการทางเครือข่ายโดยตรง ซึ่งเป็นนิยามที่ถูกวิพากษ์วิจารณ์อย่างมากเนื่องจากความกว้างขวางของนิยาม เพราะคลอบคลุมถึงผู้ประกอบธุรกิจทุกภาคส่วนที่มีส่วนเกี่ยวข้องกับอินเทอร์เน็ต[323] มีผู้ให้ความเห็นว่า รัฐบาลประสงค์จะให้นิยามมีความกว้างขวาง เพื่อใช้รับมือกับการตีความในอนาคต[324]

หน้าที่หลักของผู้ให้บริการถูกบัญญัติไว้ในมาตรา 21 ของกฎหมายความมั่นคงปลอดภัยไซเบอร์ ดังนี้

1. หน้าที่กำหนดระบบมาตรการรักษาความปลอดภัยภายในองค์กรและการควบคุมให้ปฏิบัติกฎต่างๆ ว่าด้วยความรับผิดชอบของผู้ดูแลรักษาความปลอดภัย รวมไปถึงหน้าที่ในการรับความรับผิดต่างๆ อันเกิดจากระบบรักษาความปลอดภัยนั้น
2. หน้าที่ในการนำเอามาตรการทางเทคโนโลยีต่างๆ มาใช้เพื่อป้องกันไวรัส การโจมตีหรือการบุกรุกผ่านเครือข่าย และสิ่งอื่นสิ่งใดที่เป็นอันตรายต่อความปลอดภัยของเครือข่าย
3. หน้าที่ในการนำเอามาตรการทางเทคโนโลยีต่างๆ มาใช้เพื่อกำกับดูแลและบันทึกสถานการณ์การให้บริการต่างๆ บนอินเทอร์เน็ต ภยันตรายต่างๆ ที่เกิดขึ้น และวิธีการในการเก็บข้อมูลสิ่งที่บันทึกนั้น โดยบันทึกเหล่านั้นต้องสามารถตรวจสอบย้อนหลังได้ไม่น้อยกว่า 6 เดือน
4. หน้าที่ในการนำเอามาตรการว่าด้วยการคัดแยกข้อมูล การสำรองข้อมูลสำคัญ และการเข้ารหัส รวมไปถึงมาตรการอื่น ๆ ซึ่งบัญญัติไว้ในกฎหมายหรือระเบียบบริหารที่เกี่ยวข้องมาปรับใช้

นอกจากนี้ ผู้ให้บริการต้องพัฒนามาตรการเพื่อรับมือกับภยันตรายไซเบอร์ด้วย และหากมีภยันตรายเหล่านั้นเกิดขึ้น ผู้ให้บริการต้องทำการแก้ไขที่เหมาะสมโดยเร็วและรายงานเหตุการณ์นั้นให้แก่หน่วยงานที่เกี่ยวข้องทราบด้วย หากผู้ให้บริการล้มเหลวในการปฏิบัติตามมาตรการเหล่านี้ เจ้าหน้าที่อาจสั่งให้แก้ไขหรือตักเตือนได้ และหากผู้ให้บริการไม่ปฏิบัติตามคำสั่งหรือคำเตือนนั้น ผู้ให้บริการจะถูกปรับเป็นเงิน 10,000 หยวน ถึง 100,000 หยวน และผู้ที่รับผิดชอบโดยตรงจะถูกปรับเป็นการส่วนตัวอีก 5,000 หยวน ถึง 50,000 หยวน

มาตรา 24 มอบหน้าที่ให้ผู้ให้บริการบังคับผู้ใช้งานของตนแสดงชื่อจริงเมื่อมีการสมัครการใช้บริการเพื่อเข้าถึงบริการทางอินเทอร์เน็ต จดทะเบียนโดเมน ใช้บริการโทรศัพท์บ้านหรือโทรศัพท์มือถือ การเผยแพร่ข้อมูลสาธารณะ และการใช้บริการส่งข้อความต่างๆ นอกจากนี้ กฎหมายยังห้ามไม่ให้ผู้ให้บริการให้บริการกับผู้ใช้งานที่ไม่ได้แสดงชื่อจริงของตน โดยหากผู้ให้บริการไม่ปฏิบัติตามมาตรการนี้ หน่วยงานที่เกี่ยวข้องจะมีคำสั่งให้แก้ไข และหากผู้ให้บริการยังเพิกเฉย หรือปรากฏว่าการฝ่าฝืนของผู้ให้บริการก่อให้เกิดผลร้ายแรง พวกเขาจะถูกปรับเป็นเงิน 50,000 หยวน ถึง 500,000 หยวน และหน่วยงานอาจสั่งระงับการประกอบกิจการ

[323] Cohen, Bret, Britanie Hall, and Charlie Wood. 2017. "Data Localization Laws and Their Impact on Privacy, Data Security and The Global Economy". ANTITRUST 32 (1): 107,109.

[324] Xia, Sara. 2017. "China Cybersecurity and Data Protection Laws: Change Is Coming". China Law Blog. https://www.chinalawblog.com/2017/05/china-cybersecurity-and-data-protection-laws-change-is-coming.html.

ไว้ชั่วคราว สั่งปิดเว็บไซต์ หรือเพิกถอนการอนุญาตการให้บริการที่เกี่ยวข้องนั้น จนถึงขั้นสั่งเพิกถอนใบอนุญาตให้ประกอบธุรกิจ ในขณะที่บุคคลที่มีหน้าที่รับผิดชอบโดยตรงจะต้องรับผิดส่วนตัวด้วย โดยถูกปรับเป็นเงิน 10,000 หยวน ถึง 100,000 หยวน สำหรับการฝ่าฝืนนั้น

มาตรา 28 ยังบังคับให้ผู้ให้บริการทางเครือข่ายต้องให้ความช่วยเหลือทางเทคนิคและให้การสนับสนุนต่างๆ แก่เจ้าหน้าที่รัฐในการรักษาความมั่นคงของชาติและสืบสวนอาชญากรรม ด้วยเหตุนี้ จึงทำให้เจ้าหน้าที่ของรัฐที่เกี่ยวข้องมีอำนาจกำกับดูแล ตรวจสอบ และบังคับใช้กฎหมายที่กว้างขวางมากขึ้น อย่างไรก็ดี การที่ผู้ให้บริการทางเครือข่ายให้ความร่วมมือกับเจ้าหน้าที่ของรัฐนั้นก็อาจทำให้ข้อมูลของพวกเขามีความเสี่ยงที่จะรั่วไหลได้สูงขึ้นด้วย เนื่องจากเจ้าหน้าที่ของรัฐเองอาจสั่งให้ผู้ให้บริการทางเครือข่ายช่วยเหลือในการเข้าถึงหรือถอดรหัสข้อมูลเพื่อให้ได้มาซึ่งข้อมูลส่วนตัวของผู้ใช้ก็ได้[325] โดยไม่ต้องใช้คำสั่งศาลหรือหมายศาลใด นอกจากนี้ ผู้ให้บริการทางเครือข่ายต้องสร้างช่องทางพิเศษไว้ในระบบของพวกเขาเสมอเพื่อให้รัฐบาลสามารถเข้าถึงข้อมูลต่างๆ ได้[326]

น่าสังเกตว่า กฎหมายความปลอดภัยทางไซเบอร์คล้ายคลึงกับกฎหมายต่อต้านการก่อการร้ายของประเทศจีนเป็นอย่างยิ่ง ซึ่งบังคับให้ผู้ประกอบกิจการโทรคมนาคมและผู้ให้บริการทางอินเทอร์เน็ตต้องส่งมอบวิธีการถอดรหัสข้อมูลรักษาความปลอดภัยและความช่วยเหลือทางเทคนิคต่างๆ ให้แก่รัฐบาลเพื่อป้องกันและสืบสวนกิจกรรมของผู้ก่อการร้าย[327] ถึงแม้รัฐบาลจีนจะอ้างว่า กฎหมายต่อต้านการก่อร้ายร้ายมิได้เรียกร้องให้บริษัทต้องจัดทำช่องทางลัดแก่รัฐบาลแต่อย่างใด แต่ในกฎหมายความปลอดภัยทางไซเบอร์ บริษัทอินเทอร์เน็ตต่างชาติซึ่งอยู่นอกเขตอำนาจศาลของจีนต้องให้ความร่วมมือกับรัฐบาลจีนในการให้ความช่วยเหลือด้านการถอดรหัสข้อมูลหรือสร้างช่องทางพิเศษให้แก่รัฐบาลในการเข้าถึงข้อมูลส่วนบุคคล นอกจากนี้แล้ว กฎหมายฉบับนี้ยังไม่ได้กำหนดขอบเขตการใช้กฎหมายนี้แต่เพียงในเฉพาะกรณีที่จำเป็นหรือวางแนวปฏิบัติให้แก่เจ้าหน้าที่รัฐในการใช้อำนาจแต่อย่างใด

ในกฎหมายความมั่นคงปลอดภัยไซเบอร์จีน ยังได้มอบหน้าที่เฉพาะให้แก่ผู้ให้บริการทางเครือข่ายที่เกี่ยวข้องกับข่าวสารโดยเฉพาะด้วย โดยผู้ให้บริการต้องบริหารจัดการและสอดส่องการกระจายข้อมูลข่าวสารของผู้ใช้งานของตนโดยเข้มงวด หากปรากฏว่าข้อมูลนั้นมีเนื้อหาที่ขัดต่อกฎหมายหรือกฎของฝ่ายบริหาร โดยหากเนื้อหานั้นปรากฏขึ้น ผู้ให้บริการต้องลบและสกัดกั้นการแพร่กระจายของเนื้อหานั้น พร้อมทั้งบันทึก

---

[325] Kelley, Katherine W. 2017. "China's Cybersecurity Law Goes into Effect June 1, 2017—Are You Ready?". National Association of Corporate Directors. https://blog.nacdonline.org/posts/chinas-cybersecurity-law-goes-into-effect-june-1-2017-are-you-ready.

[326] itnews. 2016. "China's New Cyber Security Laws Will 'Lock Out' Businesses". Nextmedia. https://www.itnews.com.au/news/chinas-new-cyber-security-laws-will-lock-out-businesses-440929.

[327] Shackelford, Scott, Scott Russell, and Andreas Kuehn. 2016. "Unpacking the International Law on Cybersecurity Due Diligence: Lessons from The Public and Private Sectors". Chicago Journal of International Law 17 (1): 1, 25.

เหตุการณ์ดังกล่าวและรายงานแก่หน่วยงานที่มีส่วนเกี่ยวข้องให้ทราบ[328] หากผู้ให้บริการไม่ปฏิบัติตาม ในเบื้องต้นจะถูกตักเตือนและสั่งให้แก้ไขโดยเร็ว แต่หากผู้ให้บริการนั้นไม่ปฏิบัติตาม หรือก่อให้เกิดความเสียหายร้ายแรง ผู้ให้บริการจะถูกปรับตั้งแต่ 1 แสนหยวนขึ้นไปแต่ไม่เกิน 550,000 หยวน พร้อมทั้งถูกสั่งให้ระงับการประกอบกิจการในส่วนที่เกี่ยวข้อง ปิดเว็บไซต์ หรือระงับการประกอบกิจการทุกภาคส่วน รวมทั้งการระงับใบอนุญาตประกอบกิจการทั้งชั่วคราวหรือถาวร และผู้ที่มีหน้าที่รับผิดชอบในการดูแลส่วนนั้นโดยตรงจะถูกปรับตั้งแต่ 1 หมื่นหยวนขึ้นไปแต่ไม่เกิน 1 แสนหยวน[329]

ตัวอย่างที่มีชื่อเสียงคือ ในเดือนสิงหาคม ค.ศ. 2017 หลังจากที่กฎหมายความมั่นคงปลอดภัยไซเบอร์ประกาศใช้ไปแล้วประมาณ 2 เดือน คณะกรรมการไซเบอร์เสปซมลฑลกวางตุ้ง ได้ประกาศว่าบริษัทวีแชทและเทนเซนยังไม่ได้ทำตามหน้าที่ที่กฎหมายกำหนดไว้สำหรับผู้ให้บริการทางเครือข่ายที่เกี่ยวข้องกับข่าวสาร โดยเฉพาะ เทนเซนยังไม่สามารถระงับการแพร่กระจายข้อเนื้อหาที่ก่อให้เกิดการจลาจล ข่าวปลอม และสื่อลามกต่าง ๆ ได้ ในขณะที่บริษัทวีแชทมีปัญหาในการยับยั้งการแพร่กระจายของเนื้อหาลามก และเนื้อหาที่ก่อให้เกิดความเกลียดชัง และกำหนดจำนวนค่าปรับที่ต้องจ่ายในอัตราสูงสุดคือ 550,000 หยวน แก่ทั้งสองบริษัท

2) เปรียบเทียบกฎหมายของประเทศสหรัฐอเมริกาและสหภาพยุโรป

กฎหมายสหรัฐอเมริกา

จากการศึกษา ไม่พบว่าประเทศสหรัฐอเมริกามีกฎหมายเกี่ยวกับประเด็นนี้

กฎหมายสหภาพยุโรป

ในปี ค.ศ. 2016 สหภาพยุโรปได้ออกกฎหมายชื่อ Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union ขึ้น โดยในมาตรา 16 ได้กำหนดให้ประเทศสมาชิกต้องจัดให้ผู้ให้บริการดิจิทัลในประเทศของตนมีมาตรการที่เหมาะสมในการบริหารจัดการความเสี่ยงที่อาจเกิดต่อระบบข้อมูลและเครือข่าย อันได้แก่ การตลาดออนไลน์ (online marketplace) การให้บริการเครื่องมือค้นหาออนไลน์ (online search engine) และการจัดเก็บข้อมูลออนไลน์ (cloud computing service)

เมื่อปี ค.ศ. 2018 สหราชอาณาจักรได้ออกกฎหมายฉบับแรกที่ให้หน้าที่แก่ผู้บริการทางเครือข่ายเพื่อให้เป็นไปตามกฎหมายของสหภาพยุโรป โดยกฎหมายนั้นคือระเบียบว่าด้วยระบบข้อมูลและเครือข่าย (Network and Information Systems Regulations) ได้ให้นิยามคำว่า ผู้ให้บริการดิจิทัล (digital service provider) ไว้ว่า[330] “บุคคลใดก็ตามที่ให้บริการดิจิทัล” ซึ่งโดยทั่วไปแล้ว ไม่มีหน้าที่ใดโดยเฉพาะเจาะจงตาม

[328] 《中华人民共和国网络安全法》第 47 条

[329] 《中华人民共和国网络安全法》第 68 条 第一款

[330] ส่วนที่ 1 (1) Network and Information Systems Regulations

กฎหมายฉบับนี้ อย่างไรก็ดี หากผู้ให้บริการดิจิทัลนั้นจัดเป็นผู้ให้บริการดิจิทัลที่เกี่ยวข้อง (relevant digital service provider) คือ[331] “เป็นผู้ให้บริการดังกล่าวในสหภาพยุโรปและมีคุณสมบัติทั้งสองข้อพร้อมกันต่อไปนี้ คือ 1. มีบริษัทหลักอยู่ในสหราชอาณาจักร และ 2. เป็นองค์กรธุรกิจที่มิใช่ขนาดกลางหรือขนาดเล็ก” ผู้ให้บริการดิจิทัลที่เกี่ยวข้องจะต้องมีหน้าที่ตามกฎหมายดังต่อไปนี้คือ หากปรากฏว่าผู้ให้บริการดิจิทัลให้บริการใดให้บริการเครื่องมือค้นหาออนไลน์ ตลาดออนไลน์ หรือจัดเก็บข้อมูลออนไลน์ จัดทำมาตรการในการบริหารจัดการความเสี่ยงที่อาจเกิดขึ้นต่อความปลอดภัยของระบบข้อมูลและเครือข่าย โดยมาตรการเช่นว่านั้นต้องเหมาะสม มีประสิทธิภาพในการป้องกันอันตรายที่จะเกิดขึ้นได้จริง ทั้งนี้ให้คำนึงถึงขีดจำกัดความสามารถของเทคโนโลยีในขณะนั้น (state of art) และหากมีภยันตรายเกิดขึ้น ผู้ให้บริการดิจิทัลก็มีหน้าที่ต้องแจ้งให้คณะกรรมการทราบด้วย[332]

3) เปรียบเทียบกฎหมายของประเทศไทย

มาตรา 3 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้ให้นิยามคำว่าผู้ให้บริการไว้ว่า หมายถึงบุคคล 2 ประเภท

ประเภทแรกได้แก่ บุคคลที่ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่นโดยผ่านทางระบบคอมพิวเตอร์ ไม่ว่าจะเป็นการให้บริการด้วยตนเองหรือให้บริการในนามของบุคคลอื่น

ประเภทที่สองได้แก่ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์ เพื่อประโยชน์ของบุคคลอื่น[333] โดยผู้ที่เป็นผู้ให้บริการมีหน้าที่ตามกฎหมายดังต่อไปนี้

[331] ส่วนที่ 1 (3)(e) Network and Information Systems Regulations

[332] ส่วนที่ 4 Network and Information Systems Regulations

[333] มาตรา 3 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

1. ไม่สนับสนุนหรือยินยอมให้มีการกระทำความผิดตามมาตรา 14[334] ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน มิฉะนั้นต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา 14[335]

2. ให้ความช่วยเหลือแก่พนักงานเจ้าหน้าที่ที่มีอำนาจในการส่งมอบข้อมูลดังต่อไปนี้เพื่อประโยชน์ในการสืบสอนหรือสอบสวน[336]

1. ข้อมูลจราจรทางคอมพิวเตอร์เกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์

2. ข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บหรือที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการเอง

ทั้งนี้ เจ้าพนักงานที่มีอำนาจในการสืบสวนหรือสอบสวน หากต้องการเรียกข้อมูลข้างต้นจะต้องมีคำสั่งศาลก่อน[337] เว้นเสียแต่ว่าจะปรากฏเหตุผลพิเศษคือ 1.) มีเหตุอันควรเชื่อได้ว่า มีการกระทำความผิดตามพระราชบัญญัตินี้ และ 2.) การขอข้อมูลดังกล่าวเป็นไปเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด และหาตัวผู้กระทำความผิด และ 3.) การขอข้อมูลนั้นมีความจำเป็น หากปรากฏเหตุพิเศษนี้ครบทั้งสามข้อ เจ้าพนักงานที่มีอำนาจอาจสั่งให้ผู้ให้บริการส่งมอบข้อมูลแก่ตนได้ทันที โดยมิต้องได้รับอนุญาตจากศาลก่อน[338]

3. ผู้ให้บริการอาจมีหน้าที่ต้องระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ หากปรากฏว่าข้อมูลคอมพิวเตอร์นั้นมีเนื้อหาที่อาจกระทบกระเทือนต่อความมั่นคงของประเทศ ตามที่กำหนดไว้ในภาคสอง

---

[334] มาตรา 15 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 บัญญัติไว้ว่า “ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

(1) นำเข้าสู่ระบบคอมพิวเตอร์ ซึ่งข้อมูลคอมพิวเตอร์ปลอม ไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน

(2) นำเข้าสู่ระบบคอมพิวเตอร์ ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

(3) นำเข้าสู่ระบบคอมพิวเตอร์ ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร หรือความผิดเกี่ยวกับการก่อการร้าย ตามประมวลกฎหมายอาญา

(4) นำเข้าสู่ระบบคอมพิวเตอร์ ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามก และข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

(5) เผยแพร่ หรือส่งต่อ ซึ่งข้อมูลคอมพิวเตอร์ โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม (1) (2) (3) หรือ (4)

[335] มาตรา 15 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

[336] มาตรา 18 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

[337] มาตรา 19 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

[338] มาตรา 18 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

ลักษณะ 1[339] หรือลักษณะ 1/1[340] แห่งประมวลกฎหมายอาญา หรือที่มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน และพนักงานเจ้าหน้าที่ ซึ่งได้รับความเห็นชอบจากรัฐมนตรีแล้ว อาจยื่นคำร้องพร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจ ขอให้มีคำสั่งระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้นได้ และภายหลังจากที่ศาลมีคำสั่งให้ระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้นแล้ว ผู้ให้บริการต้องระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้น หากได้รับคำสั่งจากเจ้าหน้าที่[341]

4. ผู้ให้บริการมีหน้าที่ต้องเก็บข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ หรืออาจเกินกว่านั้นก็ได้ หากได้รับคำสั่งจากพนักงานเจ้าหน้าที่ แต่ทั้งนี้ระยะเวลาดังกล่าวต้องไม่เกิน 1 ปี โดยข้อมูลที่ผู้ให้บริการต้องเก็บนั้นต้องเพียงพอเพื่อให้สามารถระบุตัวผู้ใช้บริการ โดยให้เก็บตั้งแต่วันที่เข้าใช้บริการ และสามารถกำจัดออกได้ หลังจากที่ผ่านพ้นวันสิ้นสุดการให้บริการไปแล้วเป็นเวลา 90 วัน[342]

ในปี พ.ศ. 2560 ได้มีการแก้ไขพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 โดยใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 ทำให้หน้าที่ของผู้ให้บริการเปลี่ยนไปจากเดิมบ้าง ดังต่อไปนี้

1. จากเดิมที่ผู้ให้บริการต้องไม่สนับสนุนหรือยินยอมให้มีการกระทำความผิดตามมาตรา 14 ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน มิฉะนั้นต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา 14 ได้เปลี่ยนเป็นผู้ให้บริการต้องไม่ให้ความร่วมมือ ยินยอม หรือรู้เห็นเป็นใจให้มีการกระทำความผิด มิฉะนั้นต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา 14 ด้วย[343]

2. จากเดิมที่ผู้ให้บริการต้องส่งมอบข้อมูลให้แก่พนักงานเจ้าหน้าที่ก็ต่อเมื่อมีเหตุผลพิเศษเท่านั้นคือ 1.) มีเหตุอันควรเชื่อได้ว่า มีการกระทำความผิดตามพระราชบัญญัตินี้ และ 2.) การขอข้อมูลดังกล่าวเป็นไปเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด และหาตัวผู้กระทำความผิด และ 3.) การขอข้อมูลนั้นมีความจำเป็น ได้เปลี่ยนเป็นว่า องค์ประกอบของเหตุผลพิเศษในข้อ 1.) นอกจากการเชื่อว่ามีเหตุอัน

---

[339] ฐานความผิดที่ถูกระบุไว้ในภาคสอง ลักษณะ 1 แห่งประมวลกฎหมายอาญา ชื่อว่า ความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร และประกอบด้วย 4 หมวดย่อยภายใน ได้แก่ หมวด1 ความผิดต่อองค์พระมหากษัตริย์ พระราชินี รัชทายาท และผู้สำเร็จราชการแทนพระองค์ (มาตรา 107-112) หมวด2 ความผิดต่อความมั่งคงของรัฐ ภายในราชอาณาจักร (มาตรา 113-118) หมวด3 ความผิดต่อความมั่นคงของรัฐ ภายนอกราชอาณาจักร (มาตรา 119-129) และ หมวด4 ความผิดต่อสัมพันธไมตรี กับต่างประเทศ (มาตรา 130-135)

[340] ฐานความผิดที่ถูกระบุไว้ในภาคสอง ลักษณะ 1/1 แห่งประมวลกฎหมายอาญา ชื่อว่า ความผิดเกี่ยวกับการก่อการร้าย (มาตรา 135/1-135/4)

[341] มาตรา 20 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

[342] มาตรา 26 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

[343] มาตรา 9 พระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

ควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้แล้วนั้น หากพนักงานเจ้าหน้าที่ได้รับคำร้องขอจากพนักงานสอบสวน ก็สามารถเอาเหตุนี้มาแทนองค์ประกอบดังกล่าวได้เช่นกัน[344]

3. จากเดิมที่ผู้ให้บริการต้องระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ หากปรากฏว่าข้อมูลคอมพิวเตอร์นั้นมีเนื้อหาที่อาจกระทบกระเทือนต่อความมั่นคงของประเทศ ตามที่กำหนดไว้ในภาคสองลักษณะ 1 หรือลักษณะ 1/1 แห่งประมวลกฎหมายอาญา ได้มีการเพิ่มหมวดความผิดอีกสองหมวดเข้ามาด้วย คือ[345]

1) ข้อมูลคอมพิวเตอร์ที่เป็นความผิดตามกฎหมายนี้

2) ข้อมูลคอมพิวเตอร์ที่เป็นความผิดอาญาตามกฎหมายเกี่ยวกับทรัพย์สินทางปัญญาหรือกฎหมายอื่น ซึ่งข้อมูลคอมพิวเตอร์นั้นมีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชนและเจ้าหน้าที่ตามกฎหมายนั้นหรือพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญาได้ร้องขอ

ดังนั้นแล้ว หากพนักงานเจ้าหน้าที่ ซึ่งได้รับความเห็นชอบจากรัฐมนตรีแล้ว ยื่นคำร้องและแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจ ขอให้มีคำสั่งระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ประเภทนั้นๆ แล้ว ผู้ให้บริการก็ต้องระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้นด้วย หากได้รับคำสั่งจากเจ้าหน้าที่[346]

3) จากเดิมที่ผู้ให้บริการมีหน้าที่ต้องเก็บข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าระยะเวลาที่กฎหมายกำหนดไว้นั้น เว้นแต่พนักงานเจ้าหน้าที่จะสั่งให้เก็บเกินกว่าระยะเวลาที่กฎหมายกำหนด แต่ทั้งนี้ระยะเวลาที่เจ้าหน้าที่สั่งต้องไม่เกิน 1 ปี ทว่าสำหรับกฎหมายใหม่ ได้มีการแก้ไขให้เจ้าพนักงานสามารถสั่งให้ผู้ให้บริการเก็บข้อมูลไว้ได้ยาวนานที่สุดคือ 2 ปี[347]

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เป็นกฎหมายฉบับแรกที่กำหนดหน้าที่ให้แก่ผู้ให้บริการทางเครือข่าย โดยหน้าที่สำคัญของผู้ให้บริการทางเครือข่ายไม่ใช่การรักษาเสถียรภาพของระบบที่ตนให้บริการให้สามารถทำงานต่อไปได้ แต่เป็นหน้าที่การช่วยเหลือรัฐในการป้องปรามการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กฎหมายฉบับนี้ได้เอาผิดแก่ผู้ให้บริการที่สนับสนุนหรือยินยอมให้มีการกระทำความผิดตามกฎหมายฉบับนี้ ให้ความช่วยเหลือแก่พนักงานเจ้าหน้าที่ในการสืบสวนสอบสวนอาชญากรรม ระงับการเผยแพร่ข้อมูลที่ต้องห้ามตามกฎหมายนี้ รวมถึงการเก็บข้อมูลการเข้าสู่ระบบคอมพิวเตอร์ของผู้ใช้บริการไว้เป็นระยะเวลาอย่างน้อย 90 วัน จะเห็นได้ว่าไม่มีมาตราใดหรือกฎหมายอื่นใดที่กล่าวถึงหน้าที่ของผู้ให้บริการในการเสริมสร้างระบบการรักษาความปลอดภัยของตน แม้เมื่อมีการแก้ไข

---

[344] มาตรา 13 พระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

[345] มาตรา 14 พระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

[346] เรื่องเดียวกัน.

[347] มาตรา 17 พระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

กฎหมายฉบับนี้อีกครั้งโดยพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 ผู้ให้บริการก็ยังคงมีหน้าที่เพียงช่วยรัฐในการปราบปรามอาชญากรรมแต่เพียงเท่านั้น

หากสังเกตกฎหมายของสหภาพยุโรปและประเทศจีนเกี่ยวกับหน้าที่ตามกฎหมายของผู้ให้บริการทางเครือข่าย จะพบว่าสหภาพยุโรปไม่ได้มองว่าหน้าที่ของผู้ให้บริการเครือข่ายคือการช่วยรัฐปราบปรามความผิดเกี่ยวกับคอมพิวเตอร์แต่อย่างใด หากแต่หน้าที่ของผู้ให้บริการเครือข่ายคือการจัดให้มีมาตรการที่เหมาะสมในการบริหารจัดการความเสี่ยงไซเบอร์ ในขณะที่ประเทศจีนกลับกำหนดให้หน้าที่ของผู้ให้บริการเครือข่ายเป็นไปได้ทั้งสองประการคือช่วยรัฐในการปราบปรามอาชญากรรมคอมพิวเตอร์ และกำหนดหน้าที่ให้ผู้ให้บริการในการจัดทำมาตรการป้องกันความเสี่ยงไซเบอร์ที่เหมาะสมไปพร้อมๆ กันด้วย ในขณะที่กฎหมายของสหรัฐอเมริกานั้น ไม่ปรากฏว่าได้กำหนดหน้าที่ใดๆ แก่ผู้ให้บริการ

4.2 การปกป้องระบบโครงสร้างพื้นฐานสำคัญ

1) กฎหมายจีน

“ระบบโครงสร้างพื้นฐานสำคัญ” หมายถึง สิ่งอำนวยความสะดวก ระบบ และเครือข่ายที่สำคัญของประเทศในทางเศรษฐกิจหรือสังคม ซึ่งเกี่ยวข้องกับสินค้าหรือบริการที่มีประเด็นของความมั่นคงของชาติ เสถียรภาพทางเศรษฐกิจ สุขอนามัยของประชาชนเข้ามาเกี่ยวข้อง จะเห็นได้ว่ามีความหมายที่กว้างขวางมาก อันอาจรวมไปถึงการเกษตร อาหาร น้ำ พลังงาน สุขอนามัย การสื่อสาร การคมนาคม ระบบการเงิน เป็นต้น

ระบบโครงสร้างพื้นฐานสำคัญมีแนวโน้มว่าจะตกเป็นเหยื่อจากการโจมตีทางไซเบอร์ได้สูง ด้วยเหตุนี้การปกป้องระบบโครงสร้างพื้นฐานสำคัญจึงกลายเป็นนโยบายสำคัญที่มีส่วนเกี่ยวข้องโดยตรงกับความมั่นคงปลอดภัยไซเบอร์ เมื่อปรากฏว่าระบบโครงสร้างพื้นฐานสำคัญมักอยู่ในการครอบครองของเอกชน การรักษาความปลอดภัยจากการถูกโจมตีนั้นอาจถูกละเลย เนื่องจากเอกชนขาดแรงจูงใจที่จะจัดการรักษาความปลอดภัยอย่างเพียงพอ ดังนั้น รัฐบาลจึงควรสร้างมาตรการจูงใจ เพื่อสนับสนุนให้เอกชนลงทุนในด้านความมั่นคงไซเบอร์ด้วย

ตั้งแต่ค.ศ. 2003 ประเทศจีนได้เล็งเห็นถึงความสำคัญของการปกป้องความมั่นคงไซเบอร์และระบบโครงสร้างพื้นฐานสำคัญ จนนำมาสู่การออกกฎหมายความปลอดภัยทางไซเบอร์ในปัจจุบัน โดยมาตรา 31 ของกฎหมายนี้ได้เน้นถึงความสำคัญของระบบโครงสร้างพื้นฐานสำคัญที่เกี่ยวกับข้อมูล โดยข้อมูลเหล่านั้นรวมไปถึง การโทรคมนาคม การจัดการน้ำ ธนาคารและการเงิน พลังงาน การคมนาคม และไฟฟ้า และสิ่งอื่นๆ ซึ่งหากถูกทำลาย ทำให้เสียหาย หรือเกิดการรั่วไหล จะทำให้เกิดผลเสียมหาศาลต่อความมั่นคงของชาติ สวัสดิการสาธารณะ ความเป็นอยู่ของประชาน หรือประโยชน์สาธารณะ

ถึงแม้กฎหมายนี้จะกำหนดให้คณะรัฐมนตรีกำหนดขอบเขตและมาตรการป้องกันความปลอดภัยของระบบโครงสร้างพื้นฐานสำคัญให้ชัดเจน ทำให้เกิดความกังวลว่ากฎหมายนี้มีเนื้อหาที่กว้างเกินไป เนื่องจากคณะรัฐมนตรีย่อมจะมีดุลพินิจที่จะกำหนดได้ว่าธุรกิจอินเทอร์เน็ตใดมีความเกี่ยวข้องกับ “ความมั่นคงของชาติ สวัสดิการสาธารณะ ความเป็นอยู่ของประชาน หรือประโยชน์สาธารณะ” บ้าง เมื่อบริษัทใดจัดว่าเป็นผู้ทำธุรกิจที่เกี่ยวข้องกับระบบโครงสร้างพื้นฐานสำคัญด้านข้อมูล หรือมีข้อมูลของประชาชนหรือบริษัทจีนอยู่เป็นจำนวนมาก กรณีนี้ก็อาจถือได้ว่าบริษัทนั้นเป็น “ผู้ให้บริการเครือข่ายที่เกี่ยวข้องกับระบบโครงสร้างพื้นฐานสำคัญ” ได้ โดยนิยามนี้มีความกว้างขวางมากจนอาจรวมไปถึงบริษัทขนส่งอาหารในประเทศจีนด้วย นอกจากนี้ ในมาตรา 31 ยังใช้ศัพท์ซึ่งกำกวม โดยคำว่า “ความเป็นอยู่ของประชาชน” และ “ประโยชน์สาธารณะ” ก็เป็นคำที่มีความหมายกว้างขวางและอาจตีความขยายความให้คลอบคลุมได้หลายกิจการ

ถึงแม้ผู้ให้บริการระบบโครงสร้างพื้นฐานสำคัญจะเป็นส่วนหนึ่งในนิยามของคำว่า ผู้ให้บริการทางเครือข่าย แต่การให้บริการระบบโครงสร้างพื้นฐานสำคัญกลับมีภาระทางกฎหมายมากกว่าผู้ให้บริการทางเครือข่ายประเภทอื่น จากมาตรา 34 ผู้ให้บริการทางเครือข่ายที่เกี่ยวข้องกับระบบโครงสร้างพื้นฐานสำคัญนอกจากจะต้องปฏิบัติตามหน้าที่ที่ผู้ให้บริการทางเครือข่ายทั่วไปต้องปฏิบัติตามแล้ว ยังต้องปฏิบัติตามหน้าที่เพิ่มเติมดังต่อไปนี้ด้วยคือ[348]

1. จัดให้มีเครื่องมือและบุคคลที่รับผิดชอบเกี่ยวกับความปลอดภัยเฉพาะด้านเพื่อปกป้องข้อมูลของระบบโครงสร้างพื้นฐานสำคัญโดยเฉพาะ และจัดให้มีการตรวจสอบประวัติเบื้องหลังของผู้ที่จะมาทำหน้าที่ดังกล่าวนั้นด้วย

2. จัดให้มีการอบรมและการทดสอบความรู้ทางเทคนิคแก่บุคลากรที่ทำหน้าที่รับผิดชอบในด้านนี้เป็นประจำ โดยระบุระยะเวลาไว้อย่างชัดเจน

3. จัดให้มีการสำรองข้อมูลในกรณีฉุกเฉินแก่ระบบและข้อมูลที่สำคัญ

4. จัดให้มีแผนการรับมือกรณีที่มีการคุกคามทางไซเบอร์ฉุกเฉิน และมีการซ้อมการรับมือ โดยระบุระยะเวลาไว้อย่างชัดเจน

5. ทำตามที่กฎหมายหรือมาตรการของฝ่ายบริหารกำหนด

หากผู้ให้บริการทางเครือข่ายที่เกี่ยวข้องกับระบบโครงสร้างพื้นฐานสำคัญไม่ปฏิบัติตามมาตรา 34 ในเบื้องต้นจะถูกหน่วยงานที่เกี่ยวข้องตักเตือนและสั่งให้แก้ไข หากไม่แก้ไขหรือเพราะการไม่ปฏิบัติตามกฎหมายนั้นก่อให้เกิดผลกระทบที่ร้ายแรงต่อความมั่นคงปลอดภัยไซเบอร์ ผู้ให้บริการทางเครือข่ายจะถูกปรับตั้งแต่ 1

[348] 《中华人民共和国网络安全法》第 34 条

แสนหยวนขึ้นไปแต่ไม่เกิน 1 ล้านหยวน และผู้ที่มีหน้าที่รับผิดชอบในการดูแลความมั่นคงปลอดภัยไซเบอร์โดยตรงจะถูกปรับตั้งแต่ 1 หมื่นหยวนขึ้นไปแต่ไม่เกิน 1 แสนหยวน[349]

2) เปรียบเทียบกฎหมายของประเทศสหรัฐอเมริกาและสหภาพยุโรป

กฎหมายสหรัฐอเมริกา

กระทรวงความมั่นคงแห่งมาตุภูมิ (Department of Homeland Security) ได้ให้นิยามความหมายของคำว่าระบบโครงสร้างพื้นฐานสำคัญไว้ว่า[350] “เป็นสินทรัพย์หรือระบบ ไม่ว่าจะปรากฏในรูปกายภาพหรือในพื้นที่ไซเบอร์ อันมีความสำคัญอย่างยิ่งต่อประเทศชาติ โดยหากสินทรัพย์หรือระบบดังกล่าวหยุดทำงานหรือถูกทำลาย ประเทศชาติ เศรษฐกิจ สังคมหรือสุขอนามัยของคนในชาติจะได้รับความเสียหายอย่างยิ่ง”

เมื่อปี ค.ศ. 2018 ประธานาธิบดีโดนัลด์ ทรัมป์ ได้ลงนามในกฎหมายชื่อว่า รัฐบัญญัติองค์การความมั่นคงปลอดภัยไซเบอร์และระบบโครงสร้างพื้นฐานสำคัญ (Cybersecurity and Infrastructure Security Agency Act) โดยกฎหมายฉบับนี้ได้จัดตั้งองค์การความมั่นคงปลอดภัยไซเบอร์และระบบโครงสร้างพื้นฐานสำคัญขึ้นมา โดยให้อยู่ในสังกัดของกระทรวงความมั่นคงแห่งมาตุภูมิ[351] และมีหน่วยงานภายในแยกย่อยซึ่งมีหน้าที่ดูแลเกี่ยวกับระบบโครงสร้างพื้นฐานสำคัญไว้โดยเฉพาะ คือ หน่วยงานความมั่นคงปลอดภัยของโครงสร้างพื้นฐาน (Infrastructure Security Division)

หน่วยงานความมั่นคงปลอดภัยของโครงสร้างพื้นฐานมีหน้าที่ในการเป็นตัวกลางประสานงานและให้ความร่วมมือกับทั้งภาครัฐและเอกชน เพื่อช่วยให้ระบบโครงสร้างพื้นฐานสำคัญปลอดภัยจากการถูกโจมตี พร้อมทั้งช่วยเสริมสร้างความรู้ความเข้าใจเกี่ยวกับความเสี่ยงและอันตรายที่อาจเกิดขึ้นต่อระบบโครงสร้างพื้นฐานนั้น รวมไปถึงการแบ่งปันข้อมูลต่าง ๆ ที่อาจเป็นประโยชน์ต่อการปกป้องระบบโครงสร้างพื้นฐานให้แก่กัน โดยไม่ว่าระบบโครงสร้างพื้นฐานนั้นจะอยู่ในรูปแบบทางกายภาพหรือในพื้นที่ไซเบอร์ก็ตาม [352]

สำหรับระบบโครงสร้างพื้นฐานสำคัญนั้น เป็นรูปแบบระบบโครงสร้างพื้นฐานที่เสี่ยงต่อการถูกโจมตีมากกว่าระบบโครงสร้างพื้นฐานธรรมดา ด้วยเหตุนี้ หน่วยงานความมั่นคงปลอดภัยของโครงสร้างพื้นฐานจึงได้

[349]《中华人民共和国网络安全法》第 59 条 第二款

[350] Department Of Homeland Security. 2020. "Critical Infrastructure Security". Cisa.Gov. https://www.dhs.gov/topic/critical-infrastructure-security.

[351] Department Of Homeland Security. 2020. "ABOUT CISA". Cisa.Gov. https://www.cisa.gov/about-cisa.

[352] Department Of Homeland Security. 2020. "Infrastructure Security Division | CISA". Cisa.Gov. https://www.cisa.gov/infrastructure-security-division.

ทำการระบุให้ชัดเจนว่าสิ่งใดบ้างเป็นระบบโครงสร้างพื้นฐานสำคัญ โดยแต่ละประเภทต่างมีแผนการจัดการเฉพาะ (Sector-Specific Plan) ซึ่งอาจแบ่งออกได้เป็น 16 ประเภทดังต่อไปนี้คือ:[353]

1. ภาควิทยาศาสตร์การเคมี
2. ภาคหน่วยงานเชิงพาณิชย์
3. ภาคการโทรคมนาคม
4. ภาคอุตสาหกรรมการผลิตสำคัญ
5. ภาคการบริหารจัดการน้ำ
6. ภาคอุตสาหกรรมป้องกันประเทศ
7. ภาคการให้บริการฉุกเฉิน
8. ภาคอุตสาหกรรมพลังงาน
9. ภาคการให้บริการทางการเงิน
10. ภาคอาหารและการเกษตร
11. ภาคหน่วยงานรัฐ
12. ภาคสาธารณสุข
13. ภาคเทคโนโลยีและการสื่อสาร
14. ภาคอุตสาหกรรมนิวเคลียร์
15. ภาคการคมนาคม
16. ภาคการบริหารจัดการเขื่อน

หากพิจารณาแผนการจัดการเฉพาะของแต่ละภาคจะพบว่าทุกแผนการจัดการจะมีบทของเนื้อหาที่กล่าวถึงความมั่นคงปลอดภัยไซเบอร์ไว้เป็นการเฉพาะ ว่าอุตสาหกรรมนั้นควรใช้เทคโนโลยีใด หรือวางระบบเช่นไร โดยมีเป้าหมายเดียวกันคือเพื่อป้องกันการถูกรุกรานจากภายนอก อย่างไรก็ดี ทั้งในรัฐบัญญัติองค์การความมั่นคงปลอดภัยไซเบอร์และระบบโครงสร้างพื้นฐานสำคัญ และในแผนการจัดการเฉพาะล้วนต่างไม่ได้กล่าวถึงบทลงโทษหากไม่มีการปฏิบัติตาม จึงอาจสรุปได้ว่าทั้งหน่วยงานภาครัฐและเอกชนที่มีภารกิจหรือกิจการเกี่ยวข้องกับระบบโครงสร้างพื้นฐานสำคัญ อาจไม่ต้องทำตามมาตรการเหล่านั้นก็ได้ และการจะป้องกันหรือไม่นั้น ขึ้นอยู่กับความสมัครใจของหน่วยงานรัฐหรือเอกชนเอง

กฎหมายสหภาพยุโรป

จาก COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve

[353] Department Of Homeland Security. 2020. "Critical Infrastructure Sectors". Cisa.Gov. https://www.cisa.gov/critical-infrastructure-sectors.

their protection ระบบโครงสร้างพื้นฐานสำคัญ (critical infrastructure) หมายถึง[354] “สินทรัพย์ ระบบหรือส่วนใดของสิ่งดังกล่าวในข้างต้น ซึ่งตั้งอยู่ในอาณาเขตของประเทศสมาชิก และมีส่วนสำคัญต่อความเป็นอยู่ของสังคม สุขอนามัย ความปลอดภัย ความมั่นคง เศรษฐกิจ หรือความเป็นอยู่ของประชาชน และการทำลายหรือการรบกวนซึ่งสิ่งนั้นอาจก่อให้เกิดผลกระทบรุนแรงต่อประเทศสมาชิก” และกฎหมายฉบับนี้มีเนื้อหาโดยรวมคือการให้ประเทศสมาชิกร่วมกันปกป้องระบบโครงสร้างพื้นฐานสำคัญเหล่านั้น หากปรากฏว่าการรบกวนหรือทำลายระบบโครงสร้างพื้นฐานสำคัญนั้นกระทบต่อผลประโยชน์ของประเทศสมาชิกตั้งแต่ 2 ประเทศเป็นต้นไป แต่ทั้งนี้ ไม่ได้กล่าวถึงการบังคับให้ประเทศสมาชิกปกป้องระบบโครงสร้างพื้นฐานสำคัญที่อยู่แต่เฉพาะในประเทศตนเองเท่านั้นแต่อย่างใด

จนกระทั่งในปี ค.ศ. 2013 สหภาพยุโรปได้ออกกฎหมายอีกหนึ่งฉบับที่เกี่ยวกับการปกป้องระบบโครงสร้างพื้นฐานคือ Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 โดยกฎหมายนี้ได้จัดตั้งองค์กรเพื่อความมั่นคงของของเครือข่ายและข้อมูลข่าวสารแห่งสหภาพยุโรปขึ้น (European Union Agency for Network and Information Security) และภายหลังได้เปลี่ยนชื่อเป็นองค์กรเพื่อความมั่นคงปลอดภัยไซเบอร์ (European Union Agency for Cybersecurity) เพื่อสร้างความตระหนักรู้ในเรื่องความมั่นคงของเครือข่ายและข้อมูล อันอาจเป็นประโยชน์ต่อประชาชน ผู้บริโภค องค์กรธุรกิจ และหน่วยงานภาครัฐของประเทศสมาชิกเอง[355] โดยไม่ต้องพิจารณาอีกว่าการรบกวนหรือทำลายระบบโครงสร้างพื้นฐานนั้นจะกระทบต่อประเทศสมาชิกอื่นหรือไม่

ในบทนำของกฎหมายฉบับนี้เน้นให้เห็นถึงความสำคัญว่า ความมั่นคงของข้อมูลข่าวสารและบริการที่เกี่ยวข้องมีความสำคัญเช่นเดียวกันกับระบบโครงสร้างพื้นฐานสำคัญอื่น อาทิ ระบบการบริหารจัดการน้ำ หรือการจัดการไฟฟ้า และหากข้อมูลข่าวสารและบริการที่เกี่ยวข้องถูกรบกวน ผลเสียจะเกิดขึ้นแก่เศรษฐกิจและสังคม ด้วยเหตุเช่นนี้ จึงเป็นที่มาของการจัดตั้งองค์กรดังกล่าวขึ้น และให้มีหน้าที่ในการให้คำแนะนำแก่ประเทศสมาชิกเพื่อยกระดับมาตรฐานความปลอดภัยของระบบโครงสร้างพื้นฐานสำคัญ

เมื่อปี ค.ศ. 2019 สหภาพยุโรปได้ออกกฎหมายฉบับใหม่ขึ้น คือ REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology

---

[354] มาตรา 2 (a) COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection

[355] มาตรา 1 Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004

cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) เพื่อเพิ่มบทบาทหน้าที่ขององค์กรนี้ในด้านของการรับรองมาตรฐานความปลอดภัยและการตรวจสอบคุณภาพอุปกรณ์ แต่ทั้งนี้ ในด้านการปกป้องระบบโครงสร้างพื้นฐานสำคัญนั้น องค์กรนี้ยังคงมีหน้าที่เพียงให้คำแนะนำต่าง ๆ แก่ประเทศสมาชิกหรือหน่วยงานเอกชนเท่านั้น เพื่อให้ประเทศสมาชิกนำไปออกกฎหมายภายในของประเทศตนต่อไป หรือเพื่อให้เอกชนรับมาตรการเหล่านั้นไปปฏิบัติเองตามสมควร

3) เปรียบเทียบกฎหมายของประเทศไทย

คำว่า “โครงสร้างพื้นฐานสำคัญ” ในเชิงความหมายของความมั่นคงปลอดภัยไซเบอร์นี้ ได้ถูกบัญญัติอยู่ในพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 โดยมาตรา 3 ได้นิยามให้คำว่า “โครงสร้างพื้นฐานสำคัญทางสารสนเทศ” หมายความว่า “คอมพิวเตอร์หรือระบบคอมพิวเตอร์ ซึ่งหน่วยงานของรัฐหรือหน่วยงานเอกชนใช้ในกิจการของตนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของรัฐ ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ” หน่วยงานของรัฐหรือ หน่วยงานเอกชนใดที่ได้ให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จะถูกเรียกว่า “หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ”

ในมาตรา 48 ของกฎหมายนี้ก็ได้เน้นย้ำให้เห็นถึงความสำคัญของโครงสร้างพื้นฐานสำคัญทางสารสนเทศขึ้นมาอีกว่า “โครงสร้างพื้นฐานสำคัญทางสารสนเทศเป็นกิจการที่มีความสำคัญต่อความมั่นคงของรัฐ ความมั่นคงทางทหาร ความมั่นคงทางเศรษฐกิจ และความสงบเรียบร้อยภายในประเทศ...” และได้ยกตัวอย่างสิ่งที่เข้าข่ายว่าเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศว่าอาจมีได้หลายด้านดังต่อไปนี้ [356]

1. ด้านความมั่นคงของรัฐ
2. ด้านบริการภาครัฐที่สำคัญ
3. ด้านการเงินการธนาคาร
4. ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม
5. ด้านการขนส่งและโลจิสติกส์
6. ด้านพลังงานและสาธารณูปโภค
7. ด้านสาธารณสุข
8. ด้านอื่นตามที่คณะกรรมการประกาศกำหนดเพิ่มเติม

[356] มาตรา 49 พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

เพื่อให้การรักษาความปลอดภัยไซเบอร์ในโครงสร้างพื้นฐานสำคัญเป็นไปอย่างมีประสิทธิภาพ กฎหมายนี้จึงได้จัดตั้งให้มี 3 หน่วยงานเกิดขึ้น เพื่อทำหน้าที่แยกคนละส่วนกัน ได้แก่ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ คณะกรรมการการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ และสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

สำหรับผู้มีอำนาจหน้าที่ในการกำหนดนโยบายต่างๆ ที่มีผลมากที่สุดต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ให้แก่โครงสร้างพื้นฐานสำคัญตามกฎหมายนี้ได้แก่ “คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ”[357] ซึ่งมีอำนาจหน้าที่ที่เกี่ยวกับการรักษาโครงสร้างพื้นฐานสำคัญ ดังนี้

1. กำหนดนโยบายการบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ[358]

2. ส่งเสริมการรับรองมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ[359]

3. กำหนดมาตรการและแนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของพนักงานเจ้าหน้าที่ เจ้าหน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ[360]

4. มอบหมายการควบคุมและกำกับดูแล รวมถึงการออกข้อกำหนด วัตถุประสงค์ หน้าที่และอำนาจและกรอบการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ[361]

นอกจากคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ซึ่งมีบทบาทในการกำหนดนโยบายต่างๆ ที่มีผลต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ให้แก่โครงสร้างพื้นฐานสำคัญแล้ว กฎหมายนี้ยังจัดตั้ง “คณะกรรมการการกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์” เพิ่มขึ้นมาอีกด้วย [362] ซึ่งมีอำนาจหน้าที่แยกต่างหากจากคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ดังนี้

1. กำหนดประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อันเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานโครงสร้าง

---

[357] มาตรา 5 พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

[358] มาตรา 8 (2) พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

[359] มาตรา 8 (4) พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

[360] มาตรา 8 (5) พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

[361] มาตรา 8 (8) พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

[362] มาตรา 12 พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

พื้นฐานสำคัญทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ [363]

2. กำหนดหน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน้าที่ของหน่วยงานควบคุมหรือกำกับดูแล โดยอย่างน้อยต้องกำหนดหน้าที่ให้หน่วยงานควบคุมหรือกำกับดูแลต้องกำหนดมาตรฐานที่เหมาะสมเพื่อรับมือกับภัยคุกคามทางไซเบอร์ของแต่ละหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

สำหรับหน่วยงานสุดท้ายที่ถูกจัดตั้งตามกฎหมายฉบับนี้ ได้แก่ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ[364] ซึ่งมีหน้าที่ให้ความร่วมมือหรือช่วยเหลือในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยเฉพาะภัยคุกคามทางไซเบอร์ที่กระทบหรือเกิดแก่โครงสร้างพื้นฐานสำคัญ ทางสารสนเทศ[365]

เมื่อพิจารณาทั้ง 3 หน่วยงานนี้แล้ว จะพบว่า หน่วยงานที่มีบทบาทมากที่สุด ได้แก่ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ซึ่งมีอำนาจในการกำหนด จัดทำนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ให้แก่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนำไปปฏิบัติตาม[366] ในขณะที่หน่วยงานที่มีหน้าที่รับนโยบายนั้นไปปฏิบัติตาม และให้การสนับสนุน หรือความช่วยเหลือในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่กระทบหรือเกิดแก่โครงสร้างพื้นฐานสำคัญทางสารสนเทศ ได้แก่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ[367]

นอกจากนี้ กฎหมายดังกล่าวยังมอบหน้าที่ให้แก่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้วยว่าต้องจัดให้มีมาตรฐานขั้นต่ำเรื่องความมั่นคงปลอดภัยไซเบอร์ของตนเอง และหากหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้นไม่ปฏิบัติตาม หน่วยงานที่กำกับดูแลรายงานปัญหาดังกล่าวต่อคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และคณะกรรมการก็จะแจ้งให้แก่ผู้บริหารระดับสูงสุดของหน่วยงานเพื่อใช้อำนาจในทางบริหาร สั่งการไปยังหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้น เพื่อให้ดำเนินการแก้ไขจนได้มาตรฐานโดยเร็ว โดยไม่จำกัดว่าโครงสร้างพื้นฐานนั้นจะเป็นหน่วยงานของรัฐหรือของเอกชน[368] และยังมีหน้าที่ในการจัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ทั้งโดยผู้ตรวจสอบภายในหรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละหนึ่งครั้ง[369]

---

[363] มาตรา 13 (4) พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

[364] มาตรา 20 พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

[365] มาตรา 22 (8) พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

[366] มาตรา 43 พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

[367] มาตรา 43 พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

[368] มาตรา 53 พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

[369] มาตรา 54 พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

ในกรณีที่มีภัยคุกคามทางไซเบอร์เกิดขึ้นต่อโครงสร้างพื้นฐานสำคัญ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ก็มีหน้าที่จะต้องรายงานหน่วยงานที่ควบคุมหรือกำกับดูแลตนโดยเร็ว เพื่อให้หน่วยงานนั้นทำหน้าที่สนับสนุนและให้ความช่วยเหลือต่อไป[370] โดยหากหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศใดไม่ปฏิบัติตามโดยไม่มีเหตุอันควรจะมีโทษปรับไม่เกิน 200,000 บาท[371]

ภัยคุกคามทางไซเบอร์ซึ่งอาจเกิดขึ้นต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศสามารถแบ่งได้ 3 ระดับดังนี้[372]

1. ภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง หมายถึง ภัยคุกคามทางไซเบอร์ที่มีความเสี่ยง อย่างมีนัยสำคัญถึงระดับที่ทำให้ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศด้อยประสิทธิภาพลง

2. ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง หมายถึง ภัยคุกคามที่มีลักษณะการเพิ่มขึ้นอย่างมีนัยสำคัญของการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์ โดยมุ่งหมาย เพื่อโจมตีโครงสร้างพื้นฐานสำคัญของประเทศและการโจมตีดังกล่าวมีผลทำให้ โครงสร้างสำคัญทางสารสนเทศที่เกี่ยวข้องกับการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศ ความมั่นคงของรัฐ ความสัมพันธ์ระหว่างประเทศ การป้องกันประเทศ เศรษฐกิจ การสาธารณสุข ความปลอดภัยสาธารณะ หรือความสงบเรียบร้อยของประชาชนเสียหาย จนไม่สามารถทำงานหรือ ให้บริการได้

3. ภัยคุกคามทางไซเบอร์ในระดับวิกฤติ หมายถึง ภัยคุกคามทางไซเบอร์ในระดับวิกฤติที่มีลักษณะเป็นภัยคุกคามทางไซเบอร์ที่เกิดจากการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ในระดับที่สูงขึ้นกว่าภัยคุกคามทางไซเบอร์ในระดับร้ายแรง โดยส่งผลกระทบรุนแรงต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศในลักษณะที่เป็นวงกว้าง จนทำให้การทำงานของหน่วยงานรัฐหรือการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศที่ให้กับประชาชนล้มเหลวทั้งระบบ จนรัฐไม่สามารถควบคุมการทำงานส่วนกลางของระบบคอมพิวเตอร์ของรัฐได้ หรือการใช้มาตรการเยียวยาตามปกติในการแก้ไขปัญหาภัยคุกคามไม่สามารถแก้ไขปัญหาได้และมีความเสี่ยงที่จะลุกลามไปยังโครงสร้างพื้นฐานสำคัญอื่นๆ ของประเทศ ซึ่งอาจมีผลทำให้บุคคลจำนวนมากเสียชีวิตหรือระบบคอมพิวเตอร์ คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์จำนวนมากถูกทำลายเป็นวงกว้างในระดับประเทศ

หากปรากฏว่าภัยคุกคามทางไซเบอร์ที่เกิดขึ้นต่อระบบโครงสร้างพื้นฐานเป็นภัยคุกคามไซเบอร์ในระดับร้ายแรง หรือในระดับวิกฤติ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติจะมีอำนาจ

---

[370] มาตรา 57 และ 58 พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

[371] มาตรา 73 พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

[372] มาตรา 60 พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

หน้าที่เพิ่มขึ้นตามกฎหมายฉบับนี้ ทั้งนี้ อำนาจบางประการอาจต้องใช้คำสั่งศาลก่อนจึงจะสามารถใช้อำนาจตามกฎหมายนั้นได้

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เป็นหัวใจหลักของการการปกป้องระบบโครงสร้างพื้นฐานสำคัญของประเทศไทย ซึ่งบังคับให้หน่วยงานไม่ว่าจะภาครัฐหรือเอกชนที่มีภารกิจหรือกิจการเกี่ยวข้องกับระบบโครงสร้างพื้นฐานสำคัญของประเทศมีหน้าที่ต้องจัดให้มีมาตรฐานขั้นต่ำในการบริหารจัดการภยันตรายที่จะเกิดแก่ระบบโครงสร้างพื้นฐาน และจะให้มีการตรวจสอบรายปี ซึ่งหากไม่ปฏิบัติตามหน่วยงานที่มีหน้าที่กำกับดูแลก็สามารถทำการร้องเรียนแก่ผู้ที่มีอำนาจสูงสุดของหน่วยงานนั้น เพื่อสั่งให้แก้ไขโดยเร็วก็ได้ แต่ก็ไม่ได้มีโทษอาญาแต่อย่างใด หากไม่ปฏิบัติตามคำสั่งนั้น

กฎหมายนี้จะมีสภาพบังคับ 2 กรณี คือ ประการแรก เมื่อเกิดภัยคุกคามทางไซเบอร์ต่อโครงสร้างพื้นฐานสำคัญ และหน่วยงานโครงสร้างพื้นฐานสำคัญละเลยไม่รายงานหน่วยงานที่ควบคุมหรือกำกับดูแล โดยไม่มีเหตุอันควร จึงจะมีโทษปรับ ประการถัดมาคือ หากเกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรงขึ้น แต่หน่วยงานโครงสร้างพื้นฐานกลับไม่ได้ให้ความร่วมมือ หรือปรับปรุงแก้ไขมาตรฐานความปลอดภัย จึงจะมีโทษปรับและโทษจำคุก

หากเปรียบเทียบเรื่องการคุ้มครองระบบโครงสร้างพื้นฐานของประเทศไทยกับประเทศจีน สหรัฐอเมริกา สหภาพยุโรป จะพบว่ากฎหมายเกี่ยวกับการกำหนดให้มีมาตรฐานขั้นต่ำในการบริหารจัดการความเสี่ยงที่อาจเกิดต่อระบบโครงสร้างพื้นฐานของไทยมีลักษณะคล้ายกับแนวทางของสหรัฐอเมริกาและสหภาพยุโรป กล่าวคือไม่มีสภาพบังคับหรือโทษอาญาแต่อย่างใด หากหน่วยงานใดไม่ได้จัดให้มีขึ้น และมีหน่วยงานรัฐเป็นผู้ออกแนวทางหรือคู่มือให้เอกชนนำไปปรับใช้หรือปฏิบัติตาม อย่างไรก็ดี หากปรากฏว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้นต่อระบบโครงสร้างพื้นฐานสำคัญและไม่มีการแจ้งสถานการณ์ที่เกิดขึ้นต่อหน่วยงานรัฐ หรือในกรณีที่มีภัยคุกคามทางไซเบอร์เกิดขึ้นต่อระบบโครงสร้างพื้นฐานสำคัญในระดับร้ายแรง และผู้มีอำนาจตามกฎหมายนี้ได้สั่งให้แก้ไขมาตรฐานความปลอดภัย แต่หน่วยงานนั้นกลับละเลย กรณีทั้งสองนี้จึงจะมีโทษอาญาเช่นเดียวกับกฎหมายของจีน

4.3 การเก็บรวบรวมข้อมูลไว้ภายในท้องที่

1) กฎหมายจีน

“การเก็บรวบรวมข้อมูลไว้ภายในท้องที่” (data localization) คือ มาตรการที่ใช้บังคับแก่บริษัทในการเก็บข้อมูลของผู้ใช้ในเซิฟเวอร์ซึ่งอยู่ในเขตอำนาจของประเทศนั้น โดยต้องเก็บข้อมูลไว้แต่เพียงในประเทศนั้นเท่านั้น[373] ตัวอย่างเช่น ในประเทศเบลเยียม เดนมาร์ก ฟินแลน เยอรมัน รัสเซีย สวีเดน และสหราช

[373] Shah, Reema. 2015. "Law Enforcement and Data Privacy: A Forward-Looking Approach". Yale Law Journal 125 (2): 543, 548.

อาณาจักร ต่างก็มีกฎเกณฑ์ลักษณะนี้บังคับใช้กับการเก็บข้อมูลทางการเงิน[374] ในขณะที่บางประเทศ เช่น ออสเตรเลีย หรือ สหราชอาณาจักร บังคับไปถึงการเก็บข้อมูลสุขภาพประจำตัวบุคคลด้วย[375]

การเก็บรวบรวมข้อมูลไว้ภายในท้องที่เป็นอีกส่วนสำคัญในกฎหมายความปลอดภัยทางไซเบอร์ของจีน ซึ่งตั้งอยู่บนฐานของหลักการอธิปไตยไซเบอร์ อันนำไปสู่การบังคับให้ข้อมูลต่างๆ ที่ถูกเก็บไว้ในอาณาเขตของประเทศตนต้องได้รับความคุ้มครองที่รัดกุมขึ้น แนวคิดเรื่องการเก็บรวบรวมข้อมูลไว้ภายในท้องที่ก็ทำให้รัฐบาลสามารถอ้างสิทธิการควบคุมข้อมูลทั้งหลายได้ง่ายขึ้น เพื่อป้องกันการสอดแนวข้อมูลจากต่างชาติ และเป็นเครื่องมือที่สนับสนุนการเก็บข้อมูลต่างๆ ในประเทศ รวมไปถึงการเป็นผู้สอดแนมข้อมูลเหล่านั้นเสียเองด้วย การเก็บรวบรวมข้อมูลไว้ภายในท้องที่จึงไม่ได้ช่วยยกระดับความปลอดภัยของระบบมากนัก หากแต่ทำให้การสอดแนมจากรัฐเจ้าของข้อมูลและการบังคับใช้กฎหมายบนโลกออนไลน์เป็นไปได้อย่างสะดวกขึ้น

จากมาตรา 37 ผู้ให้บริการเครือข่ายที่เกี่ยวข้องกับระบบโครงสร้างพื้นฐานสำคัญด้านข้อมูลต้องเก็บข้อมูลส่วนบุคคลและข้อมูลสำคัญต่างๆ ไว้ในประเทศจีน การถ่ายโอนข้อมูลออกไปนอกประเทศนี้จะทำได้ก็ต่อเมื่อได้ทำตามขั้นตอนที่กฎหมายกำหนดไว้ รวมไปถึงการขออนุญาตจากเจ้าหน้าที่ด้วย หากไม่ปฏิบัติตามผู้ให้บริการอาจได้รับคำเตือน หรืออาจรวมไปถึงการปิดเว็บไซต์ การเพิกถอนใบอนุญาต และโทษปรับตั้งแต่ 50,000 หยวน ถึง 5,000,000 หยวน และบุคคลที่มีหน้าที่รับผิดชอบโดยตรงจะต้องถูกปรับส่วนตัวอีกเป็นเงิน 10,000 หยวน ถึง 100,000 หยวน[376] ได้มีบุคคลให้ความเห็นว่ามาตรการดังกล่าวเป็นนโยบายการเก็บรวบรวมข้อมูลไว้ภายในท้องที่ที่เข้มงวดที่สุดในโลก ในความเป็นจริงแล้ว มาตรการการเก็บรวบรวมข้อมูลไว้ภายในท้องที่ของจีนได้ถูกใช้มานานแล้วในบางธุรกิจ เช่น ธุรกิจธนาคาร และสุดท้ายจึงกลายเป็นใช้บังคับกับทุกธุรกิจในที่สุด[377]

บริษัทต่างชาติส่วนมากวิตกกังวลกับมาตรการนี้ของจีนเป็นอย่างมาก สิ่งแรกที่บริษัทเหล่านั้นกังวลคือต้นทุนที่สูงขึ้นจากการบริหารข้อมูลเหล่านั้น[378] เนื่องจากในทางปฏิบัติแล้ว บริษัทข้ามชาติหลายบริษัทมักทำการเก็บข้อมูลเหล่านั้นแยกเป็นส่วนๆ ไว้ในหลายๆ ประเทศเพื่อบรรเทาภาระในการบริหารจัดการกลุ่มข้อมูลขนาดใหญ่และภาระด้านภาษี บางบริษัทก็ย้ายเซิฟเวอร์ของตนออกจากประเทศจีนเพื่อป้องกันการสอดแนม

[374] Savelyev, Alexander. 2016. "Russia's New Personal Data Localization Regulations: A Step Forward or A Self-Imposed Sanction?". Computer Law & Security Review 32 (1): 128, 140.

[375] Chander, Anupam, and Uyên P. Lê. 2015. "Data Nationalism". Emory Law Journal 64: 677, 680.

[376] 《中华人民共和国网络安全法》第 66 条

[377] Sacks, Samm. 2017. "China's Cybersecurity Law Takes Effect: What to Expect". Lawfare. https://www.lawfareblog.com/chinas-cybersecurity-law-takes-effect-what-expect.

[378] Horwitz, Josh. 2017. "A Key Question at The Heart of China's Cybersecurity Law: Where Should Data Live?". Quartz. https://qz.com/999613/a-key-question-at-the-heart-of-chinas-cybersecurity-law-where-should-data-live/.

และการเซ็นเซอร์[379] เมื่อกฎหมายฉบับนี้บังคับใช้ บริษัททุกบริษัทกลับต้องสร้างศูนย์รวมข้อมูลในประเทศจีน หรือใช้บริการศูนย์เก็บข้อมูลในท้องถิ่น หรือไม่ก็ต้องทำการปรับเปลี่ยนโครงสร้างการเก็บข้อมูล การเก็บรวบรวมข้อมูลไว้ภายในท้องที่ซึ่งอยู่ในกฎหมายความมั่นคงปลอดภัยไซเบอร์อาจถือได้ว่าเป็นการกีดกันทางการค้าสำหรับผู้ประกอบการ และปัจจุบัน มาตรการนี้ได้กลายเป็นคดีพิพาทซึ่งอยู่ในองค์กรการค้าโลก ซึ่งมีคู่พิพาทคือสหรัฐอเมริกา[380]

ในขณะเดียวกัน บริษัทอินเทอร์เน็ตในประเทศก็มีความกังวลเกี่ยวกับมาตรการนี้ด้วยเช่นกัน โดยมองว่าอาจเป็นอุปสรรคในการผลักดันธุรกิจของตนให้ไปสู่ระดับสากลได้ มาตรการนี้ยังอาจนำไปสู่ “การแบ่งแยกบนโลกอินเทอร์เน็ต” ด้วยการเปลี่ยนแปลงสาระสำคัญของโลกอินเทอร์เน็ตที่มีความไร้พรมแดนและมีความเสรีในการโอนถ่ายข้อมูล

อีกหนึ่งข้อกังวลที่เกิดขึ้นคือความเสี่ยงที่ไม่สามารถควบคุมได้จากการรั่วไหลของข้อมูล บริษัทข้ามชาติบางบริษัทกังวลว่ามาตรการนี้จะเปิดช่องให้รัฐบาลจีนเข้าถึงข้อมูลทรัพย์สินและความลับทางการค้า นอกจากนี้บริษัทอาจตกเป็นเป้าหมายของการถูกเซ็นเซอร์หรือสอดแนมจากรัฐบาลได้อีกด้วย ซึ่งจะทำลายความปลอดภัยของผู้ใช้บริการไปในตัว ทั้งนี้ กลุ่มข้อมูลที่มารวมตัวกันเป็นกลุ่มเดียวมีแนวโน้มว่าจะถูกแฮคได้สูงกว่า ด้วยเหตุนี้ มาตรการการเก็บข้อมูลไว้ในท้องที่อาจทำลายมากกว่าส่งเสริมความปลอดภัยไซเบอร์

แม้ว่าในมาตรา 37 จะให้คำนิยามของคำว่า “ข้อมูลส่วนบุคคล” ไว้ แต่คำว่า “ข้อมูลสำคัญ” กลับไม่ได้ให้นิยามในกฎหมาย โดยคณะกรรมการไซเบอร์เสปซจีนได้นิยามไว้ว่า “ข้อมูลสำคัญ” หมายถึง “ข้อมูลซึ่งเกี่ยวข้องใกล้ชิดกับความมั่นคงของชาติ การพัฒนาทางเศรษฐกิจ และประโยชน์สาธารณะ”[381] จึงเปิดช่องให้รัฐบาลสามารถตีความ “ความมั่นคงของชาติ การพัฒนาทางเศรษฐกิจ และประโยชน์สาธารณะ” ตามดุลยพินิจของรัฐบาลเองอย่างกว้างขวาง และสร้างต้นทุนมหาศาลให้กับบริษัทต่างๆ ในการปฏิบัติตามมาตรการดังกล่าว

2) เปรียบเทียบกฎหมายของประเทศสหรัฐอเมริกาและสหภาพยุโรป

กฎหมายสหรัฐอเมริกา

เดิมที สหรัฐอเมริกาไม่เคยมีกฎหมายใดบังคับเกี่ยวกับการเก็บรวบรวมข้อมูลไว้ภายในท้องที่มาก่อน จนกระทั่งในปี ค.ศ. 2019 สมาชิกวุฒิสภาจอร์ช ฮอว์ลีย์ (Josh Hawley) ได้เสนอร่างกฎหมายฉบับหนึ่งขึ้นคือ รัฐบัญญัติความมั่นคงของชาติและการคุ้มครองข้อมูลส่วนบุคคล (National Security and Personal Data

[379] Sargsyan, Tatevik. 2016. "Data Localization and The Role of Infrastructure for Surveillance, Privacy, And Security". International Journal of Communication 10: 2221, 2225-2226.

[380] Miles, Tom. 2017. "U.S. Asks China Not to Enforce Cyber Security Law". REUTERS. http://www.reuters.com/article/us-usa-china-cyber-trade/u-s-asks-china-not-to-enforce-cyber-security-law-idUSKCNC11D1.

[381] 《关键信息基础设施安全保护条例（征求意见稿）》（**保护条例**）第 17 条

Protection Act) ขึ้น[382] การเสนอร่างกฎหมายดังกล่าวคาดว่ามีวัตถุประสงค์เพื่อป้องกันเหตุการณ์ที่ผู้พัฒนาแอพพลิเคชั่นของประเทศจีนที่ทำการเก็บข้อมูลประชาชนในประเทศสหรัฐอเมริกากลับไปที่ประเทศจีนได้อย่างง่ายดายเกินไป อันเป็นผลให้ประเทศจีนมีความได้เปรียบในเชิงเศรษฐกิจมากเกินสมควร[383] โดยกฎหมายฉบับนี้จะบังคับให้บริษัทต่าง ๆ ในสหรัฐอเมริกาต้องไม่ถ่ายโอนข้อมูลของพลเมืองอเมริกาที่เก็บได้ในประเทศไปเก็บไว้ที่ประเทศอื่นที่มีความน่ากังวล อันอาจกล่าวได้ว่า “เสรีในการไหลเวียนของข้อมูลข่าวสารเป็นหลัก แต่การเก็บรวบรวมข้อมูลไว้ภายในท้องที่คือข้อยกเว้น”

รัฐบัญญัติความมั่นคงของชาติและการคุ้มครองข้อมูลส่วนบุคคลมีความน่าสนใจคือมาตรการเก็บรวบรวมข้อมูลไว้ภายในท้องที่นี้ไม่ได้บังคับครอบคลุมทุกบริษัท หากแต่ต้องพิจารณาว่าการโอนข้อมูลไปเก็บไว้ที่ประเทศที่หมายนั้นจัดเป็น “ประเทศที่มีความน่ากังวล” (Countries of Concern) หรือไม่ โดยประเทศเหล่านั้นได้แก่ ประเทศจีน ประเทศรัสเซีย และประเทศอื่นตามที่รัฐมนตรีว่าการกระทรวงการต่างประเทศเห็นสมควร[384] ซึ่งหากปรากฏว่าการโอนข้อมูลนั้นจะโอนไปเก็บไว้ในประเทศที่มีความน่ากังวล กฎหมายฉบับนี้จะห้ามไม่ให้บริษัทนั้นทำการโอนไป

อย่างไรก็ดี ความในข้างต้นนั้นอาจไม่ใช้บังคับกับบริษัทเทคโนโลยีอันอยู่ในข่าย (Covered technology company) อันหมายถึงบริษัทที่มีการให้บริการออนไลน์เป็นหลัก[385] อาทิ Facebook Twitter หรือ Instagram เนื่องจากว่าธุรกิจประเภทนี้เป็นธุรกิจที่ผู้ใช้มักนำข้อมูลของตนเข้าไปอย่างเป็นกิจวัตรอยู่แล้ว ทำให้ข้อมูลที่บริษัทนี้รวบรวมได้ มีปริมาณมหาศาลและมีความส่วนตัวสูง ต่างกับบริษัทอื่นที่เก็บข้อมูลได้อย่างจำกัด ดังนั้นผู้ประกอบกิจการนี้จึงต้องปฏิบัติตามมาตรการที่เคร่งครัดขึ้นกว่าบริษัททั่วไป โดยการห้ามโอนข้อมูลที่เก็บได้มานั้นไปเก็บไว้ที่ประเทศใด ๆ โดยไม่พิจารณาว่าประเทศนั้นจัดเป็นประเทศที่มีความน่ากังวลหรือไม่ก็ตาม เว้นเสียแต่ว่าประเทศนั้นจะมีข้อตกลงร่วมกันกับสหรัฐอเมริกาโดยเฉพาะเจาะจง[386] ทั้งนี้ การฝ่าฝืนกฎหมายฉบับนี้มีโทษจำคุกสูงสุด 5 ปี[387]

อนึ่ง มีข้อสังเกตคือทั้งประเทศจีนและรัสเซียต่างได้ขึ้นชื่อว่าเป็นประเทศคู่แข่งกับสหรัฐอเมริกามาอย่างช้านาน การที่กฎหมายฉบับนี้ได้ถูกเสนอขึ้นโดยมีจุดมุ่งหมายเป็นการเฉพาะต่อประเทศทั้งสองนี้โดยชัดแจ้ง อาจพิจารณาได้ว่า มูลเหตุของการคุ้มครองข้อมูลส่วนบุคคลเกิดขึ้นเพื่อปิดจุดอ่อนทางเศรษฐกิจ มากกว่าจะเป็นไปเพื่อประโยชน์ของปัจเจกชนโดยแท้จริง แต่หากพิจารณาอีกด้านหนึ่ง การที่จะบังคับให้ทุกบริษัทต้อง

---

[382] Fisher, Christine. 2019. "Senate Bill Would Block US Companies From Storing Data In China". Engadget.Com. https://www.engadget.com/2019-11-18-national-security-personal-data-protection-act.html.

[383] Davies, Jamie. 2019. "US Government To Consider Strict Data Localisation Laws". Telecoms. https://telecoms.com/500992/us-government-to-consider-strict-data-localisation-laws/.

[384] มาตรา 2(2)(A) National Security and Personal Data Protection Act

[385] มาตรา 2(3) National Security and Personal Data Protection Act

[386] มาตรา 3(a)(5) National Security and Personal Data Protection Act

[387] มาตรา 5(b) National Security and Personal Data Protection Act

ทำการการเก็บรวบรวมข้อมูลไว้ภายในท้องที่โดยไม่คำนึงว่าจะโอนไปเก็บไว้ในประเทศใดนั้น อาจเป็นการก่ออุปสรรคต่อการไหลเวียนของข้อมูลข่าวสาร และขัดขวางการดำเนินนโยบายเศรษฐกิจแบบเสรีนิยมอันว่าด้วยการรับรู้ข้อมูลของตลาดของผู้ประกอบการก็เป็นได้ ด้วยเหตุนี้ ผู้ร่างกฎหมายจึงเสนอชื่อประเทศเพียง 2 ประเทศที่ต้องเฝ้าระวัง และให้การโอนข้อมูลไปยังประเทศอื่นทำได้โดยปกติ

อย่างไรก็ดี แม้เจตนาของผู้ร่างกฎหมายจะประสงค์ให้ข้อมูลพลเมืองไม่ตกไปอยู่ในมือของชาติคู่แข่งก็ตาม แต่ในทางปฏิบัติก็ยังมีแนวโน้มที่จะหลบหลีกกฎหมายดังกล่าวได้อยู่ ยกตัวอย่างเช่น การตั้งบริษัทลูกในประเทศอื่นนอกจากในประเทศจีนและในรัสเซีย จากนั้นก็ให้บริษัทนั้นเข้าไปประกอบกิจการในสหรัฐอเมริกาและเก็บรวบรวมข้อมูลแทนบริษัทแม่ หลังจากนั้นจึงให้บริษัทลูกนั้นส่งข้อมูลให้กับบริษัทแม่ที่อยู่ในจีนหรือรัสเซียอีกทีหนึ่ง อย่างไรก็ดี ปัจจุบัน กฎหมายฉบับนี้ยังอยู่ในระหว่างการพิจารณาของสมาชิกวุฒิสภา จึงมีแนวโน้มว่ากฎหมายอาจมีการเปลี่ยนแปลงให้เหมาะสมได้ในอนาคต

กฎหมายสหภาพยุโรป

เดิมที สหภาพยุโรปมองว่าการบังคับให้ผู้ประกอบการทำการเก็บรวบรวมข้อมูลไว้ในท้องที่คือการกีดกันทางการค้าอย่างหนึ่ง เนื่องจากว่าเป็นการเพิ่มต้นทุนให้แก่ผู้ประกอบการและขัดขวางเสรีภาพในการโอนย้ายข้อมูลข่าวสารระหว่างประเทศสมาชิกด้วยกันเอง อันจะก่อให้เกิดผลกระทบต่อตลาดโดยตรง นอกจากนี้ มาตรการนี้ยังท้าทายปรัชญาพื้นฐานว่าด้วยการรวมตัวกันของประเทศสมาชิกในสหภาพยุโรป เนื่องจากเป็นการสร้างกำแพงข้อมูลข่าวสารระหว่างประเทศขึ้น อย่างไรก็ดี ในยุคแห่งการแข่งขันด้วยข้อมูล หากไม่มีมาตรการการเก็บรวบรวมข้อมูลไว้ภายในท้องที่เกิดขึ้น ข้อมูลของประชาชนในประเทศสมาชิกก็อาจไม่ได้รับความปลอดภัยและถูกนำไปใช้โดยเจ้าของข้อมูลไม่ยินยอมได้ ดังนี้ การออกกฎหมายว่าด้วยการเก็บรวบรวมข้อมูลไว้ภายในท้องที่จึงถูกนำมาพิจารณาอีกครั้ง โดยคงหลักการเดิมว่าประเทศสมาชิกสหภาพยุโรปด้วยกันยังคงสามารถเคลื่อนย้ายข้อมูลไปมาหากันได้อย่างเสรี ในขณะเดียวกัน การเคลื่อนย้ายข้อมูลไปยังประเทศอื่นที่ไม่ใช่ประเทศสมาชิกก็จะมีข้อจำกัดบางประการ เพื่อรับรองสิทธิส่วนตัวของคนในประเทศสมาชิก

กฎหมายสำคัญที่เกี่ยวข้องกับการเก็บรวบรวมข้อมูลไว้ภายในท้องที่ได้แก่ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC หรือ General Data Protection Regulation โดยเป้าหมายของกฎหมายนี้คือการคุ้มครองข้อมูลส่วนบุคคล ซึ่งหมายถึง “ข้อมูลใด ๆ ก็ตามที่สามารถทำให้ทราบถึงบุคคลใดได้โดยเฉพาะเจาะจง ไม่ว่าจะโดยตรงหรือโดยอ้อม เช่น ชื่อ หมายเลขบัตรประจำตัวประชาชน ข้อมูลสถานที่ ตัวตนบนโลกออนไลน์ ตลอดจนรูปลักษณ์ทางกายภาพ อุปนิสัย ภาวะทางจิต อารมณ์ สถานะทางเศรษฐกิจ วัฒนธรรม หรือสภาพทางสังคมของบุคคลนั้น”[388]

[388] มาตรา 4 (1) General Data Protection Regulation

กฎหมายฉบับนี้ ไม่ได้ห้ามการโอนย้ายข้อมูลระหว่างประเทศสมาชิกด้วยกัน ทว่าหากการโอนย้ายข้อมูลนั้นจะโอนไปยังประเทศอื่นที่ไม่ใช่ประเทศสมาชิก ผู้ครอบครองข้อมูลจะทำการโอนข้อมูลนั้นไปได้ก็ต่อเมื่อประเทศที่หมายที่ข้อมูลนั้นโอนไปได้มีมาตรการและการบังคับใช้กฎหมายที่เหมาะสมเพื่อบริหารจัดการข้อมูลนั้น ๆ เมื่อมีความรับผิดเกิดขึ้น[389]

3) เปรียบเทียบกฎหมายของประเทศไทย

กฎหมายที่กล่าวถึง การเก็บรวบรวมข้อมูลไว้ภายในท้องที่ถูกบัญญัติไว้ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยข้อมูลที่จะถูกคุ้มครองตามกฎหมายฉบับนี้ได้แก่ ข้อมูลส่วนบุคคล ซึ่งกฎหมายฉบับนี้ได้ให้นิยามว่าเป็น “ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ”[390]

การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศได้ถูกกำหนดไว้ว่าจะทำได้ก็ต่อเมื่อประเทศปลายทางที่ข้อมูลโอนไปนั้นมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ อย่างไรก็ดี หลักนี้อาจถูกยกเว้นได้หากปรากฏเหตุตามกฎหมายดังต่อไปนี้คือ[391]

1. เป็นการปฏิบัติตามกฎหมาย

2. ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลโดยได้แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอของประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลแล้ว

3. เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น

4. เป็นการกระทำตามสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับบุคคลหรือนิติบุคคลอื่น เพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

5. เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของเจ้าของข้อมูลส่วนบุคคล หรือบุคคลอื่น เมื่อเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมในขณะนั้นได้

6. เป็นการจำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะที่สำคัญ

ทั้งนี้ หากผู้ควบคุมข้อมูลใดไม่ปฏิบัติตาม ก็จะได้รับปรับ หรือจำคุก แล้วแต่กรณี[392]

---

[389] มาตรา 46 General Data Protection Regulation

[390] มาตรา 6 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[391] มาตรา 28 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[392] โปรดดูมาตรา 79 83 และ 84 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศได้ถูกกำหนดไว้ว่าจะทำได้ก็ต่อเมื่อประเทศปลายทางที่ข้อมูลโอนไปนั้นมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ หลักการนี้ก็เป็นหลักการเดียวกันกับกฎหมายของสหภาพยุโรป ทว่า กฎหมายไทยมีความพิเศษอยู่คือ การโอนข้อมูลส่วนบุคคลไปยังประเทศที่ไม่มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอก็อาจทำได้เช่นกัน หากเข้าเหตุยกเว้นตามที่กฎหมายกำหนดไว้[393] ซึ่งไม่ปรากฏว่ากฎหมายของสหรัฐอเมริกา สหภาพยุโรป หรือประเทศจีนจะมีเหตุยกเว้นเหล่านี้แต่อย่างใด

4.4 การรับรองมาตรฐานความปลอดภัย และการตรวจสอบ

1) กฎหมายจีน

ความปลอดภัยทางไซเบอร์จะเกิดขึ้นได้ก็เมื่อผู้ให้บริการเครือข่ายที่เกี่ยวข้องกับระบบโครงสร้างพื้นฐานสำคัญและผู้ให้บริการทั่วไปเลือกใช้ผลิตภัณฑ์หรือบริการที่มีมาตรฐานทางความปลอดภัยที่สูง ด้วยเหตุนี้ การกำหนดมาตรฐานจึงกลายเป็นอีกส่วนสำคัญของกฎหมายความปลอดภัยทางไซเบอร์ ตั้งแต่ค.ศ. 2007 ประเทศจีนได้ทำการออกแผนระดับความปลอดภัยหลายระดับ อย่างไรก็ดี แผนนี้ได้รับการวิพากจารณ์ว่า

---

[393] เหตุเหล่านั้นได้แก่

1. เป็นการปฏิบัติตามกฎหมาย

2. ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลโดยได้แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอของประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลแล้ว

3. เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือ เพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น

4. เป็นการกระทำตามสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับบุคคลหรือนิติบุคคลอื่น เพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

5. เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของเจ้าของข้อมูลส่วนบุคคล หรือบุคคลอื่น เมื่อเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมในขณะนั้นได้

6. เป็นการจำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะที่สำคัญ

ขัดแย้งกันกับมาตรฐานสากลว่าด้วยความปลอดภัยทางไซเบอร์และเป็นมาตรการที่เข้มงวดเกินไปอันอาจทำให้บริษัทในประเทศไม่สามารถแข่งขันกับบริษัทอื่นในตลาดโลกได้[394]

กฎหมายความปลอดภัยทางไซเบอร์กล่าวถึงการรับรองความปลอดภัยที่ซับซ้อนและวิธีการตรวจสอบ โดยในมาตรา 23 กำหนดให้อุปกรณ์ที่ใช้เพื่อบริการระบบโครงสร้างพื้นฐานสำคัญและผลิตภัณฑ์ที่ใช้เพื่อรักษาความปลอดภัยของโครงข่ายบางประเภทต้องเป็นไปตามมาตรฐานของชาติและข้อบังคับที่กำหนดไว้ และผ่านการรับรองมาตรฐานจากสถาบันที่กำหนดไว้หรือผ่านการตรวจสอบอย่างละเอียด นอกจากนี้ มาตรานี้ยังกำหนดให้หน่วยงานที่เกี่ยวข้องกับคณะรัฐมนตรีจัดแบ่งประเภทของอุปกรณ์เหล่านั้น และวางกฎเกณฑ์การรับรองหรือตรวจสอบมาตรฐานไม่ให้ซ้ำซ้อนกัน

ภายใต้มาตรา 35 ผลิตภัณฑ์และบริการที่เกี่ยวเนื่องกับโครงข่ายซึ่งถูกซื้อโดยผู้ให้บริการเครือข่ายที่เกี่ยวข้องกับระบบโครงสร้างพื้นฐานสำคัญด้านข้อมูลข่าวสาร ซึ่งอาจมีผลกระทบต่อความมั่นคงของชาติ ต้องนำผลิตภัณฑ์หรือบริการนั้นเข้าสู่กระบวนการพิจารณาโดยรัฐบาลเสียก่อน โดยทั้งมาตรา 23 และ 35 ต่างเป็นการสิ้นเปลืองเวลาและเป็นภาระทั้งสิ้น เพื่อบังคับใช้มาตรา 35 คณะกรรมการไซเบอร์เสปซของจีนได้ประกาศมาตรการว่าด้วยการพิจารณาความปลอดภัยสำหรับผลิตภัณฑ์และบริการที่เกี่ยวเนื่องกับโครงข่าย เมื่อวันที่ 2 พฤษภาคม ค.ศ. 2017 จากมาตรการนี้ คณะกรรมการไซเบอร์เสปซจะตั้งคณะกรรมการขึ้นมาเพื่อทำการพิจารณา[395] โดยมุ่งเน้นไปที่ว่าผลิตภัณฑ์นั้นปลอดภัยและสามารถควบคุมจัดการได้หรือไม่[396] โดยการพิจารณามีหลายขั้นตอนได้แก่ การตรวจสอบความปลอดภัย การตรวจสอบด้วยผลวิจัยทางแล็บ การตรวจสอบสถานที่ การตรวจสอบออนไลน์ และการตรวจสอบประวัติย้อนหลัง[397]

ถึงแม้ว่าในกฎหมายฉบับนี้ไม่ได้บังคับให้ผู้ผลิตเหล่านั้นต้องแสดงโค๊ดที่ใช้ในการเขียนให้กับกรรมการพิจารณา แต่กรรมการอาจร้องขอให้ผู้ผลิตแสดงสิ่งของรายการเช่นว่านั้นหรือขอให้ติดตั้งช่องทางพิเศษเพื่อให้รัฐบาลเข้าถึงลงไปในผลิตภัณฑ์หรือบริการ ซึ่งมาตรการนี้ได้นำมาใช้ในภาคธนาคารแล้วตั้งแต่ค.ศ. 2014 นอกจากนี้ มาตรการดังกล่าวยังมิได้บอกไว้อย่างชัดเจนว่าวิธีการอุทธรณ์คำสั่งคณะกรรมการเป็นเช่นไร ข้อมูลใดบ้างจะถูกร้องขอโดยคณะกรรมการ และในกรณีที่สินค้านั้นไม่ผ่านการพิจารณา ผู้ผลิตจะขอคืนได้อย่างไร และจากประโยคที่ว่า “...อาจมีผลกระทบต่อความมั่นคงของชาติ” ก็เปิดช่องให้รัฐบาลสามารถตีความได้อย่างกว้างขวางและใช้ในวัตถุประสงค์ทางการเมืองได้

---

[394] Blinderman, Eric, and Myra Din. 2017. "Hidden by Sovereign Shadows: Improving the Domestic Framework for Deterring State-Sponsored Cybercrime". Vanderbilt Journal of Transnational Law 50: 889, 896-897.

[395] 《关键信息基础设施安全保护条例（征求意见稿）》（**保护条例**） 第 5 条

[396] 《关键信息基础设施安全保护条例（征求意见稿）》（**保护条例)** 第 4 条

[397] 《关键信息基础设施安全保护条例（征求意见稿）》（**保护条例)** 第 3 条

มาตรการเหล่านี้มีวัตถุประสงค์สำคัญอย่างหนึ่งเพื่อป้องกันไม่ให้สินค้าหรือบริการเหล่านั้นถูกควบคุมโดยต่างชาติ[398] ประเทศจีนเชื่อว่าโครงข่ายดิจิทัลในประเทศจะเป็นเป้าหมายของการถูกโจมตี หากส่วนประกอบผลิตภัณฑ์ที่ระบบโครงสร้างพื้นฐานสำคัญใช้ผลิตโดยต่างชาติ ทั้งนี้ มาตรการตรวจสอบยังคงถูกวิจารณ์ในประเด็นความไม่ชัดเจนของกระบวนการและหลักเกณฑ์ที่ใช้ในการพิจารณา อันอาจนำไปสู่การสอดแนมของรัฐจีนอีกวิธีหนึ่งก็เป็นได้ ซึ่งย่อมส่งผลให้เกิดการรั่วไหลของข้อมูลต่างๆ รวมไปถึงความลับทางการค้าได้ สำนักงานผู้แทนการค้าสหรัฐ (the Office of United States Trade Representative : USTR) ก็ได้แสดงความกังวลเรื่องนี้ไว้อย่างชัดเจนในรายงานพิเศษมาตรา 301 ค.ศ. 2017 ว่าหลายบริษัทอาจถูกบังคับให้ต้องเปิดเผยเรื่องทรัพย์สินทางปัญญา เพื่อให้สอดคล้องกับมาตรการพิจารณานี้

นอกจากนี้แล้ว การรับรองมาตรฐานความปลอดภัยและการตรวจสอบในมาตรา 23 และ 35 ยังเป็นการแทรกแซงตลาด โดยใช้อำนาจทางการเมืองในการปิดกั้นหรือประวิงเวลาไม่ให้ผู้ผลิตสามารถนำสินค้าหรือบริการเหล่านั้นไปขายให้กับผู้ให้บริการเครือข่ายที่เกี่ยวข้องกับระบบโครงสร้างพื้นฐานสำคัญได้ ในขณะเดียวกันก็ส่งผลกระทบต่อการตัดสินใจของผู้ประกอบการในการเลือกซื้อสินค้าหรือบริการที่เกี่ยวข้อง[399] มาตรการดังกล่าวอาจมีขึ้นเพื่อลดการพึ่งพาเทคโนโลยีความปลอดภัยจากต่างชาติและสนับสนุนการลงทุนสินค้าและบริการดังกล่าวในประเทศจีนแทน

2) เปรียบเทียบกฎหมายของประเทศสหรัฐอเมริกาและสหภาพยุโรป

กฎหมายสหรัฐอเมริกา

โดยทั่วไป สหรัฐอเมริกาไม่มีกฎหมายใดบังคับให้ผู้ที่เกี่ยวข้องกับระบบโครงสร้างพื้นฐานสำคัญต้องใช้อุปกรณ์ที่รัฐรับรองว่าได้มาตรฐาน หากแต่เป็นเสรีภาพของผู้ประกอบการว่าจะเลือกใช้อุปกรณ์ใด อย่างไรก็ดี หากผู้ประกอบการต้องการป้องกันกิจการของตนจากการจู่โจมทางไซเบอร์ ผู้ประกอบการสามารถศึกษาได้จากคู่มือหรือแผนการจัดการเฉพาะของหน่วยงานภาครัฐดังนี้

1. กรอบทำงานด้านความมั่นคงปลอดภัยไซเบอร์ของสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (The NIST Cybersecurity Framework) จัดทำโดยสถาบันมาตรฐานและเทคโนโลยีแห่งชาติสหรัฐอเมริกา ซึ่งมีหน่วยงานในสังกัดกระทรวงพาณิชย์ [400]

---

[398] Hoffmann, Richard. 2017. "Update: China Releases New Draft Regulations regarding Cyber Security of Online Services and Products". Ecovis BEIJING. http://www.ecovis-beijing.com/enfblog-en/articles/810-update-china.

[399] Reuters. 2017. "China's Tough Cybersecurity Law to Come into Force This Week". South China Morning Post. http://www.scmp.com/news/china/policies-politics/article/2096094/chinas-tough-cybersecurity-law-come-force-week.

[400] National Institute of Standards and Technolog. 2020. "About NIST". NIST. https://www.nist.gov/about-nist.

2. แผนการจัดการเฉพาะ (Sector-Specific Plan) จัดทำโดยหน่วยงานความมั่นคงปลอดภัยของโครงสร้างพื้นฐาน หน่วยงานในสังกัดกระทรวงความมั่นคงแห่งมาตุภูมิ

อย่างไรก็ดี เมื่อต้นปี ค.ศ. 2020 การรับรองมาตรฐานความปลอดภัยและการตรวจสอบภาคบังคับได้ถูกริเริ่มขึ้นโดยกระทรวงกลาโหมสหรัฐอเมริกา หากผู้ประกอบการรายใดประสงค์จะเข้าร่วมการจัดซื้อจัดจ้างหรือรับช่วงต่อสัญญากับกระทรวงกลาโหม ผู้ประกอบการผู้นั้นต้องยินยอมให้หน่วยงานทำการตรวจสอบว่าบริษัทของผู้ประกอบการมีมาตรการรับรองความเสี่ยงภัยไซเบอร์ที่เป็นไปตามที่กำหนดก่อน[401] โดยสถานะการรับรองนั้นคือ Cybersecurity Maturity Model Certification (CMMC) ซึ่งผู้ประกอบการจะต้องมีการจัดวางโครงสร้างในองค์กรที่ดี และมีการใช้อุปกรณ์ซึ่งมีคุณสมบัติตามที่กำหนดไว้ด้วยจึงจะได้รับสถานะรับรอง[402]

กฎหมายสหภาพยุโรป

การรับรองมาตรฐานความปลอดภัยและการตรวจสอบเป็นหนึ่งในองค์ประกอบสำคัญในการส่งเสริมนโยบายตลาดเดียวสหภาพยุโรป (European Single Market) และเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ให้แก่ประเทศสมาชิกไปพร้อม ๆ กัน โดยอุปกรณ์ที่ได้รับการรับรองก็จะสามารถนำไปขายในประเทศสมาชิกอื่นได้โดยง่าย และในขณะเดียวกัน ความมั่นคงปลอดภัยไซเบอร์ก็จะไม่ถูกคุกคามจากอุปกรณ์ที่ไม่มีคุณภาพหรือไม่ปลอดภัย[403]

ในปี ค.ศ. 2019 สหภาพยุโรปได้ออกกฎหมายหนึ่งขึ้น คือ REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) เพื่อเพิ่มบทบาทหน้าที่ให้กับองค์กรเพื่อความมั่นคงปลอดภัยไซเบอร์ (European Union Agency for Cybersecurity) ให้การเป็นตัวกลางระหว่างประเทศสมาชิกในการแบ่งปันข้อมูลข่าวสาร และกรณีนี้ก็ได้รวมไปถึงการแบ่งปันข้อมูลของผลิตภัณฑ์ด้วยว่าอุปกรณ์ใดได้ผ่านการทดสอบแล้ว เพื่อให้ประเทศสมาชิกอื่นรับทราบ และทำให้การนำ

---

[401] "Cybersecurity Maturity Model Certification (CMMC) Will Replace NIST 800-171 On Dod Rfis And Rfps In 2020". 2020. Steelcloud. https://www.steelcloud.com/cybersecurity-maturity-model-certification-cmmc.

[402] Tanenbaum, Mitch. 2020. "Why and How The Dod Is Implementing The CMMC". Cmmc-Certification.Com. https://cmmc-certification.com.

[403] European Commission. 2020. "The EU Cybersecurity Certification Framework - Shaping Europe'S Digital Future - European Commission". European Commission. https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework.

อุปกรณ์นั้นไปจำหน่ายต่อในประเทศสมาชิกอื่นทำได้สะดวกขึ้น[404] แต่ทั้งนี้ก็ไม่ได้มีโทษแก่ผู้ที่หลีกเลี่ยงไม่นำสินค้าดังกล่าวไปตรวจสอบคุณภาพแต่อย่างใด

3) เปรียบเทียบกฎหมายของประเทศไทย

ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ได้กำหนดให้“หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ” ซึ่งหมายถึงหน่วยงานของรัฐหรือหน่วยงานเอกชนใดที่ได้ให้บริการโครงสร้างพื้นฐานสำคัญมีหน้าที่ในการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยประมวลแนวทางดังกล่าวนั้นต้องประกอบด้วยแผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยผู้ตรวจประเมิน ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปีละหนึ่งครั้ง[405] ทว่า ถึงแม้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะเป็นผู้จัดทำประมวลแนวทางปฏิบัติเพื่อใช้ตรวจสอบตนเองนั้นเอง แต่เนื้อหาดังกล่าวก็ต้องสอดคล้องกับข้อกำหนดขั้นต่ำที่คณะกรรมการการกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ได้กำหนดไว้ด้วย[406] ซึ่งในปัจจุบัน ยังไม่มีมาตรฐานขั้นต่ำกำหนดไว้

นอกจากนี้ หากปรากฏว่าประมวลแนวทางของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศไม่ได้มาตรฐาน คณะกรรมการการกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ก็จะมีอำนาจในการสั่งให้ผู้มีอำนาจหรือผู้บริหารจัดการแก้ไขให้เป็นมาตรฐานโดยเร็ว[407] ทว่า ไม่ปรากฏว่าหากไม่ปฏิบัติตามแล้วจะมีโทษอาญาแต่อย่างใดหากไม่ปฏิบัติตาม เว้นแต่จะปรากฏในภายหลังว่าเกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรงแล้วหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศก็ไม่ได้ให้ความร่วมมือ หรือปรับปรุงแก้ไขให้ถูกต้อง จึงจะมีโทษปรับและโทษจำคุก[408]

อนึ่ง สำหรับเรื่องการรับรองว่าการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศใดได้มาตรฐานหรือไม่นั้น กฎหมายก็ให้อำนาจหน้าที่แก่คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติในการเป็นผู้รับรอง[409]

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ได้กำหนดให้หน่วยงานที่มีกิจการหรือภารกิจเกี่ยวกับระบบโครงสร้างพื้นฐานสำคัญเท่านั้นที่ต้องจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และจัดทำประเมินปีละหนึ่งครั้ง โดยคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเป็นผู้มีอำนาจหน้าที่ในการรับรองมาตรฐาน อย่างไรก็ดี มีข้อสังเกต

---

[404] เรื่องเดียวกัน

[405] มาตรา 44 พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

[406] มาตรา 13 (4) พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

[407] มาตรา 53 พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

[408] มาตรา 75 และ 76 พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

[409] มาตรา 9 (4) พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

สองประการคือ ประการที่หนึ่ง การไม่จัดทำมาตรฐานดังกล่าวไม่มีโทษอาญาแต่อย่างใด จนกว่าจะเกิดภัยคุกคามไซเบอร์ระดับร้ายแรงขึ้นและผู้มีอำนาจได้สั่งให้แก้ไข ประการถัดมา กฎหมายฉบับนี้ ได้พูดถึงหน้าที่ของคณะกรรมการในการกำหนดมาตรฐานและตรวจสอบความปลอดภัยไซเบอร์ของตัวระบบแต่เพียงเท่านั้น แต่ไม่ได้กล่าวถึงตัวอุปกรณ์ที่ใช้ในกิจการนั้นๆ แต่อย่างใด

สำหรับกฎหมายของสหรัฐอเมริกาและสหภาพยุโรป หน่วยงานของรัฐนอกจากจะมีบริการรับรองมาตรฐานความปลอดภัยและการตรวจสอบรักษาความปลอดภัยให้แล้ว พันธกิจของหน่วยงานนั้นๆ ยังรวมไปถึงการตรวจสอบและรับรองมาตรฐานของอุปกรณ์ที่ใช้ในกิจการงานนั้นๆ ด้วย โดยไม่จำกัดว่าระบบรักษาความปลอดภัยหรืออุปกรณ์นั้นจะใช้ในระบบโครงสร้างพื้นฐานสำคัญหรือไม่ แต่กฎหมายไม่มีสภาพบังคับหากใช้สิ่งที่ไม่ได้ผ่านการรับรองมาตรฐาน ในทางตรงกันข้าม ประเทศจีนกลับบังคับให้ระบบรักษาความปลอดภัยทุกระบบและอุปกรณ์ทุกชิ้น ไม่ว่าจะใช้ในกิจการใด ต้องผ่านการรับรองจากรัฐก่อนเสมอ ดังนั้นอาจสรุปได้ว่ากฎหมายเรื่องการรับรองมาตรฐานความปลอดภัยและการตรวจสอบของประเทศไทยมีความคล้ายคลึงกับกฎหมายของสหรัฐอเมริกาและสหภาพยุโรปมากกว่า แต่ยังมีความแตกต่างกันบ้างในเรื่องขอบเขตงานว่าจะรวมไปถึงการตรวจสอบตัวอุปกรณ์ด้วยหรือไม่

4.5 การคุ้มครองข้อมูลส่วนบุคคล

1) กฎหมายจีน

การควบคุมความสมดุลระหว่างความปลอดภัยทางไซเบอร์ ความมั่นคงของชาติ และการปกป้องความเป็นส่วนตัว นับเป็นโจทย์ท้าทาย ก่อนจะมีการบังคับใช้กฎหมายความปลอดภัยทางไซเบอร์ รัฐบาลจีนได้ผ่านกฎหมายมากมายเพื่อคุ้มครองข้อมูลส่วนบุคคล ดังเช่น Decision of the Standing Committee of the National People's Congress to Strengthen the Protection of Internet Data (2012) และ The Guidelines for Personal Information Protection within Public and Commercial Services Information Systems (2013) และ the Provisions on Protecting the Personal Information of Telecommunication and Internet Users (2013) จนกระทั่งมาถึงกฎหมายความปลอดภัยทางไซเบอร์ซึ่งบัญญัติเรื่องการคุ้มครองข้อมูลส่วนบุคคลไว้อย่างชัดเจน

กฎหมายความปลอดภัยทางไซเบอร์ได้ให้นิยามคำว่า “ข้อมูลส่วนบุคคล” ไว้ว่า ข้อมูลที่ด้วยตัวมันเองหรือเมื่อนำไปรวมกับข้อมูลอื่นสามารถระบุตัวตนของบุคคลใดบุคคลหนึ่งหรือกลายเป็นข้อมูลใดข้อมูลหนึ่งอันอาจชี้ถึงตัวบุคคลนั้นๆ ได้ อาทิ ชื่อของบุคคลนั้น วันเกิด เลขบัตรประจำตัวประชาชน ข้อมูลรูปพรรณสัณฐาน

ที่อยู่ และหมายเลขโทรศัพท์[410] ดังนั้น หากข้อมูลเหล่านี้ได้รับการปกปิดหรือไม่ได้แสดงออกมาแต่แรก ก็จะไม่จัดว่าเป็นข้อมูลส่วนบุคคลตามกฎหมายนี้

จากกฎหมายความปลอดภัยทางไซเบอร์ ผู้ให้บริการโครงข่ายจะต้องรวบรวมหรือใช้ข้อมูลส่วนบุคคลอย่างถูกกฎหมาย เหมาะสม และเท่าที่จำเป็น และผู้ให้บริการต้องเปิดเผยวัตถุประสงค์ วิธีการ และขอบเขตในการรวบรวมข้อมูลของพวกเขา และได้รับความยินยอมจากบุคคลผู้นั้นก่อนที่จะทำการเก็บข้อมูลนั้นได้[411] ทั้งเจ้าของข้อมูลยังมีสิทธิในการเปลี่ยนแปลงแก้ไข หรือลบข้อมูลนั้นได้ด้วย[412] ทั้งนี้ ข้อมูลส่วนตัวใดที่ไม่เกี่ยวข้องกับการให้บริการ ห้ามผู้ให้บริการเก็บข้อมูลนั้น[413] นอกจากนี้ ห้ามผู้ให้บริการเปิดเผยข้อมูลเหล่านั้นกับบุคคลอื่น เว้นแต่ข้อยกเว้นดังนี้ 1. บุคคลที่ให้ข้อมูลนั้นได้ให้ความยินยอมแล้ว 2. ข้อมูลนั้นได้รับการแปลงสภาพให้ไม่สามารถทราบได้แล้วว่าหมายถึงบุคคลใดโดยเฉพาะเจาะจง[414] สุดท้ายนี้ ผู้ให้บริการไม่สามารถเปิดเผยดัดแปลง หรือทำลายข้อมูลที่พวกเขาเก็บมาได้[415]

หากผู้ให้บริการละเมิดบทบัญญัติที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลแล้ว ผู้ให้บริการอาจถูกตักเตือนและสั่งให้แก้ไข ยึดทรัพย์ หรือปรับไม่เกิน 1 ล้านหยวน และปรับผู้ที่มีส่วนรับผิดชอบโดยตรงและผู้บังคับบัญชาตั้งแต่ 1 หมื่นหยวน แต่ไม่เกิน 1 แสนหยวน ทว่าหากความเสียหายร้ายแรง ผู้ให้บริการอาจถูกสั่งให้ระงับการให้บริการในส่วนที่เกี่ยวข้อง ปิดเว็บไซต์ หรือระงับการประกอบกิจการทั้งหมด รวมไปถึงการระงับใบอนุญาตประกอบกิจการชั่วคราวหรือถาวร[416]

มีข้อสังเกตในประเด็นของกฎหมายอาญาคือการที่บุคคลต้องรับผิดเมื่อมีการฝ่าฝืนบทบัญญัติกฎหมายในส่วนข้อมูลส่วนบุคคล มิใช่เพียงผู้ที่มีหน้าที่ต้องรับผิดชอบโดยตรงเท่านั้นที่จะถูกโทษปรับ หากแต่ผู้บังคับบัญชาของผู้นั้นก็จะถูกโทษปรับไปด้วย ซึ่งขัดกับหลักที่ว่าบุคคลจะต้องรับผิดในทางอาญาก็ต่อเมื่อได้ทำโดยเจตนา อย่างไรก็ตาม กฎหมายอาจมองว่าผู้บังคับบัญชามีหน้าที่ต้องกำกับดูแลผู้ใต้บังคับบัญชาอยู่แล้วหากผู้ใต้บังคับบัญชาตนทำงานผิดพลาด ส่วนหนึ่งย่อมเป็นเพราะผู้บังคับบัญชาประมาทเลิกเล่อ เพิกเฉย ไม่กวดขันผู้ใต้บังคับบัญชาของตนเองให้ดี จนทำให้เกิดการละเมิดข้อมูลส่วนบุคคลได้ในที่สุด

หากพิจารณาในมาตรา 64 วรรคหนึ่งแล้วจะพบว่ามีวิธีการลงโทษที่หลากหลาย และยืดหยุ่นมาก ตั้งแต่ตักเตือน จนถึงโทษปรับ และระงับใบอนุญาตประกอบกิจการ ซึ่งเป็นการให้อำนาจแก่เจ้าหน้าที่ในการใช้ดุลพินิจที่กว้างขวางมาก จนทำให้การบังคับกฎหมายอาจไม่เป็นไปตามมาตรฐาน ดังเช่นในตัวอย่างคดีที่ 1 และ 2 ด้านล่าง แม้จะมีข้อเท็จจริงเดียวกันว่าแอปพลิเคชันเหล่านั้นไม่ได้ขอความยินยอมผู้ใช้ในการเก็บข้อมูลส่วนบุคคลแต่แรกเหมือนกัน ผลกลับปรากฏว่าผู้ให้บริการรายหนึ่งนอกจากจะถูกสั่งให้แก้ไขแล้ว ทั้ง

[410] 《中华人民共和国网络安全法》第 76 条
[411] 《中华人民共和国网络安全法》第 41 条
[412] 《中华人民共和国网络安全法》第 47 条
[413] 《中华人民共和国网络安全法》第 41 条
[414] 《中华人民共和国网络安全法》第 41 条
[415] 《中华人民共和国网络安全法》第 42 条
[416] 《中华人民共和国网络安全法》第 64 条 第一款

ผู้บังคับบัญชาและผู้ที่มีหน้าที่รับผิดชอบโดยตรงกลับต้องโดนปรับอีกคนละ 1 หมื่นหยวน ในขณะที่ผู้ให้บริการอีกหนึ่งรายนั้นกลับเพียงถูกตักเตือนแต่เพียงอย่างเดียวเท่านั้น กรณีนี้จึงมีข้อกังวลว่ากฎหมายที่มอบอำนาจดุลพินิจให้แก่เจ้าหน้าที่มากเกินไปจะทำให้การบังคับใช้กฎหมายเป็นไปตามอำเภอใจ และอาจเป็นการส่งเสริมให้ผู้กระทำผิดให้สินบนแก่เจ้าหน้าที่เพื่อหลีกเลี่ยงโทษสถานหนักแทน

ทั้งนี้ ในมาตรา 64 วรรคหนึ่ง เมื่อมีการละเมิดข้อมูลส่วนบุคคลเกิดขึ้นแล้ว กฎหมายได้ให้ดุลพินิจเจ้าหน้าที่ในการตักเตือนและสั่งให้แก้ไขได้ โดยไม่บังคับให้ลงโทษด้วยวิธีอื่นไปด้วยพร้อมกันแต่อย่างใด อำนาจนี้อาจสันนิษฐานได้ว่าผู้ร่างกฎหมายอาจยอมรับว่า การละเมิดข้อมูลส่วนบุคคลอาจเป็นความผิดที่เกิดขึ้นเพราะกฎหมายกำหนดให้เป็นความผิด (mala prohibita) ดังนั้นเป็นไปไม่ได้เลยที่สามัญสำนึกของมนุษย์จะทราบได้ว่าการเก็บข้อมูลอย่างถูกต้องนั้น ผู้ให้บริการต้องขอความยินยอมจากผู้ใช้งาน ดังนั้นผู้ร่างกฎหมายจึงกำหนดทางแก้ไขไว้ โดยให้มีการตักเตือนขึ้น เพื่อเปิดโอกาสให้บุคคลนั้นทำการแก้ไข และเพื่อให้ไม่เกิดการลงโทษแก่ผู้บริสุทธิ์โดยไม่จำเป็น โดยมากแล้ว ผู้ให้บริการที่กระทำผิดตามมาตรา 64 วรรคหนึ่ง ด้วยการไม่ได้ขออนุญาตเก็บข้อมูลส่วนบุคคลก่อน หรือละเลยปล่อยข้อมูลเหล่านั้นไปบนเว็บไซต์ของตนเองมักจะถูกตักเตือนเสียมาก มีคดีจำนวนน้อยรายมากที่การทำผิดครั้งแรกจะมีโทษปรับเกิดขึ้น

นอกจากผู้ให้บริการมีหน้าที่ตามกฎหมายที่จะต้องปฏิบัติตามเพื่อไม่ให้ละเมิดข้อมูลส่วนบุคคลแล้ว กฎหมายฉบับนี้ยังบังคับกับบุคคลอื่นโดยทั่วไปด้วยว่า “ห้ามมิให้ผู้ใดทำการโจรกรรมข้อมูลหรือทำการด้วยวิธีที่มิชอบด้วยกฎหมายอื่นใด เพื่อให้ได้มาซึ่งข้อมูลส่วนบุคคล รวมทั้งห้ามมิให้ทำการขายข้อมูลเหล่านั้นหรือมอบข้อมูลเหล่านั้นให้แก่ผู้อื่น”[417] หากผู้ใดฝ่าฝืนบทบัญญัติดังกล่าว ไม่ว่าจะมีการกระทำความผิดตามกฎหมายนี้เกิดขึ้นหรือไม่ก็ตาม ให้ตำรวจยึดทรัพย์ที่ได้มาจากการกระทำความผิดนี้ และปรับได้ตั้งแต่ 1 ถึง 10 เท่าของราคาทรัพย์นั้น และหากไม่มีทรัพย์ที่ได้มาจากการกระทำความผิด ให้ปรับไม่เกิน 1 ล้านหยวน

เมื่อพิจารณาโทษของการทำเพื่อให้ได้มาซึ่งข้อมูลส่วนบุคคลโดยมิชอบด้วยกฎหมาย หรือมอบข้อมูลเหล่านั้นให้แก่บุคคลอื่น จะพบว่ามีข้อสังเกต 2 ประการ ประการแรก กฎหมายข้อนี้ไม่ให้ดุลพินิจเจ้าหน้าที่ในการตักเตือนผู้กระทำผิดเลย อาจสันนิษฐานได้ว่าผู้ร่างกฎหมายมองว่าการโจรกรรมข้อมูลบุคคลอื่นเป็นการกระทำที่มีความผิดในตัวเอง (mala in se) และบุคคลทั่วไปสามารถเข้าใจได้เช่นเดียวกับการที่ตนเข้าใจว่าการขโมยทรัพย์สินผู้อื่นเป็นความผิด ดังนั้นการลงโทษผู้ที่กระทำการเช่นนี้จึงไม่ต้องมีการผ่อนปรน

ประการถัดมา บทลงโทษนี้มีมาตรการริบทรัพย์เด็ดขาด แม้ในกรณีที่บุคคลหนึ่งได้รับข้อมูลส่วนบุคคลของผู้อื่นมาโดยสุจริต เช่น สำคัญผิดว่าข้อมูลเหล่านั้นได้รับการยิมยอมจากเจ้าของข้อมูลส่วนบุคคลจริงทั้งในการรวบรวมและจำหน่ายต่อไปยังบุคคลที่สาม ทั้งที่จริงแล้ว ข้อมูลเหล่านั้นเป็นข้อมูลที่มิจฉาชีพเอามาปล่อยทิ้งไว้เพื่อสร้างความวุ่นวาย ถึงกระนั้น บุคคลที่รับข้อมูลมาโดยสุจริต และได้ทำการจำหน่ายไป เงินนั้นก็คงเป็นทรัพย์สินที่ได้มาจากการกระทำความผิดอยู่ ดังนั้น แม้บุคคลที่สุจริตนั้นจะไม่ต้องรับผิดในกฎหมายอาญาอื่นที่เกี่ยวข้อง บุคคลที่สุจริตนั้นก็ยังคงต้องถูกยึดเงินที่ได้มาจากการขายข้อมูลนั้น พร้อมทั้งถูกปรับด้วย บทบัญญัติ

[417] 《中华人民共和国网络安全法》第 44 条

ที่เข้มงวดนี้แสดงให้เห็นถึงความเด็ดขาดในการพยายามที่จะป้องกันไม่ให้บุคคลใดก็ตามไม่ว่าจะสุจริตหรือไม่ได้ไปซึ่งผลประโยชน์จากการใช้ข้อมูลส่วนบุคคลที่ได้มาโดยมิชอบ จนอาจคิดไปได้ว่ากฎหมายนี้ต่างจากกฎหมายลักษณะทรัพย์ที่คุ้มครองการได้มาของทรัพย์สินของผู้ที่เสียค่าตอบแทนโดยสุจริต ซึ่งอาจแสดงให้เห็นว่าข้อมูลส่วนบุคคลแม้จะมีค่า แต่ก็ไม่ได้มีถูกคุ้มครองในฐานะทรัพย์สินอย่างที่เข้าใจกัน หากแต่เป็นส่วนหนึ่งของบุคคล ๆ หนึ่ง และได้รับการเคารพในฐานะสิทธิส่วนบุคคลที่มีความสำคัญยิ่งกว่า ดังนั้นการคุ้มครองข้อมูลส่วนบุคคลจึงมีมาตรการที่เด็ดขาดกว่ามากเพื่อป้องกันความเสียหายต่าง ๆ ที่จะเกิดขึ้น

แม้กฎหมายนี้จะคุ้มครองความเป็นส่วนตัวของประชาชน โดยสร้างหน้าที่ให้กับผู้ให้บริการ ทว่าเจ้าหน้าที่รัฐกลับไม่ต้องอยู่ภายใต้บังคับของหน้าที่นี้ กล่าวคือภายในกฎหมายฉบับเดียวกัน แต่ในหมวดอื่นกฎหมายกลับเป็นเครื่องมือให้เจ้าหน้าที่รัฐใช้ในการควบคุมและสอดแนมข้อมูลส่วนบุคคลและโยนภาระต่างๆ ให้กับผู้ให้บริการ ตัวอย่างเช่น ผู้ให้บริการมีหน้าที่ให้ความช่วยเหลือทางเทคนิคแก่เจ้าหน้าที่รัฐในการรักษาความมั่นคงของชาติและสอบสวนอาชญากรรม ทำให้เจ้าหน้าที่รัฐสามารถใช้ช่องทางพิเศษเข้าถึงข้อมูลส่วนบุคคลได้โดยชอบด้วยกฎหมาย และด้วยการที่กฎหมายบังคับให้ผู้ให้บริการต้องเก็บข้อมูลส่วนตัวผู้ใช้บริการให้สามารถดูย้อนหลังได้ไม่น้อยกว่า 6 เดือน ซึ่งเพิ่มความเสี่ยงในการรั่วไหล ก็ฝ่าฝืนหลักการในการคุ้มครองข้อมูลส่วนบุคคลด้วยเช่นกัน และการเก็บข้อมูลในระยะเวลาที่ยาวนานเช่นนี้ก็เป็นการเพิ่มภาระแก่บริษัทรายย่อยด้วย

กฎหมายความปลอดภัยทางไซเบอร์นี้ รวมไปถึงการบังคับให้ผู้ใช้งานแสดงตัวตนของตนก่อนเข้าใช้งาน โดยมอบหน้าที่นี้ให้กับผู้ให้บริการ และห้ามผู้ให้บริการให้บริการกับผู้ใช้งานที่ไม่ยอมแสดงตัวตน ซึ่งมาตรการนี้ถูกอ้างว่ามีวัตถุประสงค์เพื่อใช้ปราบปรามข่าวลือ การใช้คำไม่สุภาพ สื่อลามกอนาจาร และข่าวสารที่เกี่ยวกับการก่อการร้าย อย่างไรก็ดี ในอีกมุมหนึ่ง กฎหมายนี้ก็เป็นเครื่องมือของรัฐบาลในการป้องกันไม่ให้ผู้ใช้งานอินเทอร์เน็ตวิพากษ์วิจารณ์รัฐบาลหรือกระจายข่าวของรัฐบาลว่าด้วยการทุจริต ดังนั้นระบบนี้จึงมีขึ้นเพื่อขัดขวางไม่ให้ผู้คนแสดงความคิดเห็นในที่สาธารณะ นอกจากนี้ นโยบายแสดงตัวตนอาจสร้างโอกาสให้แฮ็คเกอร์ทำการแฮ็คข้อมูลส่วนบุคคลเหล่านั้นจากผู้ให้บริการหลายรายได้อีกด้วย

2) เปรียบเทียบกฎหมายของประเทศสหรัฐอเมริกาและสหภาพยุโรป

กฎหมายสหรัฐอเมริกา

ก่อนปี ค.ศ. 2019 รัฐบาลกลางสหรัฐฯ ได้ออกกฎหมายเพียง 3 ฉบับเท่านั้นที่เกี่ยวข้องกับข้อมูลส่วนบุคคล โดยกฎหมายทั้ง 3 ฉบับนี้ได้แก่ รัฐบัญญัติว่าด้วยการเปลี่ยนแปลงแผนประกันสุขภาพและความรับผิด (Health Insurance Portability and Accountability Act) รัฐบัญญัติว่าด้วยการปฏิรูปธุรกิจการให้บริการทางการเงิน (Financial Services Modernization Act) และ รัฐบัญญัติว่าการบริหารจัดการความปลอดภัยในข้อมูลข่าวสารของรัฐบาลกลาง (Federal Information Security Management Act) ซึ่งต่างใช้คำกว้าง ๆ ว่าผู้ประกอบการหรือหน่วยงานรัฐที่ทำงานในด้านสาธารณสุข การเงิน หรือความมั่นคงต้องรักษาระบบและข้อมูลส่วนตัวให้เหมาะสม แต่ทั้งนี้ก็ไม่ได้มีบทลงโทษใด และเนื่องจากเป็นบทบัญญัติที่มีความหมายกว้างขวาง

จึงไม่อาจทราบได้ว่าควรดำเนินการไปในทิศทางใดเพื่อให้บรรลุวัตถุประสงค์นั้น ด้วยเหตุนี้ ในท้ายที่สุด การคุ้มครองข้อมูลส่วนบุคคลจึงไม่ได้รับการสนใจจากผู้ประกอบการหรือหน่วยงานภาครัฐเท่าที่ควร

นอกจากนี้ การล้มเหลวหรือละเมิดในข้อมูลส่วนบุคคลของบริษัท ๆ หนึ่งโดยการนำไปใช้ประโยชน์ต่อหรือนำไปขายต่อก็ดี มักนำไปสู่การพิจารณาโดยคณะกรรมการการค้า (Federal Trade Commission) ว่าเป็นหนึ่งในการกระทำทางการตลาดที่เป็นการหลอกลวง (Deceptive Practices) เท่านั้น โดยบริษัทจะมีความรับผิดตามการกระทำนั้นก็ต่อเมื่อบริษัทนั้นได้ทำผิดสัญญาว่าด้วยความเป็นส่วนตัว หรือไม่ได้จัดเตรียมมาตรการที่เหมาะสม และทำให้เกิดความเสียหายแก่เจ้าของข้อมูล[418]

ทั้งนี้ความรับผิดในการละเมิดข้อมูลส่วนบุคคลอาจเป็นเพียงส่วนเล็ก ๆ ที่สอดแทรกอยู่ในกฎหมายหลาย ๆ ฉบับ เช่น รัฐบัญญัติว่าด้วยการคุ้มครองความเป็นส่วนตัวของผู้ขับขี่ (Driver Privacy Protection Act) ซึ่งระบุให้ชื่อ รูปภาพ หมายเลขบัตรประจำตัวประชาชน หมายเลขประกันสังคม ที่กรมขนส่ง (Department of Motor Vehicles) ได้รวบรวมไว้ได้รับความคุ้มครองตามกฎมหาย และการเปิดเผยรายละเอียดดังข้างต้นโดยปราศจากความยินยอมถือว่าเป็นความผิด หรือรัฐบัญญัติว่าด้วยการปกป้องความเป็นส่วนตัวของเยาวชนบนโลกออนไลน์ (Children's Online Privacy Protection Act) ซึ่งห้ามมิให้ผู้ใดเก็บรวมรวมข้อมูลส่วนตัวของเด็กอายุต่ำกว่า 13 ปี ในรูปแบบออนไลน์ เว้นแต่จะได้รับความยินยอมจากผู้ปกครองก่อน [419]

ความกระจัดกระจายของกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ประกอบกับความไม่ชัดเจนของแนวทางปฏิบัติตดังกล่าวทำให้สรุปได้ว่า ในช่วงก่อนปี ค.ศ. 2019 กฎหมายของสหรัฐอเมริกายังไม่ได้เล็งเห็นถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลอย่างเป็นเฉพาะมากเท่าใดนัก

จนกระทั่งปี ค.ศ. 2019 รัฐบัญญัติความมั่นคงของชาติและการคุ้มครองข้อมูลส่วนบุคคลได้ถูกนำเสนอขึ้น โดยมีลักษณะเป็นการคุ้มครองข้อมูลส่วนบุคคล โดยคำว่าข้อมูลผู้ใช้ (User data) ซึ่งเป็นสิ่งที่ถูกคุ้มครองตามกฎหมายฉบับนี้มีนิยามว่า[420] “ข้อมูลข่าวสารใด ๆ ซึ่งบุคคลใดก็ตามได้รับมาจากการให้บริการเชิงข้อมูล เช่นผ่านทางเว็บไซด์ หรือแอปพลิเคชัน โดยข้อมูลเหล่านั้นอาจทำให้ทราบถึง แสดงถึงความสัมพันธ์ อธิบาย หรือมีส่วนเกี่ยวข้องกับพลเมืองสัญชาติอเมริกาหรือมีถิ่นพำนักอยู่ในสหรัฐอเมริกา อนึ่ง ไม่จำต้องพิจารณาว่าข้อมูลเหล่านั้นได้มาจากตัวเจ้าของข้อมูลเองหรือไม่ ได้มาจากการสังเกตพฤติกรรมของเจ้าของข้อมูลเองหรือไม่

---

[418] Chabinsky, Steven. 2019. "ICLG - Data Protection Laws And Regulations - USA Covers Relevant Legislation And Competent Authorities, Territorial Scope, Key Principles, Individual Rights, Registration Formalities, Appointment Of A Data Protection Officer And Of Processors - In 42 Jurisdictions". International Comparative Legal Guides International Business Reports. https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa.

[419] เรื่องเดียวกัน.

[420] มาตรา 2(6) National Security and Personal Data Protection Act

หรือได้ข้อมูลเหล่านั้นมาด้วยวิธีการใด”เมื่อข้อมูลเหล่านั้นตรงตามนิยามของกฎหมาย บริษัทที่ครอบครองข้อมูลนั้นจะมีหน้าที่ตามกฎหมาย

ในกรณีที่บริษัทนั้นเป็นบริษัทเทคโนโลยีอันอยู่ในข่าย (Covered technology company) อันหมายถึงบริษัทที่มีการให้บริการออนไลน์เป็นหลัก บริษัทจะมีหน้าที่ดังต่อไปนี้[421]

1. หน้าที่ในการเก็บข้อมูลเท่าที่จำเป็น (Minimal Collection of Data)

บริษัทต้องไม่เก็บข้อมูลผู้ใช้มากเกินกว่าความจำเป็นในการให้บริการนั้น ๆ

2. หน้าที่ในการไม่นำข้อมูลนั้นไปใช้ประโยชน์ต่อ (Prohibition on Secondary Uses)

การไม่นำข้อมูลนั้นไปใช้ประโยชน์ต่อรวมไปถึงการห้ามไม่ให้บริษัทนำข้อมูลนั้นไปใช้ประกอบการวิเคราะห์เพื่อให้การโฆษณานั้นตรงต่อกลุ่มเป้าหมาย หรือแสดงข้อมูลต่อบุคคลที่สามหรือระบุถึงตัวตนของเจ้าของข้อมูลโดยไม่จำเป็น

3. หน้าที่ในการอนุญาตให้เจ้าของข้อมูลดูข้อมูลและลบข้อมูลนั้น (Right to Review and Delete Data)

บริษัทต้องอนุญาตให้เจ้าของข้อมูลดูข้อมูลที่บริษัทนั้นครอบครองอยู่และลบข้อมูลเหล่านั้นอย่างถาวรตามความประสงค์ของเจ้าของข้อมูล โดยไม่จำกัดว่าข้อมูลนั้น บริษัทได้มาโดยวิธีการใด

4. หน้าที่ในการรายงานผล (Reporting Requirement)

ผู้บริหารสูงสุดของบริษัทมีหน้าที่ในการรายงานไปยังหน่วยงานภาครัฐรายปีว่าบริษัทได้ทำตามมาตรการเหล่านี้แล้วอย่างไรบ้าง

ทว่า สำหรับบริษัทเทคโนโลยีทั่วไป ไม่ปรากฏว่ามีหน้าที่ใดในการการคุ้มครองข้อมูลส่วนบุคคล ทั้งนี้ไม่ว่าบริษัทเทคโนโลยีจะจัดเป็นประเภทใด มาตรการการเก็บรวบรวมข้อมูลไว้ในท้องที่ยังเป็นสิ่งที่ต้องปฏิบัติตามอยู่เสมอ

กฎหมายสหภาพยุโรป

กฎหมายสำคัญที่เกี่ยวข้องกับการเก็บรวบรวมข้อมูลไว้ภายในท้องที่ได้แก่ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC หรือ General Data Protection Regulation ซึ่งได้นิยามคำว่าข้อมูลส่วนบุคคล ไว้ว่าหมายถึง “ข้อมูลใด ๆ ก็ตามที่สามารถทำให้ทราบถึงบุคคลใดได้โดย

[421] มาตรา 3 National Security and Personal Data Protection Act

เฉพาะเจาะจง ไม่ว่าจะโดยตรงหรือโดยอ้อม เช่น ชื่อ หมายเลขบัตรประจำตัวประชาชน ข้อมูลสถานที่ ตัวตนบนโลกออนไลน์ ตลอดจนรูปลักษณ์ทางกายภาพ อุปนิสัย ภาวะทางจิต อารมณ์ สถานะทางเศรษฐกิจ วัฒนธรรม หรือสภาพทางสังคมของบุคคลนั้น”[422]

ในการจัดเก็บข้อมูล ผู้รวบรวมข้อมูลจะต้องปฏิบัติตามวิธีการที่กฎหมายกำหนดไว้ เช่นการขอความยินยอมแก่เจ้าของข้อมูลก่อน การจัดให้รูปแบบการขอความยินยอมต้องแยกออกมาจากข้อตกลงการใช้บริการอื่นอย่างชัดเจน หรือการแจ้งให้ทราบถึงสิทธิของเจ้าของข้อมูลในการถอนความยินยอม[423] และนอกจากวิธีการทั่วไปในการขอความยินยอมแล้ว หากปรากฏว่าเจ้าของข้อมูลอายุต่ำกว่า 16 ปี ผู้ปกครองของเจ้าของข้อมูลจะต้องให้ความยินยอมร่วมด้วย[424]

ในการคุ้มครองข้อมูล กฎหมายกำหนดให้ผู้ควบคุมมีหน้าที่ต้องใช้มาตรการที่เหมาะสมในการคุ้มครองข้อมูลที่ได้มา[425] และมีการจำกัดบัญญัติรองรับสิทธิของเจ้าของข้อมูลด้วยเช่น สิทธิในการเข้าถึงข้อมูลของตนเอง[426] สิทธิในการแก้ไขข้อมูลของตนเองให้ถูกต้อง[427]สิทธิในการถูกลืม[428] สิทธิในการยับยั้งการประมวลผลข้อมูล[429]

การฝ่าฝืนทั้งในการจัดเก็บข้อมูล การคุ้มครองข้อมูล หรือการละเมิดสิทธิของเจ้าของข้อมูลก็ดี ผู้ฝ่าฝืนจะได้รับโทษปรับตามมาตรา 83 และมาตรา 84 ของกฎหมายฉบับนี้ ซึ่งค่าปรับอาจปรับเป็นจำนวนเงินแน่ชัดหรือเป็นอัตราส่วนร้อยละจากผลประกอบการรายปีของบริษัทนั้นก็ได้ แล้วแต่กรณี

3) เปรียบเทียบกฎหมายของประเทศไทย

จากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 คำว่าข้อมูลส่วนบุคคล หมายถึง “ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ”[430] และมีบุคคลอีกสองประเภทซึ่งมีส่วนเกี่ยวข้องกับข้อมูลส่วนบุคคลได้แก่ “ผู้ควบคุมข้อมูลส่วนบุคคล” ซึ่งได้แก่ บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจ เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล[431] และ “ผู้ประมวลผลข้อมูลส่วนบุคคล” ซึ่งได้แก่ บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับ

---

[422] มาตรา 4 (1) General Data Protection Regulation

[423] มาตรา 7 General Data Protection Regulation

[424] มาตรา 8 General Data Protection Regulation

[425] มาตรา 25 General Data Protection Regulation

[426] มาตรา 15 General Data Protection Regulation

[427] มาตรา 16 General Data Protection Regulation

[428] มาตรา 17 General Data Protection Regulation

[429] มาตรา 18 General Data Protection Regulation

[430] มาตรา 6 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[431] เรื่องเดียวกัน.

การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล[432]

เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลเกิดขึ้นได้ กฎหมายได้บัญญัติหน้าที่ให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล ดังต่อไปนี้

1. ผู้ควบคุมข้อมูลส่วนบุคคลจะกระทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไม่ได้ หากเจ้าของข้อมูลส่วนบุคคลไม่ได้ให้ความยินยอมไว้ก่อนหรือในขณะนั้น[433] โดยการขอความยินยอมต้องทำโดยชัดแจ้ง เป็นหนังสือหรือทำโดยผ่านระบบอิเล็กทรอนิกส์[434] โดยการขอความยินยอมนั้น ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งไปยังเจ้าของข้อมูลส่วนบุคคลด้วยว่าจะทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นไปเพื่อวัตถุประสงค์ใด ด้วยภาษาที่อ่านง่ายและชัดเจน ทั้งนี้การขอความยินยอมนั้นจะต้องแยกออกมาจากข้อความอื่น ๆ ด้วย[435]

อนึ่ง ผู้ควบคุมข้อมูลส่วนบุคคลอาจทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลได้ แม้ปราศจากความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ถ้าหากกฎหมายนี้หรือกฎหมายอื่นกำหนดให้ทำได้[436]

2. ในการเข้าทำสัญญาหรือให้บริการใดๆ ผู้ควบคุมข้อมูลส่วนบุคคลต้องไม่ขอความยินยอมเพื่อเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ไม่มีความจำเป็นในการเข้าทำสัญญาหรือการให้บริการนั้น ๆ[437]

3. ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลจะขอความยินยอมเจ้าของข้อมูลส่วนบุคคลในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล หากปรากฏว่าเจ้าของข้อมูลเป็นผู้ไร้ความสามารถในการทำนิติกรรมตามกฎหมาย การขอความยินยอมอาจต้องปฏิบัติตามหลักเกณฑ์ ดังต่อไปนี้

1) เจ้าของข้อมูลส่วนบุคคลเป็นผู้เยาว์ที่มีอายุตั้งแต่สิบปีขึ้นไป หากปรากฏว่าการให้ความยินยอมของผู้เยาว์นั้นไม่เกี่ยวข้องกับการใดๆ ซึ่งผู้เยาว์อาจให้ความยินยอมได้โดยลำพังได้ตามที่บัญญัติไว้ในมาตรา 22[438]

---

[432] เรื่องเดียวกัน.

[433] มาตรา 19 วรรคหนึ่ง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[434] มาตรา 19 วรรคสอง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[435] มาตรา 19 วรรคสาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[436] มาตรา 19 วรรคหนึ่ง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[437] มาตรา 19 วรรคสี่ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[438] มาตรา 22 ประมวลกฎหมายแพ่งและพาณิชย์ “ผู้เยาว์อาจทำการใด ๆ ได้ทั้งสิ้น หากเป็นเพียงเพื่อจะได้ไปซึ่งสิทธิอันใดอันหนึ่ง หรือเป็นการเพื่อให้หลุดพ้นจากหน้าที่อันใดอันหนึ่ง”

มาตรา 23[439] หรือมาตรา 24[440] แห่งประมวลกฎหมายแพ่งและพาณิชย์ และผู้เยาว์ประสงค์จะให้ความยินยอมในการดังกล่าว ก็จะต้องได้รับความยินยอมจากผู้ใช้อำนาจปกครอง[441]

2) เจ้าของข้อมูลส่วนบุคคลเป็นผู้เยาว์อายุต่ำกว่าสิบปี คนไร้ความสามารถ หรือคนเสมือนไร้ความสามารถ ผู้ควบคุมข้อมูลต้องขอความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์ ผู้อนุบาลที่มีอำนาจกระทำการแทนคนไร้ความสามารถ หรือผู้พิทักษ์ที่มีอำนาจกระทำการแทนคนเสมือนไร้ความสามารถเท่านั้น ไม่สามารถขอกับเจ้าของข้อมูลส่วนบุคคลนั้นได้เองโดยตรง[442]

4. ผู้ควบคุมข้อมูลส่วนบุคคลต้องทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ได้แจ้งเจ้าของข้อมูลส่วนบุคคลไว้ก่อนหรือในขณะที่เก็บรวบรวม อนึ่ง หากผู้ควบคุมข้อมูลส่วนบุคคลจะทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนอกขอบวัตถุประสงค์ที่ได้แจ้งเจ้าของข้อมูลส่วนบุคคลนั้น ผู้ควบคุมข้อมูลส่วนบุคคลจะทำได้ก็ต่อเมื่อตรงตามเงื่อนไขข้อใดข้อหนึ่งดังนี้[443]

1) ผู้ควบคุมข้อมูลส่วนบุคคลได้แจ้งวัตถุประสงค์ใหม่แก่เจ้าของข้อมูล และได้รับความยินยอมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลแล้ว

2) กฎหมายนี้หรือกฎหมายอื่นกำหนดให้ทำได้

ประเด็นที่น่าสนใจสำหรับการวิเคราะห์กฎหมายฉบับนี้ คือหลักการที่ว่าผู้ควบคุมข้อมูลส่วนบุคคลจะกระทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไม่ได้โดยปราศจากความยินยอมของเจ้าของข้อมูลส่วนบุคคล ซึ่งมีข้อยกเว้นว่าอาจทำการข้างต้นได้ หากมีกฎหมายนี้หรือกฎหมายอื่นให้อำนาจไว้ โดยจากที่พบได้คือพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้บัญญัติถึงสิทธิและวิธีการเก็บข้อมูลส่วนบุคคลไว้ไม่ต่างจากกฎหมายของสหภาพยุโรปมากนัก ซึ่งอาจทำให้เข้าใจได้ว่าประเทศไทยต้องการให้เกิดการไหลเวียนเสรีทางข้อมูลระหว่างสหภาพยุโรปและไทย เนื่องจากตามกฎหมายของสหภาพยุโรปแล้ว หากประเทศปลายทางที่โอนข้อมูลไปนั้นมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่ด้อยกว่าสหภาพยุโรป การโอนข้อมูลส่วนบุคคลไปมาหากันอาจจะทำไม่ได้เลย และกลายเป็นอุปสรรคสำหรับภาคธุรกิจ

อย่างไรก็ดี แม้ประเทศไทยจะมีกฎหมายคุ้มครองข้อมูลส่วนบุคคลแล้วก็ตาม แต่ก็มีกฎหมายหลายฉบับที่เป็นข้อยกเว้นของกฎหมายฉบับนี้ด้วย เช่น พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.

---

[439] มาตรา 23 ประมวลกฎหมายแพ่งและพาณิชย์ “ผู้เยาว์อาจทำการใด ๆ ได้ทั้งสิ้น ซึ่งเป็นการต้องทำเองเฉพาะตัว”

[440] มาตรา 24 ประมวลกฎหมายแพ่งและพาณิชย์ “ผู้เยาว์อาจทำการใด ๆ ได้ทั้งสิ้น ซึ่งเป็นการสมแก่ฐานานุรูปแห่งตนและเป็นการอันจำเป็นในการดำรงชีพตามสมควร”

[441] มาตรา 20 (1) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[442] มาตรา 20 (2) มาตรา 20 วรรคสามและสี่ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[443] มาตรา 21 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

2562 หรือพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ที่มอบอำนาจให้ฝ่ายบริหารสามารถขอให้ผู้ให้บริการทางเครือข่ายส่งมอบข้อมูลที่ตนเองต้องการมาได้ หากเป็นไปเพื่อยับยั้งความผิดเกี่ยวกับคอมพิวเตอร์ ความผิดเกี่ยวกับความมั่นคง หรือความผิดอื่นๆ โดยผู้ให้บริการต้องส่งมอบข้อมูลระบุตัวตนผู้ที่เข้าสู่ระบบคอมพิวเตอร์ไปให้ ซึ่งแท้จริงแล้ว ข้อมูลนั้นก็คือข้อมูลส่วนบุคคลนั่นเอง หรือตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ที่มอบอำนาจให้ ได้แก่ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติในการเข้าถึงข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทำสำเนา หรือสกัดคัดกรองข้อมูลสารสนเทศหรือโปรแกรมคอมพิวเตอร์ ซึ่งมีเหตุอันควรเชื่อได้ว่าเกี่ยวข้อง ดังนั้นข้อมูลส่วนบุคคลก็อาจมีความเสี่ยงที่จะถูกคุกคามได้เช่นกัน

ด้วยเหตุนี้ ถึงแม้ว่าประเทศไทยจะจัดให้มีพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เพื่อให้มาตรฐานการคุ้มครองข้อมูลส่วนบุคคลในประเทศสอดคล้องกับกฎหมายของสหภาพยุโรปแล้วก็ตาม อย่างไรก็ดี ด้วยความที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีข้อยกเว้นเป็นกฎหมายอื่นหลายฉบับ โดยเฉพาะอย่างยิ่งที่เป็นกฎหมายที่อ้างเหตุผลด้านความมั่นคงและให้อำนาจฝ่ายบริหารได้โดยปราศจากการใช้คำสั่งศาล กรณีจึงเป็นที่น่าสงสัยว่าพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลจะใช้ได้อย่างมีประสิทธิภาพและตรงตามมาตรฐานขั้นต่ำตามที่กฎหมายของสหภาพยุโรปกำหนดไว้หรือไม่

5. บทเรียนด้านกฎหมาย

จากการศึกษาเปรียบเทียบข้างต้น สามารถสรุปว่าในแต่ละประเด็น ประเทศไทยเลือกเดินตามโมเดลกฎหมายประเทศใด ดังนี้

หัวข้อ	ประเทศไทยใช้โมเดลกฎหมายประเทศใด
หน้าที่ตามกฎหมายของผู้ให้บริการทางเครือข่าย	**โมเดลจีน** โดยหน้าที่สำคัญของผู้ให้บริการทางเครือข่ายเป็นหน้าที่การช่วยเหลือรัฐในการป้องปรามการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ส่วนนี้ไม่มีในกฎหมายสหภาพยุโรปและกฎหมาย

หัวข้อ	ประเทศไทยใช้โมเดลกฎหมายประเทศใด
	สหรัฐอเมริกา) อย่างไรก็ตาม ในกฎหมายไทย ไม่มีมาตราใดหรือกฎหมายอื่นใดที่กล่าวถึงหน้าที่ของผู้ให้บริการในการเสริมสร้างระบบการรักษาความปลอดภัยของตน ซึ่งเป็นส่วนที่มีทั้งในกฎหมายจีนและกฎหมายของสหภาพยุโรป
การปกป้องระบบโครงสร้างพื้นฐานสำคัญ	**โมเดลสหรัฐอเมริกาและโมเดลสหภาพยุโรป** โดยกฎหมายเกี่ยวกับการกำหนดให้มีมาตรฐานขั้นต่ำในการบริหารจัดการความเสี่ยงที่อาจเกิดต่อระบบโครงสร้างพื้นฐานของไทยไม่มีสภาพบังคับหรือโทษอาญาแต่อย่างใด หากหน่วยงานใดไม่ได้จัดให้มีขึ้นและมีหน่วยงานรัฐเป็นผู้ออกแนวทางหรือคู่มือให้เอกชนนำไปปรับใช้หรือปฏิบัติตาม **โมเดลจีน** กฎหมายไทยกำหนดโทษอาญาเช่นเดียวกับกฎหมายของจีนเฉพาะในสองกรณี ได้แก่ หากปรากฏว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้นต่อระบบโครงสร้างพื้นฐานสำคัญและไม่มีการแจ้งสถานการณ์ที่เกิดขึ้นต่อหน่วยงานรัฐ หรือในกรณีที่มีภัยคุกคามทางไซเบอร์เกิดขึ้นต่อระบบโครงสร้างพื้นฐานสำคัญในระดับร้ายแรง และผู้มีอำนาจตามกฎหมายนี้ได้สั่งให้แก้ไขมาตรฐานความปลอดภัย
การเก็บรวบรวมข้อมูลไว้ภายในท้องที่	**โมเดลสหภาพยุโรป** ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศได้ถูกกำหนดไว้ว่าจะทำได้ก็ต่อเมื่อประเทศปลายทางที่ข้อมูลโอนไปนั้นมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ อย่างไรก็ตาม กฎหมายไทยมีความพิเศษอยู่คือ การโอนข้อมูลส่วนบุคคลไปยังประเทศที่ไม่มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอก็อาจทำได้เช่นกัน หากเข้าเหตุยกเว้นตามที่กฎหมายกำหนดไว้ ซึ่งไม่ปรากฏว่ากฎหมายของสหรัฐอเมริกา สหภาพ

หัวข้อ	ประเทศไทยใช้โมเดลกฎหมายประเทศใด
	ยุโรป หรือประเทศจีนจะมีเหตุยกเว้นเหล่านี้แต่อย่างใด
การรับรองมาตรฐานความปลอดภัยและการตรวจสอบ	**โมเดลสหรัฐอเมริกาและโมเดลสหภาพยุโรป** หน่วยงานของรัฐนอกจากจะมีบริการรับรองมาตรฐานความปลอดภัยและการตรวจสอบรักษาความปลอดภัยให้แล้ว พันธกิจของหน่วยงานนั้นๆ ยังรวมไปถึงการตรวจสอบและรับรองมาตรฐานของอุปกรณ์ที่ใช้ในกิจการงานนั้นๆ ด้วย โดยไม่จำกัดว่าระบบรักษาความปลอดภัยหรืออุปกรณ์นั้นจะใช้ในระบบโครงสร้างพื้นฐานสำคัญหรือไม่ แต่กฎหมายไม่มีสภาพบังคับหากใช้สิ่งที่ไม่ได้ผ่านการรับรองมาตรฐาน อย่างไรก็ตาม กฎหมายไทยมีความแตกต่างกันในเรื่องขอบเขตงานว่าจะรวมไปถึงการตรวจสอบตัวอุปกรณ์ด้วยหรือไม่
การคุ้มครองข้อมูลส่วนบุคคล	**โมเดลสหภาพยุโรป** พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลในประเทศสอดคล้องกับกฎหมายของสหภาพยุโรป **โมเดลจีน** พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีข้อยกเว้นเป็นกฎหมายอื่นหลายฉบับ โดยเฉพาะอย่างยิ่งที่เป็นกฎหมายที่อ้างเหตุผลด้านความมั่นคงและให้อำนาจฝ่ายบริหารได้โดยปราศจากการใช้คำสั่งศาล

หากสรุปในภาพกว้าง จะเห็นว่า แนวคิดด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของสหรัฐอเมริกา อยู่ที่การรักษาโครงสร้างพื้นฐานอินเทอร์เน็ต ในขณะที่แนวคิดด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของจีนอยู่ที่การรักษาความมั่นคงของรัฐ ส่วนแนวคิดด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของยุโรปมุ่งไปที่การคุ้มครองดูแลผู้ใช้งาน โดยเน้นความปลอดภัยและการรักษาข้อมูลส่วนบุคคล จากการศึกษา เห็นได้ชัดเจนว่า โมเดลกฎหมายจีนเริ่มมีอิทธิพลต่อการบัญญัติกฎหมายของประเทศไทยในการกำกับดูแลเศรษฐกิจดิจิทัลในยุคไทยแลนด์ 4.0 ถึงแม้ว่าในทางรูปแบบและเนื้อหาของกฎหมายส่วนใหญ่ จะมีความพยายามยึดตามโมเดลของสหภาพยุโรปและสหรัฐอเมริกา แต่ก็มีการสอดแทรกเนื้อหาหรือลักษณะเด่น

ของโมเดลจีนด้วย อาทิ ในประเด็นหน้าที่ทางกฎหมายของผู้ให้บริการทางเครือข่าย ซึ่งมีลักษณะคล้ายกฎหมายจีน การปกป้องระบบโครงสร้างพื้นฐานสำคัญ ซึ่งมีการกำหนดโทษอาญาในสองกรณี รวมทั้งการคุ้มครองข้อมูลส่วนบุคคล ซึ่งแม้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะบัญญัติมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลในประเทศสอดคล้องกับกฎหมายของสหภาพยุโรป แต่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ก็มีข้อยกเว้นเป็นกฎหมายอื่นหลายฉบับ โดยเฉพาะอย่างยิ่งที่เป็นกฎหมายที่อ้างเหตุผลด้านความมั่นคงและให้อำนาจฝ่ายบริหารได้โดยปราศจากการใช้คำสั่งศาล

ขณะเดียวกัน ก็มีข้อสังเกตที่น่าสนใจว่า ในประเทศตะวันตกเอง ก็เริ่มมีกระแสการเดินตามโมเดลจีนบ้างเช่นกัน เนื่องจากความกังวลเรื่องภัยคุกคามต่อความมั่นคง การแข่งขันทางเทคโนโลยีระหว่างมหาอำนาจและความปลอดภัยทางไซเบอร์ ดังนั้น เส้นการแบ่งแยกที่ชัดเจนระหว่างสำนัก Cyber Paternalism ตามแนวจีน กับสำนัก Cyber Commons ตามแนวตะวันตก อาจไม่สามารถแบ่งได้ชัดเจนดังเช่นในอดีต โดยจะมีความซับซ้อนมากขึ้นตามแต่ละประเด็นกฎหมาย รวมทั้งจะมีแนวโน้มเป็นเรื่องของระดับการที่รัฐเข้ามากำกับดูแลไซเบอร์สเปซมากกว่าเรื่องว่ารัฐจะเข้ามากำกับหรือไม่ ตัวอย่างที่ชัดเจน เช่น กฎหมายการเข้ารหัสข้อมูลของประเทศออสเตรเลีย ซึ่งบังคับให้บริษัทผู้ให้บริการเทคโนโลยีคอมพิวเตอร์ยอมให้รัฐ ตำรวจ หรือข้าราชการในองค์การเกี่ยวกับความปลอดภัยเข้าถึงข้อมูลที่เข้ารหัสหรือเป็นความลับของผู้ใช้งานโดยที่ผู้ใช้งานไม่รู้ตัว เพื่อจัดการอาชญากรรม การก่อการร้าย และดูแลความมั่นคงของประเทศ หรือเช่นร่างกฎหมายรัฐบัญญัติความมั่นคงของชาติและการคุ้มครองข้อมูลส่วนบุคคล (National Security and Personal Data Protection Act) ของสหรัฐอเมริกา ซึ่งจะบังคับให้บริษัทต่าง ๆ ในสหรัฐอเมริกาต้องไม่ถ่ายโอนข้อมูลของพลเมืองอเมริกาที่เก็บได้ในประเทศไปเก็บไว้ที่ประเทศอื่นที่มีความน่ากังวล เช่น จีนหรือรัสเซีย อย่างไรก็ตาม จะเห็นว่าสหภาพยุโรปยังมีความชัดเจนในเรื่องอุดมการณ์ตามแนวทางของสำนัก Cyber Commons และมีมาตรฐานที่สูงกว่าสหรัฐอเมริกาในเรื่องการคุ้มครองข้อมูลส่วนบุคคลและการสร้างหลักประกันให้ไซเบอร์สเปซเป็นโลกเสรี

บทเรียนด้านกฎหมายที่สำคัญ คือ ในการวางแนวทางการกำกับดูแลเศรษฐกิจดิจิทัลในยุคไทยแลนด์ 4.0 จะต้องก้าวข้ามกรอบคิดว่าจะเลือกแบบสำนัก Cyber Paternalism ตามแนวจีน หรือสำนัก Cyber Commons ตามแนวตะวันตก แต่จะต้องพิจารณาถึงการสร้างสมดุลระหว่าง 2 แนวคิด ผ่านการออกแบบกลไกที่เหมาะสม และการออกแบบเกณฑ์หรือมาตรฐานที่จำกัดการใช้ดุลยพินิจของรัฐเกินสมควร ตัวอย่างเช่น ในกฎหมายการเข้ารหัสของออสเตรเลียนั้น เจ้าหน้าที่สามารถขอความช่วยเหลือจากผู้ให้บริการโดยต้องมีหมายศาล มีเกณฑ์ระบุชัดถึงเหตุผลของเจ้าหน้าที่ในการใช้อำนาจตามกฎหมาย และในทางเทคนิค เพียงบังคับให้ผู้ให้บริการสร้างช่องทางพิเศษไว้เตรียมพร้อม ซึ่งแตกต่างจากแนวทางของจีนที่ขาดกลไกในการจำกัดการใช้ดุลยพินิจของรัฐ เป็นที่น่าเสียดายว่า ในกฎหมายของไทยในส่วนที่คล้ายกับโมเดลจีน มักขาดการออกแบบกลไกหรือเกณฑ์ที่ชัดเจน แต่มักอาศัยการให้ดุลยพินิจแก่เจ้าหน้าที่รัฐด้วยภาษากฎหมายที่กำกวมและเปิดให้มีการตีความเพื่อใช้ดุลยพินิจได้อย่างกว้างขวาง ตัวอย่างเช่น ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งมีข้อยกเว้นเป็นกฎหมายที่อ้างเหตุผลด้านความมั่นคงและให้อำนาจฝ่ายบริหารได้โดยปราศจากการใช้คำสั่งศาล

รายชื่อผู้จัดทำ

นักวิจัยหลัก

ชื่อ ดร. อาร์ม ตั้งนิรันดร

หน่วยงานสังกัดและสถานที่ติดต่อ

คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ซอยจุฬาฯ
เลขที่ 42 ถนนพญาไท แขวงวังใหม่ เขตปทุมวัน
กรุงเทพมหานคร 110330
โทรศัพท์: 02-218-2017
E-mail: armtung@gmail.com