



วิทยาการบริหารภาครัฐสมัยใหม่
Modern Public Administrative Science-MPAS

homepage: <https://so17.tci-thaijo.org/index.php/jppi>
E-mail: jppissues@gmail.com



From Digital to the Core to Trust First: Reading Singapore's Digital Government Success through the Lens of Trust Costs, and Its Implications for Thailand

Sakon Duangkhampha ^{1*}

¹ Bachelor of Public Administration Programme, Faculty of Management Science, Sakon Nakhon Rajabhat University, Thailand

*Corresponding author's e-mail: sakon.duangkampa@gmail.com

ARTICLE INFO

Article history:

Received: February 1, 2026

Revised: August 29, 2026

Accepted: August 30, 2026

Keyword: digital government, Singapore, Smart Nation 2.0, public trust, data integration, GovTech, policy transfer

ABSTRACT

Singapore ranked third worldwide in the 2024 United Nations E-Government Development Index and is commonly presented in Thai scholarship as a model of centralized digital government built on the Government Technology Agency, the Digital Government Blueprint and four service pillars. This academic article argues that such an account is incomplete because it stops at the architecture and omits its price. The article draws attention to a decisive but under-analysed fact: when Singapore refreshed its national vision as Smart Nation 2.0 on 1 October 2024, it organised the strategy around three goals and placed Trust first, ahead of Growth and Community, whereas the 2014 and 2018 framings had been organised around digitalization and service transformation. Through documentary analysis of Singaporean policy instruments, official inquiry reports and recent peer-reviewed literature, the article reads this reordering as a policy admission that deep data integration generates trust costs. Two episodes are examined: the 2018 SingHealth breach, in which the personal particulars of 1.5 million patients were stolen and the Prime Minister was specifically targeted, and the 2021 TraceTogether episode, in which the government acknowledged its error in stating that the data was exempt from the Criminal Procedure Code and subsequently legislated to confine police access to seven categories of serious offence. From these the article develops the concept of a trust ceiling: the depth of data integration a state can sustain is bounded by the trust it can maintain, and guarantees must be legislated before integration deepens, because retrospective correction repairs the rule but not the trust. Implications for Thailand, a state with roughly 7,776 local administrative organizations and no equivalent to Singapore's single administrative tier, are then set out.

จาก Digital to the Core สู่ Trust First: อ่านความสำเร็จของภาครัฐดิจิทัลสิงคโปร์ ผ่านต้นทุนความไว้วางใจ และนัยต่อประเทศไทย

สากล ดั่งคำภา ^{1*}

¹ หลักสูตรรัฐประศาสนศาสตรบัณฑิต สาขาวิชารัฐประศาสนศาสตร์ คณะวิทยาการจัดการ มหาวิทยาลัยราชภัฏสกลนคร

*Corresponding author's e-mail: sakon.duangkampa@gmail.com

ข้อมูลบทความ

ประวัติบทความ:

Received: February 1, 2026

Revised: August 29, 2026

Accepted: August 30, 2026

คำสำคัญ: ภาครัฐดิจิทัล, สิงคโปร์,

Smart Nation 2.0, ความไว้วางใจ

สาธารณะ, การบูรณาการข้อมูล, การ

ถ่ายโอนนโยบาย

บทคัดย่อ

สิงคโปร์อยู่ในอันดับที่สามของโลกในดัชนีรัฐบาลอิเล็กทรอนิกส์ขององค์การสหประชาชาติ ปี ค.ศ. 2024 และมักถูกนำเสนอในวงวิชาการไทยในฐานะต้นแบบของภาครัฐดิจิทัลแบบรวมศูนย์ ที่ตั้งอยู่บนหน่วยงานเทคโนโลยีภาครัฐ แผนแม่บทรัฐบาลดิจิทัล และเสาหลักการให้บริการสู่ประชากร บทความวิชาการนี้เสนอว่าคำอธิบายดังกล่าวยังไม่ครบถ้วน เพราะหยุดอยู่ที่สถาปัตยกรรมและละเว้นราคาที่ต้องจ่าย บทความชี้ให้เห็นข้อเท็จจริงที่มีนัยสำคัญแต่ยังถูกวิเคราะห์น้อย กล่าวคือ เมื่อสิงคโปร์ปรับวิสัยทัศน์แห่งชาติใหม่เป็น Smart Nation 2.0 เมื่อวันที่ 1 ตุลาคม ค.ศ. 2024 ได้จัดวางยุทธศาสตร์ไว้บนเป้าหมายสามประการ โดยยก “ความไว้วางใจ” ขึ้นเป็นเป้าหมายแรก นำหน้าการเติบโตและชุมชน ขณะที่กรอบเดิมในปี ค.ศ. 2014 และ ค.ศ. 2018 จัดวางไว้รอบการเปลี่ยนผ่านสู่ดิจิทัล และการปฏิรูปบริการเป็นหลัก โดยใช้การวิเคราะห์เอกสารจากเครื่องมือเชิงนโยบายของสิงคโปร์ รายงานคณะกรรมการสอบสวนและวรรณกรรมร่วมสมัย บทความอ่านการจัดลำดับใหม่นี้ว่าเป็นการยอมรับเชิงนโยบายว่าการบูรณาการข้อมูลเชิงลึก ก่อให้เกิดต้นทุนความไว้วางใจ บทความวิเคราะห์เหตุการณ์สองกรณี ได้แก่ การโจมตีทางไซเบอร์ต่อ SingHealth ในปี ค.ศ. 2018 ซึ่งข้อมูลส่วนบุคคลของผู้ป่วย 1.5 ล้านรายถูกโจรกรรมและนายกรัฐมนตรีถูกมุ่งเป้าโดยเฉพาะ และกรณี TraceTogether ในปี ค.ศ. 2021 ซึ่งรัฐบาลยอมรับความผิดพลาดที่ไม่ได้ระบุข้อมูลดังกล่าวไม่ได้รับยกเว้น จากประมวลกฎหมายวิธีพิจารณาความอาญา และต่อมาได้ออกกฎหมายจำกัดการเข้าถึงของตำรวจไว้เฉพาะความผิดร้ายแรงเจ็ดประเภท จากทั้งสองกรณี บทความพัฒนามโนทัศน์ “เพดานความไว้วางใจ” ซึ่งเสนอว่าระดับความลึกของการบูรณาการข้อมูล ที่รัฐจะรักษาไว้ได้อย่างยั่งยืนถูกจำกัดด้วยระดับความไว้วางใจที่รัฐรักษาไว้ได้ และหลักประกันต้องถูกบัญญัติไว้ล่วงหน้าก่อนที่การบูรณาการจะลึกขึ้น เพราะการแก้ไขย้อนหลังทำได้เพียงกฎเกณฑ์ แต่ซ่อมความไว้วางใจไม่ได้ พร้อมทั้งเสนอแนะต่อประเทศไทยซึ่งมีองค์กรปกครองส่วนท้องถิ่นราว 7,776 แห่ง และไม่มีโครงสร้างชั้นเดียวแบบสิงคโปร์

บทนำ

ในการสำรวจรัฐบาลอิเล็กทรอนิกส์ขององค์การสหประชาชาติ ปี ค.ศ. 2024 สิงคโปร์อยู่ในอันดับที่สามของโลก ด้วยค่าดัชนี 0.96912 และเป็นประเทศเดียวในอาเซียนที่อยู่ในกลุ่มสูงสุด ขณะที่ประเทศไทยอยู่ในอันดับที่ 52 จาก 193 ประเทศ (United Nations Department of Economic and Social Affairs [UN DESA], 2024; สำนักงานพัฒนารัฐบาลดิจิทัล [สพร.], 2568) ระยะห่างนี้ทำให้สิงคโปร์เป็นกรณีศึกษาที่ถูกอ้างถึงมากที่สุดกรณีหนึ่งในวงวิชาการไทย โดยคำอธิบายที่พบทั่วไปมักประกอบด้วยองค์ประกอบสามอย่าง คือ การมีหน่วยงานเทคโนโลยีภาครัฐที่เข้มแข็ง การมีแผนแม่บทรัฐบาลดิจิทัล และการยึดเสาหลักการให้บริการสู่ประชากร

บทความวิชาการนี้เห็นว่าคำอธิบายดังกล่าวถูกต้องแต่ยังไม่ครบถ้วน เพราะหยุดอยู่ที่การบรรยายสถาปัตยกรรมและละเว้นคำถามว่าสถาปัตยกรรมนั้นมีราคาอะไรที่ต้องจ่าย ข้อเท็จจริงที่บทความนี้ถือเป็นจุดตั้งต้นของการวิเคราะห์ คือ เมื่อวันที่ 1 ตุลาคม ค.ศ. 2024 สิงคโปร์ได้ปรับวิสัยทัศน์แห่งชาติใหม่เป็น Smart Nation 2.0 โดยจัดวางยุทธศาสตร์ไว้บนเป้าหมายสามประการ ได้แก่ ความไว้วางใจ (Trust) การเติบโต (Growth) และชุมชน (Community) และยก “ความไว้วางใจ” ขึ้นเป็นเป้าหมายแรก (Ministry of Digital Development and Information [MDDI], 2024) การจัดลำดับเช่นนี้แตกต่างอย่างมีนัยสำคัญจากกรอบเดิมเมื่อปี ค.ศ. 2014 และแผนแม่บทรัฐบาลดิจิทัลปี ค.ศ. 2018 ซึ่งจัดวางไว้รอบการเปลี่ยนผ่านสู่ดิจิทัลและการปฏิรูปบริการเป็นหลัก ภายใต้วิสัยทัศน์ “Digital to the Core, and Serves with Heart” (Smart Nation and Digital Government Office [SNDGO], 2018)

ข้อโต้แย้งหลักของบทความนี้คือ การเลื่อนความไว้วางใจขึ้นมาเป็นเป้าหมายแรกมิใช่การปรับถ้อยคำเชิงประชาสัมพันธ์ หากแต่เป็นการยอมรับเชิงนโยบายว่าการบูรณาการข้อมูลในระดับลึกก่อให้เกิดต้นทุนความไว้วางใจที่สะสมและต้องบริหาร ข้อสังเกตนี้มีฐานจากเหตุการณ์สองกรณีที่เกิดขึ้นระหว่างสองกรอบวิสัยทัศน์ ได้แก่ การโจมตีทางไซเบอร์ต่อระบบของ SingHealth ในปี ค.ศ. 2018 และการเปิดเผยเรื่องการเข้าถึงข้อมูล TraceTogether โดยตำรวจในปี ค.ศ. 2021 ทั้งสองกรณีชี้ว่าคุณสมบัติที่ทำให้ระบบของสิงคโปร์มีประสิทธิภาพสูง คือการรวมศูนย์และการเชื่อมโยงข้อมูลอย่างกว้างขวางเป็นคุณสมบัติเดียวกับที่ทำให้ความเสียหายเมื่อเกิดเหตุมีขนาดใหญ่และกระทบความไว้วางใจในวงกว้าง

บทความนี้มีวัตถุประสงค์ 4 ประการ ได้แก่

- 1) เพื่อวิเคราะห์สถาปัตยกรรมเชิงสถาบันของภาครัฐดิจิทัลสิงคโปร์และเงื่อนไขที่ทำให้ทำงานได้
- 2) เพื่อวิเคราะห์ต้นทุนความไว้วางใจที่เกิดจากการบูรณาการข้อมูลเชิงลึกผ่านกรณีศึกษาสองกรณี
- 3) เพื่อพัฒนาโมเดลที่อธิบายความสัมพันธ์ระหว่างระดับการบูรณาการกับระดับความไว้วางใจ
- 4) เพื่อเสนอแนะและข้อเสนอแนะเชิงนโยบายที่ใช้ได้จริงในบริบทการบริหารราชการของประเทศไทย

ในเชิงระเบียบวิธี บทความใช้การวิเคราะห์เอกสารจากเอกสารนโยบายและแถลงการณ์ทางการของรัฐบาลสิงคโปร์ รายงานของคณะกรรมการสอบสวน สถิติของหน่วยงานระหว่างประเทศ และบทความวิชาการที่ผ่านการประเมินโดยผู้ทรงคุณวุฒิ โดยให้น้ำหนักกับเอกสารที่เผยแพร่ระหว่างปี ค.ศ. 2021-2025 เป็นหลัก และใช้วิธีวิเคราะห์เชิงเวลาเพื่อเชื่อมโยง เหตุการณ์กับการเปลี่ยนแปลงของกรอบนโยบาย

สถาปัตยกรรมเชิงสถาบันของภาครัฐดิจิทัลสิงคโปร์

1. การวางหน่วยขับเคลื่อนไว้ที่ศูนย์กลางอำนาจ

องค์ประกอบแรกที่อธิบายความสำเร็จของสิงคโปร์คือการออกแบบตำแหน่งแห่งที่ขององค์การ สำนักงานเพื่อรัฐอัจฉริยะและรัฐบาลดิจิทัล (Smart Nation and Digital Government Office: SNDGO) ทำหน้าที่ด้านนโยบาย ขณะที่หน่วยงานเทคโนโลยีภาครัฐ (Government Technology Agency: GovTech) ทำหน้าที่ด้านการปฏิบัติ โดยทั้งสองหน่วยงานอยู่ภายใต้การกำกับของสำนักนายกรัฐมนตรี การจัดวางเช่นนี้มีนัยเชิงรัฐประศาสนศาสตร์ที่สำคัญกว่าที่เห็น เพราะ

ทำให้หน่วยขับเคลื่อนมีอำนาจประสานงาน ข้ามกระทรวงโดยไม่ต้องรองในฐานะหน่วยงานระดับเดียวกัน ซึ่งเป็นอุปสรรคที่พบทั่วไปในประเทศที่มอบภารกิจนี้ให้แก่กระทรวงใดกระทรวงหนึ่ง

2. การสร้างสมรรถนะวิศวกรรมไว้ภายในภาครัฐ

องค์ประกอบที่สองคือการเลือกสร้างขีดความสามารถทางวิศวกรรมไว้ภายในองค์กร แทนการจ้างเหมาภายนอกทั้งหมด GovTech วางตำแหน่งตนเองเป็นหน่วยงานวิศวกรรมที่มีนักพัฒนา นักวิทยาศาสตร์ข้อมูล และผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ทำงานประจำ และพัฒนาแพลตฟอร์มกลางของรัฐด้วยตนเอง ทางเลือกเชิงสถาบันนี้มีนัยต่อประเทศที่พึ่งพาการจัดซื้อจัดจ้างเป็นหลัก เพราะหน่วยงานที่ไม่มีสมรรถนะทางเทคนิคภายใน จะไม่สามารถกำหนดความต้องการ ตรวจจับ หรือปรับปรุงระบบได้อย่างเท่าทันผู้รับจ้าง และมักลงเอยด้วยระบบที่แยกส่วน ตามสัญญาแต่ละฉบับ

3. การสร้างโครงสร้างพื้นฐานดิจิทัลกลางเป็นพันธะ มิใช่ทางเลือก

องค์ประกอบที่สามคือการสร้างชั้นโครงสร้างพื้นฐานดิจิทัลกลางที่หน่วยงานทั้งระบบต้องใช้ร่วมกัน ประกอบด้วยระบบยืนยันตัวตนกลาง ระบบข้อมูลบุคคลที่ดึงมารองรับให้อัตโนมัติเพื่อลดการยื่นข้อมูลซ้ำ และชุดเทคโนโลยีกลางของรัฐที่หน่วยงานใช้เครื่องมือและบริการร่วมกัน ประเด็นสำคัญมิได้อยู่ที่การมีระบบเหล่านี้ แต่อยู่ที่การกำหนดให้เป็นทางเลือกแรกหรือเป็นพันธะของหน่วยงาน จึงเกิดการประหยัดต่อขนาดและความสอดคล้องของประสบการณ์ผู้ใช้ มาตรฐานบริการดิจิทัล และแนวทางการจัดทำแผนดิจิทัลระดับกระทรวงทำหน้าที่เป็นกลไกกำกับให้บริการที่พัฒนาขึ้นทั่วทั้งระบบ มีคุณภาพและรูปแบบที่สอดคล้องกัน โดยเน้นการออกแบบที่ใช้งานง่าย การเข้าถึงได้ของผู้ใช้ทุกกลุ่ม และความสม่ำเสมอ

4. เสาหลักการให้บริการสู่ประชากร

ในระดับการออกแบบบริการ สิงคโปร์ใช้กรอบสี่ด้านเป็นเข็มทิศ ได้แก่ การให้บริการที่ยึดประชาชนเป็นศูนย์กลาง ซึ่งออกแบบตามช่วงชีวิตของประชาชนแทนการออกแบบตามโครงสร้างหน่วยงาน การให้บริการที่เอื้อต่อภาคธุรกิจ ซึ่งมุ่งลดภาระด้านกฎระเบียบและเพิ่มความคาดการณ์ได้ของกระบวนการ การมีส่วนร่วมของชุมชนและภาคส่วนต่าง ๆ และความเป็นเลิศในการดำเนินงานภายในซึ่งเป็นฐานรองรับสามด้านแรก กรอบนี้สอดคล้องกับแนวคิดการอภิบาลสาธารณะแนวใหม่ ที่มองว่าผลลัพธ์สาธารณะเกิดจากการร่วมผลิระหว่างรัฐกับผู้มีส่วนได้ส่วนเสีย (Osborne, 2010) และกับข้อเสนอว่าคุณค่าสาธารณะของรัฐบาลอิเล็กทรอนิกส์มีหลายมิติที่ต้องประเมินร่วมกัน (Twizeyimana & Andersson, 2019)

สรุปหัวข้อที่ 1

สถาปัตยกรรมของสิงคโปร์ประกอบด้วย การวางหน่วยขับเคลื่อนไว้ที่ศูนย์กลางอำนาจ การสร้างสมรรถนะวิศวกรรมไว้ภายในรัฐ การกำหนดให้โครงสร้างพื้นฐานกลางเป็นพันธะ และการมีกรอบออกแบบบริการที่ชัดเจน องค์ประกอบทั้งสี่อธิบายประสิทธิภาพได้ดี แต่ยังไม่อธิบายว่าเหตุใดสิงคโปร์จึงต้องยกความไว้วางใจขึ้นเป็นเป้าหมายแรก ในกรอบวิสัยทัศน์ล่าสุด ซึ่งเป็นคำถามของหัวข้อถัดไป

ต้นทุนความไว้วางใจของการบูรณาการข้อมูลเชิงลึก

1. กรณีที่หนึ่ง การโจมตีระบบข้อมูลสุขภาพ ค.ศ. 2018

ระหว่างวันที่ 27 มิถุนายนถึง 4 กรกฎาคม ค.ศ. 2018 ระบบฐานข้อมูลผู้ป่วยของ SingHealth ซึ่งเป็นเครือข่ายบริการสุขภาพที่ใหญ่ที่สุดของสิงคโปร์ ถูกโจมตีและมีการเข้าถึงและคัดลอกข้อมูลส่วนบุคคล ของผู้ป่วย 1.5 ล้านราย รวมทั้งข้อมูลการจ่ายยาผู้ป่วยนอกของผู้ป่วยอีก 160,000 ราย โดยมีการมุ่งเป้าไปที่ข้อมูลของนายกรัฐมนตรีเป็นการเฉพาะและซ้ำหลายครั้ง คณะกรรมการสอบสวนที่ตั้งขึ้นในเวลาต่อมา สรุปว่าการโจมตีเป็นการกระทำที่วางแผนมาอย่างดี และชี้ว่าเหตุการณ์อาจถูกยับยั้งได้หากมาตรการด้านความมั่นคงปลอดภัย การฝึกอบรมบุคลากร และการแก้ไขช่องโหว่ดำเนินไปอย่างเหมาะสม (Committee of Inquiry, 2019)

สิ่งที่มินยัเชิงรัฐประศาสนศาสตร์มิใช่ตัวเหตุการณ์ แต่คือความสัมพันธ์ระหว่างขนาดความเสียหายกับระดับการรวมศูนย์ จำนวนผู้ได้รับผลกระทบคิดเป็นสัดส่วนราวหนึ่งในสี่ของประชากรทั้งประเทศในคราวเดียว ซึ่งเป็นไปได้ก็เพราะข้อมูลถูกรวมไว้ ในระบบเดียวเพื่อประโยชน์ด้านประสิทธิภาพ ข้อสังเกตนี้สอดคล้องกับข้อเสนอในวรรณกรรมว่าเมื่อระบบดิจิทัลกลายเป็น โครงสร้างพื้นฐานที่สังคมพึ่งพาถึงระดับหนึ่ง การบริหารความเสี่ยงจะเปลี่ยนลักษณะไปโดยสิ้นเชิง เพราะทางเลือกในการหยุดระบบเพื่อความปลอดภัยแทบไม่มีอยู่จริง (Skierka, 2023)

2. กรณีที่สอง การเข้าถึงข้อมูลติดตามสัมผัส ค.ศ. 2021

ในเดือนมกราคม ค.ศ. 2021 มีการยืนยันในรัฐสภาว่าตำรวจสามารถเข้าถึงข้อมูลจากระบบติดตามสัมผัส TraceTogether ได้ตามมาตรา 20 แห่งประมวลกฎหมายวิธีพิจารณาความอาญา ทั้งที่เมื่อเริ่มโครงการมีการสื่อสารว่าข้อมูลจะถูกใช้ เพื่อการติดตามผู้สัมผัสโรคเท่านั้น ต่อมารัฐมนตรีผู้รับผิดชอบได้ชี้แจงต่อรัฐสภาและหน่วยงานที่เกี่ยวข้อง ได้ยอมรับความผิดพลาดที่มีได้ระบุตั้งแต่ต้นว่าข้อมูลดังกล่าวไม่ได้รับยกเว้นจากประมวลกฎหมายวิธีพิจารณาความอาญา (Balakrishnan, 2021) หลังจากนั้นรัฐสภาได้ออกกฎหมายจำกัดการเข้าถึงข้อมูลดังกล่าวโดยเจ้าหน้าที่ตำรวจ ไว้เฉพาะความผิดร้ายแรงเจ็ดประเภท

กรณีนี้มีคุณค่าเชิงวิเคราะห์สูงกว่ากรณีแรก เพราะมิใช่ความล้มเหลวทางเทคนิค แต่เป็นความล้มเหลวของการออกแบบ หลักประกันเชิงสถาบัน กล่าวคือ รัฐได้สร้างความไว้วางใจด้วยคำสัญญาเชิงนโยบายซึ่งไม่มีสถานะทางกฎหมายรองรับ และเมื่อคำสัญญานั้นขัดกับกฎหมายที่มีอยู่เดิม ความไว้วางใจจึงเสียหายแม้ในภายหลังจะมีการออกกฎหมายแก้ไข บทเรียนที่ตามมาคือ ลำดับเวลามีความสำคัญ หลักประกันที่ออกภายหลังสามารถซ่อมกฎหมายได้ แต่ไม่สามารถซ่อมความรู้สึกของประชาชนที่พบว่าคำรับรองก่อนหน้านี้ไม่เป็นความจริง

3. การจัดลำดับใหม่ในปี ค.ศ. 2024

เมื่อพิจารณาสองกรณีข้างต้นร่วมกับการปรับวิสัยทัศน์เป็น Smart Nation 2.0 ในปี ค.ศ. 2024 ซึ่งยกความไว้วางใจขึ้นเป็นเป้าหมายแรกและระบุแนวทางย่อยที่มุ่งเสริมความมั่นคงและความยืดหยุ่นของโครงสร้างพื้นฐานดิจิทัล การรับมือภัยออนไลน์ และการดูแลผู้ใช้ (MDDI, 2024) จะเห็นเส้นทางที่ต่อเนื่องกัน สิงคโปร์มิได้ลดระดับการบูรณาการลง แต่เปลี่ยนลำดับความสำคัญของเป้าหมาย จากการเร่งความเป็นดิจิทัลเป็นการรักษาเงื่อนไขที่ทำให้ความเป็นดิจิทัลดำรงอยู่ได้ ตารางที่ 1 สรุปลำดับเหตุการณ์และการเปลี่ยนแปลงกรอบนโยบายภาครัฐดิจิทัลของสิงคโปร์

ตารางที่ 1 ลำดับเหตุการณ์และการเปลี่ยนแปลงกรอบนโยบายภาครัฐดิจิทัลของสิงคโปร์

ปี ค.ศ.	เหตุการณ์หรือกรอบนโยบาย	นัยต่อความสัมพันธ์ระหว่างรัฐกับประชาชน
2014	ประกาศวิสัยทัศน์ Smart Nation	เน้นการใช้เทคโนโลยียกระดับคุณภาพชีวิตและขีดความสามารถของประเทศ
2018	แผนแม่บทรัฐบาลดิจิทัล วิสัยทัศน์ Digital to the Core, and Serves with Heart	เน้นการแปลงบริการเป็นดิจิทัลแบบเบ็ดเสร็จและการบูรณาการข้ามหน่วยงาน
2018	การโจมตีระบบข้อมูลผู้ป่วย SingHealth ข้อมูล 1.5 ล้านราย	เปิดเผยว่าการรวมศูนย์ขยายขนาดความเสียหายเมื่อเกิดเหตุ
2021	การยืนยันว่าตำรวจเข้าถึงข้อมูล TraceTogether ได้และการออกกฎหมายจำกัดในภายหลัง	เปิดเผยว่าคำสัญญาเชิงนโยบายที่ไม่มีกฎหมายรองรับไม่อาจสร้างความไว้วางใจได้
2024	Smart Nation 2.0 เป้าหมาย Trust, Growth, Community	ยกความไว้วางใจขึ้นเป็นเป้าหมายแรกของยุทธศาสตร์แห่งชาติ

ที่มา: ผู้เขียนสังเคราะห์จาก SNDGO (2018); Committee of Inquiry (2019); Balakrishnan (2021); MDDI (2024)

สรุปหัวข้อที่ 2

การบูรณาการข้อมูลเชิงลึกให้ประสิทธิภาพที่วัดได้ แต่ก็สร้างต้นทุนความไว้วางใจสองประเภทพร้อมกัน ประเภทแรกคือความเสี่ยงเชิงระบบที่ทำให้ความเสียหายเมื่อเกิดเหตุมีขนาดใหญ่ผิดปกติ ประเภทที่สองคือความเสี่ยงเชิงสถาบันที่เกิดเมื่อขอบเขตการใช้ข้อมูลกว้างกว่าที่ประชาชนเข้าใจ การที่สิงคโปร์ยกความไว้วางใจขึ้นเป็นเป้าหมายแรกในปี ค.ศ. 2024 จึงอ่านได้ว่าเป็นการยอมรับต้นทุนทั้งสองประเภทนี้

นัยต่อประเทศไทยและเงื่อนไขที่ถ่ายโอนไม่ได้

1. เงื่อนไขตั้งต้นที่แตกต่างอย่างมีนัยสำคัญ

ความแตกต่างที่สำคัญที่สุดระหว่างสองประเทศมีเชิงปริมาณหรือเทคโนโลยี แต่คือโครงสร้างการปกครอง สิงคโปร์เป็นนครรัฐที่ไม่มีราชการส่วนท้องถิ่นเป็นชั้นแยกต่างหาก การกำหนดให้ใช้แพลตฟอร์มกลางจึงเป็นคำสั่งเดียว ที่มีผลทั่วทั้งระบบ ขณะที่ประเทศไทยมีองค์กรปกครองส่วนท้องถิ่นราว 7,776 แห่ง ซึ่งมีความเป็นอิสระตามกฎหมาย มีสภาท้องถิ่นของตนเอง และมีความแตกต่างด้านสมรรถนะอย่างมาก การผลักดันมาตรฐานกลางในบริบทไทยจึงเป็น งานเจรจาเชิงสถาบันมากกว่างานสั่งการ และช่องว่างระหว่างระดับชาติกับระดับท้องถิ่นเป็นปัญหาที่ปรากฏชัด ในระดับปฏิบัติ (ไพลิน สังครุท, 2569)

ความแตกต่างประการที่สองคือขนาดและความเป็นเนื้อเดียวของประชากร ซึ่งทำให้การออกแบบบริการเดียวสำหรับทั้งประเทศ เป็นไปได้ในสิงคโปร์ แต่ยากกว่ามากในไทยที่มีความหลากหลายทางพื้นที่และทักษะดิจิทัล วรรณกรรมที่ทบทวนกรณีต้นแบบ ด้านรัฐดิจิทัลจึงสรุปตรงกันว่าแนวปฏิบัติไม่อาจถ่ายโอนข้ามบริบททางสังคมวัฒนธรรมได้อย่างตรงไปตรงมา สิ่งที่ถ่ายโอนได้คือหลักการและลำดับความสำคัญ (Himma-Kadakas & Köuts-Klemm, 2023)

2. สิ่งที่ประเทศไทยถอดมาให้ได้

แม้เงื่อนไขตั้งต้นจะต่างกัน แต่หลักการสามประการยังถ่ายโอนได้ ประการแรก การสร้างสมรรถนะทางเทคนิคไว้ในภาครัฐ อย่างน้อยในระดับที่เพียงพอต่อการกำหนดความต้องการและตรวจรับงาน ซึ่งเป็นเงื่อนไขของการกำกับผู้รับจ้างอย่างเท่าทัน ประการที่สอง การกำหนดให้แพลตฟอร์มกลางเป็นทางเลือกแรกสำหรับหน่วยงานที่ยังไม่มีระบบของตนเอง ซึ่งเปลี่ยนต้นทุนการพัฒนาาระบบเป็นต้นทุนการเชื่อมต่อและเหมาะกับหน่วยงานขนาดเล็กเป็นพิเศษ และประการที่สาม การบัญญัติหลักประกันการใช้ข้อมูลไว้ล่วงหน้าก่อนที่การบูรณาการจะลึกขึ้น ซึ่งเป็นบทเรียนโดยตรงจากกรณี TraceTogether

ในบริบทไทย ฐานทางกฎหมายที่จำเป็นมีอยู่แล้วบางส่วน โดยพระราชบัญญัติการปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. 2565 ได้กำหนดให้การติดต่อราชการทางอิเล็กทรอนิกส์มีผลตามกฎหมาย และห้ามปฏิเสธการรับเรื่องด้วยเหตุผลเชิงรูปแบบ (สำนักงานคณะกรรมการกฤษฎีกา, 2565) ขณะที่แผนพัฒนารัฐบาลดิจิทัลของประเทศไทย พ.ศ. 2566-2570 ได้วางเป้าหมายไว้แล้ว (สำนักงานพัฒนารัฐบาลดิจิทัล [สพร.], 2566) สิ่งที่ยังต้องเสริมคือมิติความไว้วางใจ ซึ่งงานที่ศึกษาความเชื่อมั่นของประชาชนต่อหน่วยงานรัฐไทยชี้ว่าเป็นตัวแปรที่ต้องบริหารอย่างจริงจัง (พัทธนันท์ โรจนไพรัชส์, 2569) และการเสริมสร้างความโปร่งใสในระดับปฏิบัติเป็นกลไกสำคัญของการรักษาความไว้วางใจนั้น (สัญญาศรณ์ สวัสดิ์ไธสง และอภิชัย บัวละพา, 2569)

ตารางที่ 2 การจำแนกบทเรียนจากสิงคโปร์ตามระดับความสามารถในการถ่ายโอนสู่บริบทไทย

องค์ประกอบ	ระดับการถ่ายโอน	ข้อเสนอสำหรับประเทศไทย
การวางหน่วยขับเคลื่อนไว้ที่ศูนย์กลางอำนาจ	ถ่ายโอนได้บางส่วน เพราะไทยมีหลายกระทรวงที่เกี่ยวข้องและ มีท้องถิ่นที่เป็นอิสระ	ให้อำนาจประสานงานข้ามกระทรวงที่มีฐานทางกฎหมาย พร้อมกลไกเจรจากับท้องถิ่น
สมรรถนะวิศวกรรมภายในภาครัฐ	ถ่ายโอนได้ เพราะไม่ขึ้นกับขนาดประเทศ	สร้างทีมเทคนิคกลางที่เพียงพอต่อการกำหนด ความต้องการและตรวจรับงาน
แพลตฟอร์มกลางเป็นทางเลือกแรก	ถ่ายโอนได้ และมีประโยชน์สูงกับอปท. ขนาดเล็กเป็นพิเศษ	กำหนดให้หน่วยงานที่ยังไม่มีระบบของตนเอง ใช้แพลตฟอร์มกลางก่อนพัฒนาระบบใหม่
การบัญญัติหลักประกันการใช้ข้อมูลล่วงหน้า	ถ่ายโอนได้ และเป็นบทเรียนที่มีต้นทุนต่ำที่สุดในการนำมาใช้	ระบุขอบเขตการใช้ข้อมูลและข้อยกเว้นไว้ในกฎหมายก่อนเปิดการเชื่อมโยงข้อมูลใหม่
โครงสร้างการปกครอง ชั้นเดียว	ถ่ายโอนไม่ได้ เพราะเป็นเงื่อนไขตั้งต้นของนครรัฐ	ออกแบบมาตรการเฉพาะสำหรับช่องว่างระหว่างระดับชาติกับระดับท้องถิ่นแทน

ที่มา: ผู้เขียนสังเคราะห์

สรุปหัวข้อที่ 3

บทเรียนจากสิงคโปร์ที่ถ่ายโอนได้ดีที่สุดคือสิ่งที่ไม่ขึ้นกับขนาดของประเทศ ได้แก่ สมรรถนะทางเทคนิคภายในภาครัฐ การกำหนดให้แพลตฟอร์มกลางเป็นทางเลือกแรก และการบัญญัติหลักประกันการใช้ข้อมูลไว้ล่วงหน้า ส่วนสิ่งที่ถ่ายโอนไม่ได้คือโครงสร้างการปกครองชั้นเดียว ซึ่งหมายความว่าประเทศไทยต้องออกแบบกลไกเฉพาะ สำหรับการทำงานร่วมกับองค์กรปกครองส่วนท้องถิ่น แทนการคาดหวังว่าคำสั่งจากส่วนกลางจะมีผลโดยอัตโนมัติ

องค์ความรู้ใหม่

บทความนี้เสนอมนทัศน์ “เพดานความไว้วางใจ” (trust ceiling) เป็นองค์ความรู้ใหม่ สารของมนทัศน์นี้คือระดับความลึกของการบูรณาการข้อมูลที่รัฐจะรักษาไว้ได้อย่างยั่งยืน มิได้ถูกกำหนดโดยขีดความสามารถ ทางเทคโนโลยีหรืองบประมาณเป็นด้านหลัก หากแต่ถูกจำกัดด้วยระดับความไว้วางใจที่รัฐสามารถรักษาไว้ได้ เมื่อการบูรณาการเดินหน้าไปเกินเพดานดังกล่าว ระบบจะยังทำงานได้ในเชิงเทคนิค แต่จะเริ่มสะสมความเปราะบางเชิงสถาบัน ซึ่งปรากฏออกมาเมื่อเกิดเหตุการณ์กระตุก ไม่ว่าจะเป็นการรั่วไหลของข้อมูลหรือการเปิดเผยว่าขอบเขตการใช้ข้อมูล กว้างกว่าที่ประชาชนเข้าใจ มนทัศน์นี้นำไปสู่หลักการปฏิบัติที่บทความเรียกว่า “หลักการรับประกันล่วงหน้า” ซึ่งเสนอว่าหลักประกันเกี่ยวกับขอบเขตการใช้ข้อมูล ผู้มีสิทธิเข้าถึง และข้อยกเว้นตามกฎหมาย ต้องถูกบัญญัติให้ชัดเจนก่อนที่การบูรณาการจะลึกขึ้น มิใช่ออกตามหลังเมื่อเกิดข้อกังขา เหตุผลอยู่ที่ความไม่สมมาตรระหว่างการซ่อมกฎเกณฑ์กับการซ่อมความไว้วางใจ กล่าวคือ กฎเกณฑ์แก้ไขได้ในเวลาไม่นาน ดังที่ปรากฏในกรณี TraceTogether ที่มีการออกกฎหมายจำกัดการเข้าถึงในเวลาต่อมา แต่ความไว้วางใจที่เสียไปจากการพบว่าคำรับรองก่อนหน้านี้ไม่ครบถ้วน ต้องใช้เวลานานกว่ามากในการฟื้นคืน และในบางกรณีอาจไม่ฟื้นกลับสู่ระดับเดิม

คุณูปการเชิงวิเคราะห์ของมนทัศน์นี้อยู่ที่การเปลี่ยนวิธีตั้งคำถามเชิงนโยบาย จากคำถามว่า “เราสามารถเชื่อมโยงข้อมูลได้ลึกเพียงใด” เป็นคำถามว่า “เรามีหลักประกันที่ผูกพันตามกฎหมายรองรับ การเชื่อมโยงในระดับนั้นแล้วหรือยัง” ข้อเสนอแนะนี้สามารถแปลงเป็นสมมติฐานที่ทดสอบได้ว่า โครงการบูรณาการข้อมูลที่มีบัญญัติขอบเขตและข้อยกเว้นไว้ล่วงหน้า จะ

มีอัตราการยอมรับของประชาชนสูงกว่า และมีความต่อเนื่องของนโยบายมากกว่าโครงการที่อาศัยการรับรองเชิงนโยบายเพียงอย่างเดียว เมื่อควบคุมประโยชน์ที่ผู้ใช้ได้รับไว้แล้ว ซึ่งเป็นวาระวิจัยเชิงประจักษ์ที่ควรดำเนินการต่อไปในบริบทไทย

บทสรุป

บทความวิชาการนี้ทบทวนกรณีภาครัฐดิจิทัลของสิงคโปร์ โดยเสนอว่าคำอธิบายที่แพร่หลายซึ่งเน้นหน่วยงานเทคโนโลยีภาครัฐ แผนแม่บท และเสาหลักการให้บริการสู่ประชากร อธิบายประสิทธิภาพได้ดีแต่ยังไม่อธิบายราคาที่ต้องจ่าย บทความจึงหันไปวิเคราะห์ข้อเท็จจริงที่ว่าสิงคโปร์ยกความไว้วางใจขึ้นเป็นเป้าหมายแรกของ Smart Nation 2.0 ในปี ค.ศ. 2024 และอ่านการจัดลำดับใหม่นี้เป็นการยอมรับเชิงนโยบายว่าการบูรณาการข้อมูลเชิงลึกสร้างต้นทุนความไว้วางใจ

หลักฐานสนับสนุนมาจากสองกรณี ได้แก่ การโจมตีระบบข้อมูลผู้ป่วยในปี ค.ศ. 2018 ซึ่งแสดงว่าการรวมศูนย์ขยายขนาด ความเสียหายเมื่อเกิดเหตุ และกรณีการเข้าถึงข้อมูลติดตามสัมผัสในปี ค.ศ. 2021 ซึ่งแสดงว่าคำสัญญาเชิงนโยบาย ที่ไม่มีกฎหมายรองรับไม่อาจแก้ความไว้วางใจได้ บทความจึงเสนอโมทัศน์เพดานความไว้วางใจและหลักการรับประกันล่วงหน้าเป็นองค์ความรู้ใหม่

สำหรับประเทศไทย ข้อเสนอแนะเชิงนโยบายมีสี่ประการ คือ สร้างสมรรถนะทางเทคนิคไว้ภายในภาครัฐให้เพียงพอต่อการกำหนดความต้องการและตรวจรับงาน กำหนดให้แพลตฟอร์มดิจิทัลกลางเป็นทางเลือกแรกสำหรับหน่วยงาน ที่ยังไม่มีระบบของตนเองซึ่งจะเป็นประโยชน์ต่อองค์กรปกครองส่วนท้องถิ่นขนาดเล็กเป็นพิเศษ บัญญัติขอบเขตการใช้ข้อมูลและขอยกเว้นให้ชัดเจนก่อนเปิดการเชื่อมโยงข้อมูลชุดใหม่ และออกแบบกลไกเฉพาะสำหรับการทำงานร่วมกับท้องถิ่น แทนการคาดหวังว่าคำสั่งจากส่วนกลางจะมีผลโดยอัตโนมัติ เพราะประเทศไทยไม่มีโครงสร้างการปกครองชั้นเดียวแบบสิงคโปร์

ข้อจำกัดของบทความนี้คือการอาศัยการวิเคราะห์เอกสารเป็นหลัก จึงยังไม่ได้วัดระดับความไว้วางใจของประชาชนไทย ต่อการเชื่อมโยงข้อมูลภาครัฐด้วยข้อมูลปฐมภูมิ งานวิจัยในระยะต่อไปควรสำรวจว่าประชาชนไทยยอมรับการเชื่อมโยงข้อมูล ในระดับใด และหลักประกันแบบใดที่มีผลต่อการยอมรับมากที่สุด ข้อเสนอโดยรวมของบทความนี้คือ ความสำเร็จของภาครัฐดิจิทัลมิได้วัดจากความลึกของการเชื่อมโยงข้อมูลเพียงอย่างเดียว แต่วัดจากความสามารถของรัฐในการรักษาความไว้วางใจไว้ให้ทันกับความลึกล้ำนั้น

เอกสารอ้างอิง

พัทธนันท์ โรจนไพรัชส์. (2569). ความเชื่อมั่นของประชาชนที่มีต่อสำนักงานตำรวจแห่งชาติ. *วิทยาการบริหารภาครัฐสมัยใหม่*, 3(3), 295-309.

ไพลิน สังครุท. (2569). ประสิทธิภาพของการให้บริการผ่านช่องทางอิเล็กทรอนิกส์ขององค์กรปกครองส่วนท้องถิ่น. *วิทยาการบริหารภาครัฐสมัยใหม่*, 3(3), 327-339.

รัชนิกร ผาวันษ์, จิรภา มาตราข, วรณัฐ ไชยพรม และจิตติยา พรใส. (2567). ภาครัฐยุคใหม่: การวิเคราะห์ข้อดี ข้อจำกัด และแนวทางการปรับใช้. *วารสารการบริหาร การจัดการ และการพัฒนาที่ยั่งยืน*, 2(3), 591-597. เข้าถึงจาก <https://so15.tci-thaijo.org/index.php/jamsd/article/view/475>

สัญญาศรณ์ สวัสดิ์โสสง. (2569). การปฏิรูปการบริหารราชการไทยสู่ความทันสมัยและความเป็นสากลด้วยรัฐบาลดิจิทัล. *วิทยาการบริหารภาครัฐสมัยใหม่*, 3(3), 310-326.

สัญญาศรณ์ สวัสดิ์โสสง และอภิชัย บัวละพา. (2569). การเสริมสร้างความโปร่งใสในการดำเนินงานขององค์กร ปกครองส่วนท้องถิ่นไทย. *วิทยาการบริหารภาครัฐสมัยใหม่*, 3(3), 340-354.

- สำนักงานคณะกรรมการกฤษฎีกา. (2565). *พระราชบัญญัติการปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. 2565*. ประกาศในราชกิจจานุเบกษา เมื่อวันที่ 12 ตุลาคม 2565 และมีผลใช้บังคับครบทุกมาตราตั้งแต่วันที่ 10 มกราคม 2566.
- สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน). (2566). *แผนพัฒนารัฐบาลดิจิทัลของประเทศไทย พ.ศ. 2566-2570*. กรุงเทพฯ: สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน). เข้าถึงจาก <https://www.dga.or.th/policy-standard/policy-regulation/dga-019/dga-027/dg-plan-2566-2570/>
- สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน). (2568). *ผลการจัดอันดับดัชนีรัฐบาลอิเล็กทรอนิกส์ของประเทศไทย ปี ค.ศ. 2024*. เข้าถึงจาก <https://www.dga.or.th/en/document-sharing/en-dga-news/118668/>
- Balakrishnan, V. (2021). *Clarification on the usage of TraceTogether data* [Ministerial statement, 5 January 2021]. Singapore: Ministry of Digital Development and Information. <https://www.mddi.gov.sg/newsroom/20210105/>
- Committee of Inquiry into the Cyber Attack on Singapore Health Services Private Limited's Patient Database. (2019). *Public report of the Committee of Inquiry*. Singapore: Ministry of Communications and Information.
- Himma-Kadakas, M., & Kõuts-Klemm, R. (2023). Developing an advanced digital society: An Estonian case study. In S. Davydov (Ed.), *Internet in the post-Soviet area* (pp. 109-133). Cham: Springer. https://doi.org/10.1007/978-3-031-32507-6_6
- Ministry of Digital Development and Information. (2024). *Launch of Smart Nation 2.0* [Press release, 1 October 2024]. Singapore: MDDI. <https://www.mddi.gov.sg/newsroom/smart-nation-2-press-release/>
- OECD. (2014). *Recommendation of the Council on digital government strategies*. Paris: OECD Publishing.
- Osborne, S. P. (Ed.). (2010). *The new public governance? Emerging perspectives on the theory and practice of public governance*. London: Routledge.
- Skierka, I. (2023). When shutdown is no option: Identifying the notion of the digital government continuity paradox in Estonia's eID crisis. *Government Information Quarterly*, 40(1), 101781. <https://doi.org/10.1016/j.giq.2022.101781>
- Smart Nation and Digital Government Office. (2018). *Digital Government Blueprint*. Singapore: Prime Minister's Office.
- Twizeyimana, J. D., & Andersson, A. (2019). The public value of e-government: A literature review. *Government Information Quarterly*, 36(2), 167-178. <https://doi.org/10.1016/j.giq.2019.01.001>
- United Nations Department of Economic and Social Affairs. (2024). *United Nations e-government survey 2024: Accelerating digital transformation for sustainable development*. New York: United Nations. <https://desapublications.un.org>