

The Digital State Paradox: Cybersecurity, Personal Data Protection, and Public Trust in Thailand's Digital Government

Sipim Sornbanlang

Srinakharinwirot University, Bangkok, Thailand

Abstract

This article reviews concepts, theories, policies, legal frameworks, and empirical studies concerning Thailand's digital government policy and its response to cybersecurity threats, synthesizing scholarly works published between 2021 and 2026 across multiple disciplines, including political science, public administration, law, and computer science.

Three key findings emerge from the synthesis.

First, Thailand's transition toward digital government—from the IT2000 policy to the Digital Government Development Plan 2023–2027—has significantly expanded the cyber attack surface of the public sector, particularly affecting educational and public health agencies.

Second, Thailand has achieved substantial institutional and legal progress since 2019 with the enactment of the Cybersecurity Act, the Digital Government Administration Act, and the Personal Data Protection Act. However, a structural content analysis of the National Cybersecurity Policy and Action Plan (2022–2027) reveals a fragmented governance arrangement: the National Cybersecurity Agency (NCSA) is designated as the lead agency in nearly all 34 projects, while the Digital Government Development Agency (DGA) plays only a supporting role. Moreover, personal data protection appears in merely 1 of 10 strategies and 1 of 34 projects, reflecting a national security-centric approach that potentially undermines citizens' privacy rights.

Third, public trust and personnel cybersecurity awareness are equally critical determinants of digital government success as technical measures.

The article proposes an integrated analytical framework comprising three dimensions—policy and institutional arrangements, risk management based on the people-process-technology framework, and public trust and participation—while identifying research gaps that warrant empirical investigation using mixed-methods approaches.

Keywords

Digital government, cybersecurity, public policy, personal data protection, new public management.