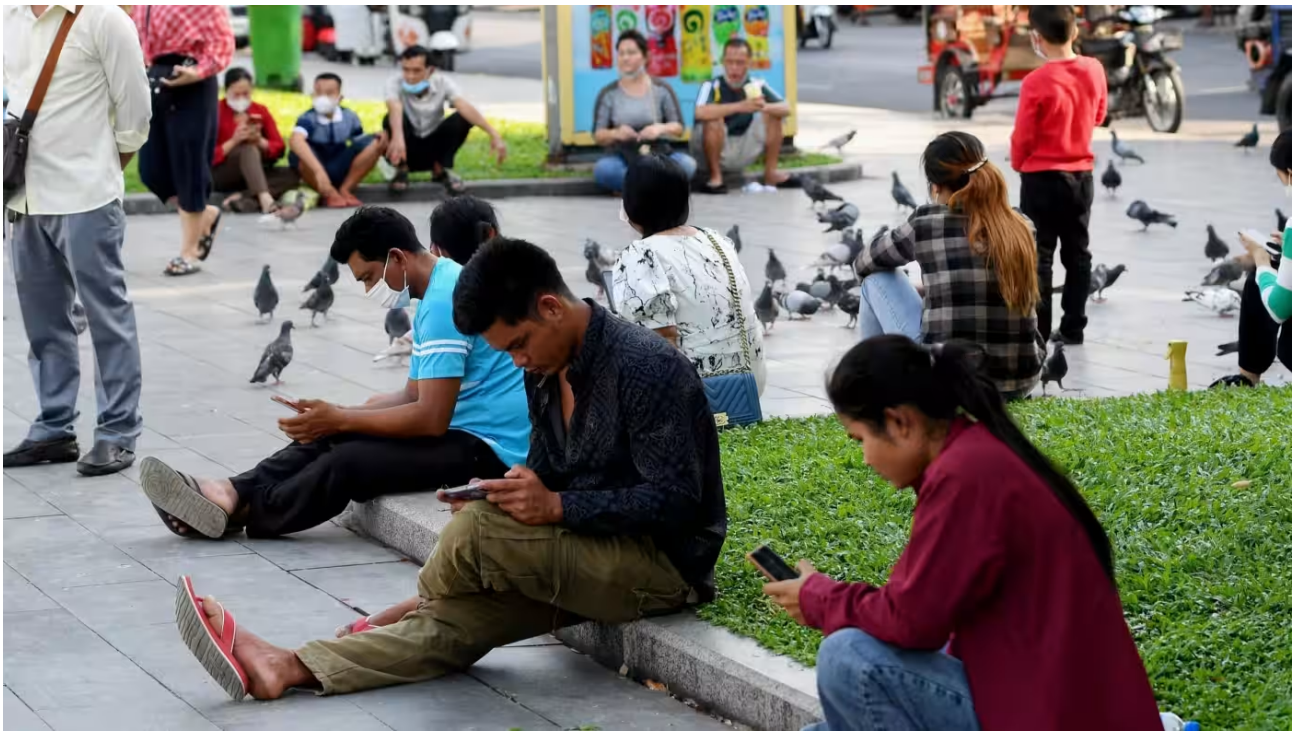
POLITICS

Cambodia's draft data protection law fans fears of government abuse

Leaked legislation says personal data could be exposed in the 'national interest'



People using their smartphones in a Phnom Penh park. Cambodia follows other Southeast Asian nations that have rolled out data protection laws. © AFP/Jiji

FIONA KELLIHER, Contributing writer
December 8, 2023 11:28 JST

PHNOM PENH -- Cambodia is poised to become the next Southeast Asian nation to roll out a personal data protection law, but experts warn it could leave internet users and tech companies vulnerable to the whims of an authoritarian government.

The draft proposal, obtained by Nikkei Asia, marks Cambodia's latest controversial internet law and has surfaced in the wake of alleged cyberattacks that highlight the country's susceptibility to outside surveillance.

Data protection laws have become increasingly prevalent in the last decade, especially after the European Union's General Data Protection Regulation (GDPR) became effective in 2018 and influenced some governments to examine their own data practices.

In order to handle EU data, controllers in other countries must provide safeguards at a comparable level to Europe. Cambodia would be the seventh Southeast Asian nation to implement such legislation, after Singapore, the Philippines, Malaysia, Thailand, Indonesia and Vietnam.

The July 25 draft by the Ministry of Posts and Telecommunications (MPTC) said the law would apply to all private entities that collect and use personal data, but not public authorities.

It was not clear when the ministry would bring it to Parliament. The agency did not respond to a request for comment.

Although the proposal lays out personal data rights in line with international law, lawyers who reviewed the text said its requirement for local data storage and vague language could give companies and the government broad leeway to access or share information without consent.

"The risk is actually that it puts people's data in an even more vulnerable situation, while also restricting their rights to control their data," said Golda Benjamin, Asia-Pacific campaigner at the international digital rights group Access Now. "So personal data is out there, but the safeguards are not in place."

The draft would require any data controller, including multinational companies, to keep user data within Cambodia "in its own personal data storage system or a data center or a secure cloud system of a third party licensed by MPTC."

That clause would give "a loophole, or back door, to government authorities to access private data without a need for a warrant or other judicial oversight," said Zach Lampell, a senior legal adviser at the International Center for Not-for-Profit Law. "What data localization provisions really do is enable authorities to go to that data collector or controller and say, 'Give us the data, or get out of the country.'"

Cambodian leader Hun Manet attends the opening ceremony of a new airport in Siem Reap on Nov. 16. His father, Hun Sen, ruled the country for decades. © Reuters

Tech companies have balked at the localization clause because of the costs associated with managing data centers, as well as security risks. The law would also restrict data transfers to countries outside of Cambodia.

The Asia Internet Coalition, which represents tech giants such as Google, Apple and Meta, warned in an October letter to the ministry that "the economic consequences of data localization mandates are severe" and the legislation would "impact many personal data processors and may lead them to limit their services in Cambodia."

"Enabling cross-border data transfers protects consumers by allowing businesses to implement best practices for data privacy and security, such as decentralized cloud data storage solutions and shared systems that are resilient to outages from malfunctions or natural disasters, and unauthorized access by third parties," the coalition said.

Cambodia has shown itself to be at risk for cyberattacks. An American cybersecurity firm, Palo Alto Networks, reported recently that China had penetrated two dozen Cambodian government organizations as part of "a long-term espionage campaign." Similar reports arose ahead of the country's 2018 national election.

The draft also allows the collection or disclosure of data without consent for matters of "national interest." Cambodian officials have used similar terms, including "national security" and "public order," to justify the surveillance and arrests of opposition activists amid a yearslong crackdown on political dissent.

Jingting Liu, a research fellow at National University of Singapore's Asia Competitiveness Institute who studies the cross-border flow of data, said that for better data governance, such language should be detailed in compliance guides to protect against misuse by companies or law enforcement.

"It boils down to, what are national security concerns? What is legitimate and what is not so legitimate?" Liu said. "If there's more transparency and less ambiguity, that would generally help firms in compliance."

Cambodia, which has been ruled by the Hun family for nearly four decades, has pushed several contentious internet laws.

A cybersecurity law remains in draft form after receiving similar criticism from rights groups, while the status of the National Internet Gateway, which would route traffic through centralized government servers, has been in flux since officials said early last year that it had been delayed.

Although the European regulations have become a reference point for countries around the world, Southeast Asia's patchwork approach -- and governments' different capacities to enforce their own laws -- is a challenge for companies, said Xuechen Chen, a professor of politics and international relations at Northeastern University London.

"ASEAN is looking to the EU and perhaps wants to endorse some of its spirit," Chen said. "But in terms of the actual implementation, I don't think at the moment ASEAN has the preconditions to evolve or develop into a common and also effective data regulatory framework."