

INSIGHTS

Digital Sovereignty in the Age of AI : What Choices for Cambodia ?

SAIDNATTAR Ryanna¹, Ph.D. Candidate in Science and Technology Policy

¹ *AIDNATTAR Ryanna is a Ph.D. Candidate at the Korea Advanced Institute of Science and Technology (KAIST) and a Research Fellow in AI Forum.*

What is digital sovereignty?

Over the last decade, *digital sovereignty* (DS) has become a political slogan with global appeal (Pohle, Nanni and Santaniello, 2024). Yet, “digital” and “sovereignty” seem contradictory at first glance. “Sovereignty” belongs to an old political tradition where states hold final and absolute authority within a territory (Hinsley, 1966). “Digital”, by contrast, evokes a world of networks, data flows, and infrastructures that do not respect territorial borders. In today’s world, nearly every critical aspect of state authority, from finance to security, runs on digital networks (Chander and Sun, 2023). Territorial authority has become inseparable from digital control, calling for a redefinition of what sovereignty means in this context.

The scholarship defines digital sovereignty as a state's, an economy's, or an individual's autonomous control over its digital means and activities (Floridi, 2020; Glasze et al., 2023; Mügge, 2024). Several adjacent terms such as technology sovereignty and data sovereignty are often used interchangeably, with shifting scopes and definitions (Chander and Sun, 2023); in current policy discourse, DS has become the umbrella term subsuming them. Beyond its conceptual fuzziness, DS’s meaning also varies widely by regions and actors, but also by the kind of self-determination these actors pursue (Pohle and Thiel, 2020).

In Europe, DS refers to "strategic autonomy" through regulatory authority over US Big Tech (Bellanova et al., 2022; Farrand and Carrapico, 2022; Mügge, 2024). In China, it refers to the state’s full control over their digital sphere without any foreign interference (Creemers, 2020). In the United States, the term is rarely invoked because it already exercises *de facto sovereignty* through its dominance over the digital economy. When addressing partner states however, it has recently framed sovereignty as adopting American AI infrastructure with local data, languages, and policies (Kratsios, 2026). For a small nation like Cambodia, the questions it raises are different, as earlier techno-sovereignty work recognised (Gilberg and Chhem, 2021). This commentary extends on those questions and implications in the context of AI’s rise.

What does AI change?

The arrival of large-scale AI² has heightened the stakes of digital sovereignty. AI can itself be understood as an extension of the digital field, amplifying its features and fault lines such as market oligopolies and governance gaps (Nocetti, 2024). Thus, it is the domain where the sovereignty question becomes most acute. Three features of AI shape what is at stake.

First, AI is built on a vertically integrated stack of compute, semiconductors, training data, models, and applications, whose layers are technically interdependent (Song et al., 2026). No country controls all of them, so its relationship to AI must be negotiated layer by layer. The sovereignty question also differs by layer:

² In this commentary, “AI” refers to the current large-scale paradigm, meaning systems built on foundation models, including generative systems (LLMs) and not the narrower predictive tools already common in everyday services. Only the former depends on scarce compute and frontier models, which is what makes the sovereignty stakes acute.

high-cost layers (e.g., compute) pose the question "which foreign provider do we trust?", while accessible layers (e.g., data) make us wonder "how do we govern our own?" Which of these a country can realistically answer depends on which layers it can credibly act on.

Second, the capacity to build AI is concentrated in a very small number of countries and firms: the United States and China alone control more than 90% of global AI data-centre capacity (Song et al., 2026). At the high-cost layers, compute and frontier models, smaller states have little choice but to adopt one great power's stack or the other's — the pressure Gilberg and Chhem (2021) call "techno-imperialism"³. But beyond dependence lies a second risk: the risk of extraction. Couldry and Mejias (2019) call "data colonialism" the conversion of everyday life into an extractable resource by a handful of firms based in those same two powers. For a small state, the danger is to supply the data on which others build, with little say over how it is used or who benefits from it.

Lastly, AI systems embed worldviews (Birhane et al., 2022). LLMs such as ChatGPT and DeepSeek learn by reproducing the patterns in their training data, absorbing the assumptions and categories built into it. Consequently, no model is neutral. Because today's LLMs are trained mostly on English and Mandarin, they perform worse in languages with little digital presence. The cost, beyond weak performance, is erasure, shown when a community's history and knowledge are missing from the data, often because they were passed down orally or never well digitised (Weidinger et al., 2021). The United Nations Development Programme (UNDP, 2025) calls this "data invisibility": communities absent from the inputs are absent in the outputs.

Taken together, these features leave a small state one realistic move in the field of AI: acting on the layers within reach and shaping the terms on which it depends for the rest, so that its dependencies are deliberately chosen rather than absorbed by default (Musiani, 2025; Pohle and Thiel, 2020).

What does this mean for Cambodia?

The DS literature discussed above has been largely written from Western European and/or great-power vantage points, less so from the position of small states. For Cambodia, it is crucial that we open a different conversation and do not import great-power framings of DS naively, but adapt them to local conditions. This agency is exercised from a thin base (e.g., weak infrastructure, limited financing) but even so, a small base still leaves room for choice. What follows sets out three implications moving from the layer Cambodia can act on, to the scale at which it can bargain, to the practices through which sovereignty is sustained.

The first is that data and language are the most accessible layers. Sovereignty today is epistemic (Chhem, 2026): a country must know its environment through its own data and decide how that knowledge is used.

³ Gilberg and Chhem (2021) distinguish *techno-nationalism*, where a state emphasises its own technical and scientific development and seeks to protect it from others, from *techno-imperialism*, the attempt by major powers to entice or force other states to accept a particular version of the technology. *Techno-sovereignty* is their proposed small-state alternative: cooperating with others for mutual benefit while retaining sovereign control over technological development and use.

SEA-LION, AI Singapore's open-source large language model (LLM), has supported Khmer since its earlier versions (AI Singapore, 2025), however being included in a regional model is not the same as helping build it. In January 2025, AI Forum Cambodia and AI Singapore took steps towards this by agreeing to build a dedicated Khmer model and train Cambodian researchers, the existing Khmer foundation being too weak to work well (Khmer Times, 2025). This is a clear illustration of how Cambodia can actively shape the layer it can — the data — and ensure the kingdom's own contexts are built into the region's models.

The second is that regional coordination is where small-state sovereignty can actually be exercised. In this context, sovereignty can be plural, a capacity held at several levels, including regional groupings (Jiang and Belli, 2024; Couture and Toupin, 2019). The ASEAN Working Group on AI Governance, formed in Phnom Penh in 2024, now coordinates regional initiatives (IMDA, 2024), and the Digital Economy Framework Agreement (DEFA)⁴ (ASEAN, 2025) expected by end-2026, will make parts binding. A frontier provider can ignore the demands of one small market, but not a coordinated bloc. For Cambodia, bargaining power over these providers is possible at the ASEAN level.

The third implication is that sovereignty is socio-technical; it is lived in practices and infrastructures. The draft National AI Strategy positions Cambodia as a "skilful adopter" of AI (MPTC, 2025), but skilful adoption should not become passive procurement. The audit, disclosure, and localisation conditions the state attaches to each contract for health, education, or administration decide if it builds Cambodian capacity or entrenches dependence. This is what Chhem (2026) calls the "quiet cultivation of competence", the slow institutional work of building the ability to verify, adapt, and maintain rather than simply buy. Without it, sovereignty becomes dependence by default.

Cambodia is not competing to lead the AI race, nor should it be. What it can do is decide the terms of its dependence, shape the data that carries its language, negotiate through ASEAN where a single voice would not carry weight, and attach to each contract conditions that build competence instead of buying convenience. In the age of AI, sovereignty is practised rather than owned, and a "skilful adopter", to stay sovereign, must remain a deliberate one.

⁴ The ASEAN-wide agreement on digital trade covering cross-border data flows, digital payments, and emerging areas such as AI cooperation and source code. Negotiations were substantially concluded in October 2025, with signing expected in 2026; once in force, its provisions will bind member states.

References

- AI Singapore. (2025). *SEA-LION v4: Advancing open, multimodal AI for Southeast Asia*. <https://aisingapore.org/aiproducts/sea-lion/>
- Association of Southeast Asian Nations. (2025, October 24). *ASEAN Economic Community Council statement on the substantial conclusion of the ASEAN DEFA negotiations*. <https://asean.org/asean-economic-community-council-statement-on-the-substantial-conclusion-of-the-asean-defa-negotiations/>
- Bellanova, R., Carrapico, H., & Duez, D. (2022). Digital/sovereignty and European security integration: An introduction. *European Security*, 31(3), 337–355. <https://doi.org/10.1080/09662839.2022.2101887>
- Birhane, A., Kalluri, P., Card, D., Agnew, W., Dotan, R., & Bao, M. (2022). The values encoded in machine learning research. In *2022 ACM Conference on Fairness, Accountability, and Transparency (FAccT '22)* (pp. 173–184). Association for Computing Machinery. <https://doi.org/10.1145/3531146.3533083>
- Chander, A., & Sun, H. (Eds.). (2023). *Data sovereignty: From the digital silk road to the return of the state*. Oxford University Press.
- Chhem, K. R. (2026, February 19). Teaching sovereignty in the AI age: A self-reflection. *AIF Insights*, 2026(8). AI Forum Cambodia.
- Couldry, N., & Mejias, U. A. (2019). Data colonialism: Rethinking big data's relation to the contemporary subject. *Television & New Media*, 20(4), 336–349. <https://doi.org/10.1177/1527476418796632>
- Couture, S., & Toupin, S. (2019). What does the notion of "sovereignty" mean when referring to the digital? *New Media & Society*, 21(10), 2305–2322. <https://doi.org/10.1177/1461444819865984>
- Creemers, R. (2020). China's conception of cyber sovereignty: Rhetoric and realization. In D. Broeders & B. van den Berg (Eds.), *Governing cyberspace: Behavior, power and diplomacy* (pp. 107–142). Rowman & Littlefield.
- Farrand, B., & Carrapico, H. (2022). Digital sovereignty and taking back control: From regulatory capitalism to regulatory mercantilism in EU cybersecurity. *European Security*, 31(3), 435–453. <https://doi.org/10.1080/09662839.2022.2102896>
- Floridi, L. (2020). The fight for digital sovereignty: What it is, and why it matters, especially for the EU. *Philosophy & Technology*, 33(3), 369–378. <https://doi.org/10.1007/s13347-020-00423-6>
- Gilberg, T., & Chhem, R. (2021). *Techno-nationalism and techno-sovereignty* (AVI Policy Brief No. 01). Asian Vision Institute.
- Glasze, G., Cattaruzza, A., Douzet, F., Dammann, F., Bertran, M.-G., Bômout, C., Braun, M., Danet, D., Desforges, A., G ry, A., Grumbach, S., Hummel, P., Limonier, K., M n binger, M., Nicolai, F., P tinaud, L., Winkler, J., & Zanin, C. (2023). Contested spatialities of digital sovereignty. *Geopolitics*, 28(2), 919–958. <https://doi.org/10.1080/14650045.2022.2050070>
- Hinsley, F. H. (1966). *Sovereignty*. Cambridge University Press.

- Infocomm Media Development Authority. (2024). *ASEAN Working Group on AI Governance (WG-AI)*. <https://www.imda.gov.sg/about-imda/international-relations/asean-working-group-on-ai-governance>
- Jiang, M., & Belli, L. (Eds.). (2024). *Digital sovereignty in the BRICS countries: How the Global South and emerging power alliances are reshaping digital governance*. Cambridge University Press.
- Khmer Times. (2025, January 22). *Khmer language gets AI-infusion*. <https://www.khmertimeskh.com/501627225/khmer-language-gets-ai-infusion/>
- Kratsios, M. (2026, February). *Remarks at the India AI Impact Summit* [Speech]. White House Office of Science and Technology Policy.
- Ministry of Post and Telecommunications. (2025, June). *Draft national artificial intelligence strategy: Public consultation*. Kingdom of Cambodia. <https://ai.gov.kh>
- Mügge, D. (2024). EU AI sovereignty: For whom, to what end, and to whose benefit? *Journal of European Public Policy*, 31(8), 2200–2225. <https://doi.org/10.1080/13501763.2024.2318475>
- Musiani, F. (2025). Reassessing "infrastructuring digital sovereignty": Digital self-determination as a set of infrastructure-embedded practices. *Frontiers in Communication*, 10, Article 1562072. <https://doi.org/10.3389/fcomm.2025.1562072>
- Nocetti, J. (2024, March 27). *Qu'est-ce que la souveraineté numérique ?* [Interview]. Renaissance Numérique. <https://www.renaissancenumerique.org/publications/souverainete-numerique/>
- Pohle, J., Nanni, R., & Santaniello, M. (2024). Unthinking digital sovereignty: A critical reflection on origins, objectives, and practices. *Policy & Internet*, 16(4), 666–671. <https://doi.org/10.1002/poi3.437>
- Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*, 9(4). <https://doi.org/10.14763/2020.4.1532>
- Song, H., Tsukioka, K., Ubaldi, B., Andersen, R., Harvard, J., Ward-Jackson, G., Langengen, T., West, D., & Teo, M. (2026, January). *Sovereignty in the age of AI: Strategic choices, structural dependencies and the long game ahead*. Tony Blair Institute for Global Change. <https://institute.global/insights/tech-and-digitalisation/sovereignty-in-the-age-of-ai-strategic-choices-structural-dependencies>
- United Nations Development Programme. (2025). *The next great divergence? Human development in Asia and the Pacific in the age of AI* [Regional human development report].
- Weidinger, L., Mellor, J., Rauh, M., Griffin, C., Uesato, J., Huang, P.-S., Cheng, M., Glaese, M., Balle, B., Kasirzadeh, A., Kenton, Z., Brown, S., Hawkins, W., Stepleton, T., Biles, C., Birhane, A., Haas, J., Rimell, L., Hendricks, L. A., ... Gabriel, I. (2021). *Ethical and social risks of harm from language models* (arXiv:2112.04359). arXiv. <https://doi.org/10.48550/arXiv.2112.04359>

* Edited with ChatGPT for clarity; all views expressed are solely those of the author.

* The opinions expressed are the author's own and do not reflect the views of AI Forum.