

Sovereign AI: From a Technological Idea to a Matter of State Resilience

Author: Bernaziuk Ian

Affiliation: Supreme Court

Publication: Конституціоналіст · 2026

Publication date: 2026-05-20

Permanent URL: <https://constitutionalist.com.ua/sovereign-ai-from-a-technological-idea-to-a-matter-of-state-resilience/>

Author information

Ian Bernaziuk, Professor, J.S.D.

Judge of the Supreme Court (Ukraine)

ORCID: 0000-0002-2353-4836

bernaziuk1979@gmail.com

Abstract

Part I. What Is Sovereign AI

In contemporary international discourse, sovereign AI is increasingly understood not as complete technological isolation, but as the capacity of a State or an association of States to preserve strategic resilience and real influence over critical AI capabilities. This concerns, above all, control over infrastructure, computing resources, data, language models, testing procedures, cybersecurity, and the safe deployment of such technologies.

Thus, sovereign AI is not a separate product and does not necessarily mean a State's "own large model". It is, first and foremost, a system of controlled capabilities that enables the reduction of critical dependence on external providers, infrastructural constraints, and the like. For this reason, the issue is now directly connected not only with innovation, but also with digital sovereignty, cyber resilience, protection of personal data, and trust in public institutions.

The key features of sovereign AI include strategic control over critical AI capabilities; guaranteed access to computing power; control over data, models, and their national and linguistic suitability; territorially or operationally controlled infrastructure; and institutional capacity to assess, test, certify, and support the safe use of advanced AI systems.

The rise of artificial intelligence adds a new dimension to this challenge. Artificial intelligence systems trained on opaque datasets, governed by private providers, or hosted on foreign infrastructure introduce inherent vulnerabilities. They may distort institutional language or legal traditions, or generate outputs that undermine, rather than uphold, legislative and administrative integrity. For democratic institutions, including parliaments, required to demonstrate democratic legitimacy under the most demanding circumstances, these risks are real.

Part II. International Practice in Building Sovereign AI

International practice demonstrates that models for building sovereign AI may vary.

India provides one of the clearest examples of combining sovereign compute and a sovereign model. The State not only uses ready-made foreign solutions, but also builds its own foundation: it is deploying a national network of computing centres and developing BharatGen — a State multilingual AI project capable of operating in many of the country's official languages. This is an example of how the combination of public investment and technological control creates the foundation for digital autonomy.

The United Kingdom has chosen a different approach: rather than creating a single State model, it focuses on strengthening control over critical links in the AI ecosystem, supporting national AI companies, and investing in its

own segment of the AI value chain. This shows that sovereignty may be formed not only through a state-developed baseline model, but also through the development of a domestic market, infrastructure, and investment capacity. In this case, the emphasis is not on technological self-isolation, but on ensuring that the key nodes in the creation, deployment, and support of AI solutions do not remain entirely outside national influence.

France demonstrates one of the most comprehensive European approaches: combining sovereign AI infrastructure with specialised institutions for assessing the safety and reliability of AI systems. In this case, sovereign AI appears as a combination of infrastructure, evaluation capacity, and governance.

Lithuania is an illustrative example of an effective model for approaching the study of this issue. The LitAI Factory project provides for the development of high-performance computing, data storage systems, and access to computing accelerators within the European network of AI Factories. This approach demonstrates a model of “sovereignty through integration”, rather than through isolation. In practical terms, this means that even a State without exceptionally large resources of its own can strengthen digital autonomy if it ensures controlled access to critical infrastructure, its own data, and procedures for the safe use of AI within an allied technological ecosystem.

Part III. Ukraine: From Concept to Practical Policy

For Ukraine, this issue already has not merely a prospective, but also an entirely practical dimension. Over the recent period, the Ministry of Digital Transformation of Ukraine has already taken a number of concrete steps towards the formation of a sovereign AI ecosystem. In particular, cooperation with NVIDIA has been launched to develop sovereign AI infrastructure for Ukraine, including national AI infrastructure for critical public AI services based on NVIDIA accelerated computing; at the same time, the creation of a Ukrainian large language model (LLM) has been identified as a separate State priority, serving as an instrument for strengthening the position of the Ukrainian language in the digital space and in public services. In parallel, the Ministry of Digital Transformation has publicly emphasised that over the past year Ukraine has moved from discussion to the implementation of real AI solutions for the State, including in the fields of security and defence — from the analysis of satellite imagery to object-recognition systems. Another area is cooperation with Microsoft on digital infrastructure, cloud technologies, cybersecurity, and AI-related solutions for public administration.

In addition, an approach has already been announced for creating small specialised language models for the judicial sphere, which are to be trained in a secure environment without the risk of personal data leakage. At the same time, it is fundamentally important that such systems be used exclusively for informational, analytical, reference, organisational, and technical support of court activity, and not for delegating to AI the assessment of evidence, the legal classification of the circumstances of a case, or the formation of a judicial decision on the merits.

It is the combination of these steps that indicates that, in Ukraine, sovereign AI is beginning to take shape not only as a concept, but as a practical State policy.

Part IV. Sovereign AI in the Sphere of Justice

For the sphere of justice, this issue is particularly sensitive. In this area, not just any AI is acceptable, but only AI that does not interfere with the judge's independent judicial assessment, does not substitute the assessment of evidence, does not concern the process of adopting a judicial decision, and does not create a risk of leakage of personal data or non-public state information. For this very reason, for the judicial system, sovereign AI means, above all, control over data, infrastructure, language models, cybersecurity, and procedures for safe use. Without this, digitalisation may weaken, rather than strengthen, the independence, trust, and security of justice.

This approach can already be traced in Ukrainian regulatory and institutional documents. In particular, the Code of Judicial Ethics and its official commentary define the limits of permissible use of AI technologies by a judge, while emerging institutional frameworks emphasise the need to protect restricted-access information, prevent AI from substituting independent legal reasoning, and preclude the delegation to AI of the judicial decision-making function.

Part V. Conclusion

Ultimately, sovereign AI should be regarded not as a technological symbol of prestige and not as a short-term innovation trend, but as a new dimension of independence. In the twenty-first century, a State is not only an entity that possesses territory, institutions, an army, and legislation, but also an entity capable of maintaining control over critical digital infrastructure, data, models, and the rules for their safe use. It is in this context that sovereign AI is

gradually becoming a matter not only of technological development, but also of national security, legal certainty, and institutional resilience.

Disclaimer: The views expressed in this blog are personal and academic in nature and do not represent the official position of the Supreme Court of Ukraine or any public authority.

Material files

[Original author file](#)