Issue Brief

Vol.134, No.9, 2025

Implications of Neural Data Issues in the AI Era from the Perspective of Cognitive Sovereignty

Junghyun Yoon
(Research Fellow, INSS)

INSS INSTITUTE FOR NATIONAL SECURITY STRATEGY 국가안보전략연구원

Abstract

As reliance on AI-driven decision-making increases, a growing concern is that the cognitive environment enabling individuals to discern what is true and accurate—independently and without external interference—is under threat. In light of such concerns, the European Union's *Guidelines on Data Protection in the Neurosciences*, released this past March, highlight the pressing need to safeguard cognitive sovereignty through practical measures. The guidelines emphasize the unique sensitivity of neurodata in the age of AI, asserting the need for special protections. They explicitly prohibit exploitative practices and present a comprehensive framework to strengthen national security. South Korea should examine the normative principles and legislative proposals laid out in the EU guidelines to establish a legal foundation for responding to emerging threats. In particular, given the broad societal and security implications of neuroscience, cognitive sovereignty should not be regarded as a subset of data protection but approached as an independent policy objective. Furthermore, it is crucial to commit to long-term investments in "cognitive security technologies," capable of early detection and analysis of cognitive interferences.

Keywords

Guidelines on Data Protection in the Neurosciences, Cognitive Sovereignty, Neuroscience, Data Protection

Implications of Neural Data Issues in the AI Era from the Perspective of Cognitive Sovereignty

Junghyun Yoon
(Research Fellow, INSS)

As the era of "AX" (Artificial Intelligence Transformation) gains momentum, the threats posed by AI are expanding beyond technical domains into areas concerning human cognition, decision-making, and social trust. In particular, disinformation, market disruption, and distorted public opinion through generative AI can lead to destructive consequences, such as undermining trust in government and weakening social cohesion.

The concept of cognitive warfare—the act of manipulating or influencing the cognitive processes of target groups by external actors to achieve specific political objectives—is also expected to become increasingly sophisticated through the convergence of neuroscience and AI. With access to vast datasets, it is now possible to conduct highly customized psychological operations based on the analysis of a group's key concerns and value preferences.

Amid such developments, the issue of cognitive sovereignty is increasingly being discussed. Notably, the EU *Guidelines on Data Protection in the Neurosciences*, published in March, call attention to the need for practical efforts to secure cognitive sovereignty. The guidelines explicitly recognize the sensitive nature of neural data in the AI era and emphasize the need for special safeguards and controlled access. Furthermore, they stress the protection of individuals' cognitive integrity as a fundamental

component of democratic societies.

The document goes beyond the individual level, offering a comprehensive framework that includes principles for explainable AI using neural data and guidelines concerning the development of neurotechnology-based weapons. In doing so, it presents multidimensional standards aimed at reinforcing not only individual rights but also national-level cognitive sovereignty.

Cognitive Sovereignty in the Era of High-Impact AI

Cognitive sovereignty refers to the ability of individuals or groups to retain control over their cognitive processes such as thinking, perception, and decision-making. In today's advanced digital information environment, it is increasingly recognized as a national and civic right essential for preserving autonomous judgment.[1] However, with advances in neuroscience, major powers have started to regard the "cognitive domain"—the space of the human mind and thought—as the next battlefield. Cognitive warfare is being pursued as a strategic means to influence this domain. Moreover, when combined with emerging technologies such as AI and cyber capabilities, the cognitive domain is redefined as a complex strategic space with wide-ranging implications for national security.

The proliferation of generative AI services, particularly those based on large language models (LLMs), has further amplified the threat of AI-driven influence operations. In this context, cognitive sovereignty serves as a critical safeguard—enabling citizens to maintain autonomy, critical thinking, and independent judgment against the persuasive force of algorithmic manipulation.

1) Lee A. Bygrave, "Machine Learning, Cognitive Sovereignty and Data Protection Rights with Respect to Automated Decisions", Cambridge Handbook of Life Sciences, Information Technology and Human Rights, (May 2022), Cambridge University Press.

In response to these growing risks, the European Union has taken early action through frameworks such as the *General Data Protection Regulation* (GDPR, 2018) and the EU *Artificial Intelligence Act* (2024). The GDPR affirms individuals' rights to autonomy and control over all personal data, including sensitive neural signals and emotional responses. The EU AI Act, in turn, imposes legal obligations of transparency, explainability, and safety on high-impact AI systems that may influence human cognition. These measures are designed to safeguard mental autonomy and decisional independence from automated manipulation and psychological interference.

EU's Normative Efforts to Institutionalize Cognitive Sovereignty

The EU Guidelines on Data Protection in the Neurosciences,[2] recently issued by the Council of Europe, underscore the need to treat brain-based data collected in the field of neuroscience as a special category of data, going beyond conventional frameworks of personal data protection. Neural data—comprising patterns of brain activity and neural signals derived from the human nervous system—poses distinct regulatory challenges due to its sensitive nature. Unlike general personal data, neural data can reveal deeply intimate aspects of an individual's thoughts, emotions, preferences, and even identity. As such, it carries significant risks of data breaches, unauthorized surveillance, and manipulation.

Historically, the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), and its updated version, Convention 108+ (CETS No. 223), have provided a robust institutional foundation

2) Council of Europe, "Draft Guidelines on Data Protection in the context of neurosciences: CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA" (5 March 2025).

for ensuring privacy and data protection. These conventions established general standards prohibiting the unauthorized use, access, disclosure, or misuse of personal data. However, due to the heightened sensitivity and technical specificity of neural data, additional normative efforts have become necessary to adapt these principles to neurotechnology.

The new guidelines were developed against this backdrop. They address a wide array of regulatory concerns, including the increasing sensitivity of neural data, the risk of re-identifying anonymized brain data, the scope of lawful processing based on legitimate purposes, and the enforcement of the purpose limitation principle throughout the data lifecycle.

A central concern highlighted by the guidelines is the cognitive harm that may result when AI or automated systems interpret or analyze neural data. The use of algorithms for emotional inference, personality profiling, and behavioral prediction may infringe on individuals' rights to cognitive self-determination. To mitigate such risks, the guidelines call for implementing the explainable AI principle, emphasizing the individual's right to understand and contest both the process and outcome of brain data interpretation.

Furthermore, the guidelines emphasize the need for continuous institutional efforts to protect individual autonomy over thoughts, emotions, and intentions—the core of one's internal mental life. As cognitive information constitutes sensitive data, it must be governed by protective principles, including stringent consent procedures and control measures before data processing begins. By codifying such protections, cognitive sovereignty is elevated from a theoretical ideal to a concrete legal and social value upheld through enforceable norms.

Key Ethical Principles for Responsible Use

The guidelines stipulate that every stage of collecting, processing, storing, and utilizing neural signal data must respect the fundamental digital-era rights of mental privacy, cognitive integrity, and cognitive self-determination. Key principles include data minimization, purpose limitation, necessity and proportionality, and transparency. Institutions handling brain signal data must inform subjects about the types of collected data, the purpose and legal basis for processing, the authorized user, and the rights of data subjects regarding access, rectification, deletion, objection, and portability. In particular, the guidelines explicitly state that the right to explanation and human intervention must be guaranteed when automated decision-making based on neural signal data is involved. Furthermore, all stakeholders, including supervisory bodies and manufacturers, are urged to establish systems for data impact assessment, cybersecurity, explainability, and accountability following the principle of human rights by design. Policymakers are especially advised to clarify the legal basis for neural data processing and to establish independent oversight mechanisms and continuous ethical evaluation systems.

The use of neurodata for predictive profiling, behavioral assessment, or inference of sensitive mental characteristics is restricted to public interest or scientific research purposes and even then is only allowed under strict legal and ethical safeguards. Data security is designated as a top priority, with the application of advanced encryption, access control, and incident response systems strongly recommended. The data retention period must also be limited to the minimum necessary to fulfill its stated purpose, after which the data must be promptly deleted or anonymized. Regarding data transfers, highly stringent standards apply, and when data is to be transferred to countries with lower levels of regulatory protection, additional safeguards must be

ensured. In short, the guidelines emphasize establishing a multi-layered protection framework to ensure that the use of neurodata does not violate ethical norms or fundamental rights.

Implications for AI Security

These recommendations go beyond personal data protection, elevating cognitive sovereignty to a principle directly tied to national security in the age of AI. This aligns with key strategic directions currently being developed in "AI security," which is increasingly the subject of in-depth global discussions. AI security is defined as the prevention of risks and harmful consequences arising from AI-driven threats—including the potential for malicious use by adversarial actors—iand encompasses areas such as military applications of AI, responses to cyber threats, protection of AI technological sovereignty, and preemptive efforts against cognitive warfare and influence operations.[3] Leading AI powers, including the United States and the United Kingdom, are already incorporating institutional, technical, and policy-level measures to counter AI-related threats and misuse within their national AI security strategies.[4] Within this context, the EU's guidelines reflect growing concern about technologies that enable external actors to directly influence the cognitive structures of individuals or social groups through the use of brain signal data. Therefore, the EU's initiative can be seen not only as an effort to safeguard cognitive sovereignty but also as a broader attempt to establish institutional safeguards for national AI security by preventing the misuse of AI innovations combined with neuroscience that could instrumentalize and exploit human thought and inner life.

3) https://www.hpe.com/emea_africa/en/what-is/ai-security.html
4) AP News, "New rules for US national security agencies balance AI's promise with need to protect against risks" (October 25, 2024).

Policy Recommendations

The Guidelines on Data Protection in the Neurosciences demonstrate the EU's policy stance of maintaining strong norms and controls over AI, even amid the aggressive deregulatory trends in the United States—particularly under the second Trump administration. This reflects how seriously the EU regards the importance of cognitive sovereignty in neural data. The Republic of Korea needs to examine these guidelines closely and explore institutional improvements for the following reasons:

First, there is an urgent need to prepare for the military, intelligence, and psychological warfare uses of neuroscience technologies, such as influence operations based on large language models (LLMs) and cognitive warfare. South Korea must establish systematic response measures for such threats by reviewing the application of normative principles and legislative discussions for neurodata management.

Second, the guidelines offer insights for addressing blind spots in the domestic data regulatory framework. While Korea is revising its Personal Information Protection Act to define biometric information and specify collection procedures and usage scopes, it has yet to address neural data or emotion-based profiling. As the EU guidelines include cognitive sovereignty impact assessments and concrete implementation principles, they can serve as a useful reference for comprehensive legislation in response to future trends of AI and biotechnology convergence. Furthermore, such proactive consideration is necessary to ensure alignment with international norms as Korean AI and bio industries expand globally.

Third, given the broad social and security impact of neuroscience, cognitive sovereignty in the AI era should be regarded not as a

subcategory of data protection but as an independent policy objective. Korea should consider comprehensive legislative directions such as a "Digital Cognitive Sovereignty Framework."

Fourth, the guidelines highlight the need for medium- to long-term investments in "cognitive security technologies" capable of detecting and analyzing attempts at cognitive intrusion. Representative technologies include neural interfaces, LLM-based persuasion algorithms, and biosensor-based emotion analysis. The promotion of such research and development should seek approaches that sustain innovative momentum through cooperation involving military, intelligence, and private-sector actors.

The views and opinions expressed in this report are those of the author(s) and do not necessarily reflect the official position of INSS.