DIGITAL SOVEREIGNTY OF STATES: INTERNATIONAL LEGAL ASPECTS AND CHALLENGES

Turgunbaev Akmyrza Maksatbekovich

Student of the Institute of History and Law of Osh State University

Kyrgyz Republic, Osh

E-mail: blablablashkabek@gmail.com

T: +996990001700

ABSTRACT

This article analyzes the phenomenon of digital sovereignty as a new dimension in international relations and international law. It examines various states' approaches to defining and implementing digital sovereignty, identifies key international legal aspects and contradictions related to internet governance, cross-border data flows, and cybersecurity. Special attention is given to international initiatives aimed at developing digital law norms and the necessity for coordinated regulatory mechanisms.

Keywords: digital sovereignty, international law, cybersecurity, cross-border data, internet governance.

Introduction

The digitization of all spheres of social life has led to the emergence of a new dimension of state sovereignty — digital sovereignty. This concept refers to a state's ability to independently determine the rules regulating the digital space within its territory, including the management of information flows, protection of personal data, and ensuring cybersecurity.

The growing importance of digital sovereignty is connected with the global interdependence in the Internet environment, where transnational corporations dominate and there is a lack of universal international legal norms that balance the interests of states. This necessitates the development of new international legal approaches capable of reconciling state rights with the global interests of humanity.

Concept and Content of Digital Sovereignty

Digital sovereignty derives from classical state sovereignty and includes:

Control over digital infrastructure (servers, communication channels, data centers).

The right to regulate cross-border data flows, including personal and commercial information.

Cybersecurity — protection against cyberattacks, malicious interference, and illegal use of digital technologies.

The right to determine digital policy in accordance with national interests.

Different states interpret digital sovereignty differently. For example, China links it with the concept of "cyber sovereignty," implying full state control over internet space. The European Union emphasizes data protection and technological independence, promoting GDPR standards. Russia views digital sovereignty as the ability to ensure stable operation of its national segment of the internet (Runet) and regulate foreign internet companies.

International Legal Aspects of Digital Sovereignty

Digital sovereignty is directly connected with the principles of the UN Charter, primarily the non-intervention in domestic affairs and territorial integrity of states. However, the transboundary nature of the digital space creates tensions between national interests and the principle of internet freedom.

Key international legal aspects include:

The right to control data: There is no unified international regime regulating cross-border data transfers.

State responsibility for cyberattacks: The Tallinn Manual considers cyberattacks under international humanitarian law, but legally binding norms are still lacking.

Role of international organizations: ITU, ICANN, and the UN discuss internet governance mechanisms, but no consensus on sovereignty issues has been reached.

Challenges in Implementing Digital Sovereignty

Key challenges include:

Internet fragmentation: States' attempts to control the network may lead to the creation of "national segments" of the internet.

Dominance of transnational corporations: Large IT companies (Google, Meta, Amazon) often operate beyond the scope of state regulation.

Lack of international rules: The absence of universal norms creates a legal vacuum, exacerbating conflicts in the digital environment.

Conclusion

Digital sovereignty is not only a matter of domestic policy but also a crucial element of international relations requiring legal regulation. Currently, international law lacks universal norms governing digital sovereignty, which necessitates the development of new international treaties and rules of state behavior in cyberspace.

Establishing a balance between states' rights to control their digital sphere and the need to preserve the global interconnectedness of the internet should become a priority for the international community.

References:

1. Charter of the United Nations, 1945.
2. Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press, 2017.
3. European Union. General Data Protection Regulation (GDPR), 2018.
4. Nye, J. The Regime Complex for Managing Global Cyber Activities. Global Commission on Internet Governance, 2014.
5. DeNardis, L. The Global War for Internet Governance. Yale University Press, 2014.