INTERNATIONAL SCIENTIFIC JOURNAL OF BIRUNI
ISSN (E) 2181-2993
Volume 5, Issue 2. (2026)

УДК: 130.2:321.01:004.8

СУБЪЕКТЫ И ГРАНИЦЫ СУВЕРЕНИТЕТА В ЦИФРОВОМ ПРОСТРАНСТВЕ: СОЦИАЛЬНО-ФИЛОСОФСКИЙ АНАЛИЗ

Кобулов Бехзод
Самостоятельный соискатель
Наманганского государственного университета,
Наманган, Узбекистан
E-mail: justprogress2030@gmail.com. ORCID: 0009-0008-2009-0038
Тел.: +998993706601

АННОТАЦИЯ

В статье рассматривается трансформация государственного суверенитета в цифровом пространстве через анализ смещения его субъектов и границ. Показано, что цифровая среда порождает многосубъектную конфигурацию власти, в которой наряду с государством действуют транснациональные платформы, технические сообщества и индивиды. Предложено различать «суверенитет над территорией», «суверенитет над данными» и «суверенитет над алгоритмической инфраструктурой». Обосновано, что цифровой суверенитет следует понимать как способность политического сообщества к самоопределению в условиях технологической взаимозависимости, а не как автаркию. Рассмотрены основные направления политики Узбекистана в этой сфере.

Ключевые слова: *цифровой суверенитет, платформы, данные, легитимность, социальная философия, цифровое пространство, самоопределение.*

ABSTRACT

This article examines the transformation of state sovereignty within the digital space by analyzing shifts in its subjects and boundaries. It demonstrates that the digital environment gives rise to a multi-actor configuration of power, in which transnational platforms, technical communities, and individuals operate alongside the state. The author proposes distinguishing between "sovereignty over territory," "sovereignty over data," and "sovereignty over algorithmic infrastructure." It is argued that digital sovereignty should be understood as a political community's capacity for self-determination amidst technological interdependence, rather than as autarky. The article also explores the key policy directions of Uzbekistan in this domain.

Keywords: digital sovereignty, platforms, data, legitimacy, social philosophy, digital space, self-determination.

ВВЕДЕНИЕ

Цифровизация изменила не только способы коммуникации, но и структуру общественной власти. Ключевые общественные функции, такие как идентификация граждан, публичная дискуссия, распределение информации и финансовые расчёты, всё чаще опосредуются частными платформами и глобальной технической инфраструктурой. Это ставит под вопрос центральный тезис классической теории суверенитета: государство как единственный носитель высшей власти на своей территории.

Проблема усугубляется концептуальной неопределённостью. Термины «цифровой суверенитет», «суверенитет данных» и «технологический суверенитет» употребляются в научном и политическом дискурсе непоследовательно [1; 2]. Одни авторы связывают их с усилением государственного контроля, другие — с правами личности, третьи — с автономией сообществ. Это требует социально-философского уточнения.

Цель статьи заключается в выявлении субъектов и границ суверенитета в цифровом пространстве и обосновании его социально-философской модели. **Задачи:** 1) проанализировать смещение субъектов власти; 2) описать трансформацию границ суверенитета; 3) определить критерии легитимного цифрового суверенитета.

Материалы и методы

Исследование выполнено в русле социальной философии и опирается на:

диалектический подход, позволяющий рассматривать суверенитет как противоречивое единство автономии и взаимозависимости;

институционально-структурный анализ распределения власти между государством, рынком и гражданским обществом;

сравнительно-концептуальный метод для разграничения близких понятий;

критическую герменевтику для интерпретации политико-правовых документов и научных текстов.

Теоретическая база включает работы К. Шмитта, М. Фуко, Ю. Хабермаса, М. Кастельса, С. Сассен, Ш. Зубофф, Л. Лессига, а также современные исследования цифрового суверенитета [1–10]. В качестве нормативного материала использованы документы Республики Узбекистан: Указ Президента

№ УП-6079 от 5 октября 2020 г. («Цифровой Узбекистан – 2030»), Закон «О персональных данных» (2019) и Закон «О кибербезопасности» (2022) [11–13].

Результаты

1. Смещение субъектов: от монополии к сети

В классической модели носителем суверенитета выступает государство, обладающее монополией на легитимное насилие. К. Шмитт определял суверена как того, кто принимает решение о чрезвычайном положении [3]. В цифровом пространстве способность «принимать решение» частично распределена. Платформы устанавливают правила публичной коммуникации, модерируют контент и определяют доступ к сервисам. Технические стандарты вырабатываются международными организациями и профессиональными сообществами, а алгоритмы ранжирования фактически структурируют публичную сферу.

Л. Лессиг показал, что программный код выполняет регулятивную функцию, сопоставимую с правом [4]. Тем самым возникает **«регуляторная конкуренция»** между правом и архитектурой. Государство остаётся ключевым, но не единственным субъектом. Правильнее говорить о **многосубъектной конфигурации власти**, где суверенитет реализуется как способность государства координировать и ограничивать иные центры влияния.

Ш. Зубофф описывает механизм, при котором пользовательские данные становятся сырьём для предсказания поведения [5]. Формируется асимметрия знания: платформа знает о пользователе значительно больше, чем он о ней. Для социальной философии это означает, что власть всё определённее опирается на **эпистемическое превосходство**, что усложняет традиционные способы контроля и подотчётности.

2. Трансформация границ

Цифровое пространство не отменяет границ, но меняет их природу. Выделены три типа границ суверенитета:

1) **территориальная граница.** Сохраняется в физической инфраструктуре: дата-центры, кабели, узлы обмена трафиком находятся под конкретной юрисдикцией. С. Сассен подчёркивает, что глобальное не «вытесняет» национальное, а встраивается в него, образуя новые сборки территории, власти и прав [6];

2) **информационная граница.** Определяется режимами доступа, правилами трансграничной передачи данных и требованиями к их локализации;

3) **алгоритмическая граница.** Отделяет пространство, где правила определены прозрачно и подконтрольно обществу, от пространства «чёрного ящика».

Таким образом, суверенитет из «линейной» категории превращается в **многослойную**. Государство может обладать достаточным контролем на одном уровне и быть зависимым на другом, что требует дифференцированной оценки суверенитета, а не бинарного «есть или нет».

3. Критерии легитимного цифрового суверенитета

Ю. Хабермас связывает легитимность с возможностью граждан быть одновременно адресатами и авторами норм [7]. Применительно к цифровой среде выделены четыре критерия:

- **правовая определённость:** правила понятны, публичны и оспариваемы;
- **защита автономии личности:** контроль граждан над персональными данными и цифровой идентичностью;
- **прозрачность и подотчётность:** возможность общественного контроля над алгоритмами, влияющими на существенные решения;
- **инклюзивность:** доступ к цифровым благам без дискриминации по региону, возрасту и социальному положению.

Суверенитет, не удовлетворяющий этим критериям, рискует превратиться в технологический контроль без социальной легитимации.

Обсуждение

Полученные результаты позволяют полемизировать с двумя упрощёнными позициями. Первая, «киберлибертарианская», восходит к декларации Дж.П. Барлоу о независимости киберпространства [10] и утверждает несостоятельность государственного суверенитета в сети. Практика последних десятилетий, от регулирования персональных данных до создания национальных систем кибербезопасности, опровергает этот тезис. Вторая позиция, «изоляционистская», отождествляет цифровой суверенитет с закрытостью и импортозамещением. Однако она недооценивает взаимозависимость глобальной технологической цепочки и риски утраты инновационной динамики.

Мы полагаем, что содержательной альтернативой служит понимание цифрового суверенитета как **способности к самоопределению в условиях взаимозависимости**. Эта способность включает контроль над критическими элементами инфраструктуры, правовую субъектность в регулировании данных и участие в выработке международных технических и правовых норм.

Направления политики Узбекистана, включая стратегию «Цифровой Узбекистан – 2030», закрепление правового режима персональных данных и институционализацию кибербезопасности, можно интерпретировать как движение к укреплению инфраструктурного и нормативного уровней суверенитета [11–13]. Вместе с тем сохраняются вызовы на уровне алгоритмической границы: зависимость от зарубежных платформ и облачных решений, а также необходимость развития национальных компетенций и цифровой грамотности населения. Ограничение исследования состоит в его теоретическом характере: для верификации выводов необходимы эмпирические данные, включая социологические опросы и экспертные интервью.

ЗАКЛЮЧЕНИЕ

1. Цифровая среда трансформирует суверенитет из моносубъектной и линейной категории в многосубъектную и многослойную.

2. Власть в цифровом пространстве всё в большей степени опирается на владение данными и знанием, что смещает акцент с территориального контроля на эпистемический.

3. Легитимность цифрового суверенитета определяется правовой определённостью, защитой автономии личности, прозрачностью алгоритмов и инклюзивностью.

4. Наиболее продуктивна модель суверенитета как самоопределения в условиях взаимозависимости, предполагающая баланс открытости и защищённости.

СПИСОК ЛИТЕРАТУРЫ

1. Couture S., Toupin S. What does the notion of "sovereignty" mean when referring to the digital? // New Media & Society. 2019. Vol. 21(10). P. 2305–2322.
2. Pohle J., Thiel T. Digital sovereignty // Internet Policy Review. 2020. Vol. 9(4).
3. Schmitt C. Politische Theologie. München: Duncker & Humblot, 1922.
4. Lessig L. Code and Other Laws of Cyberspace. New York: Basic Books, 1999.
5. Zuboff S. The Age of Surveillance Capitalism. New York: PublicAffairs, 2019.
6. Sassen S. Territory, Authority, Rights. Princeton: Princeton University Press, 2006.
7. Habermas J. Die postnationale Konstellation. Frankfurt am Main: Suhrkamp, 1998.
8. Castells M. The Rise of the Network Society. Oxford: Blackwell, 1996.
9. Foucault M. Surveiller et punir. Paris: Gallimard, 1975.
10. Barlow J.P. A Declaration of the Independence of Cyberspace. 1996.

11. Указ Президента Республики Узбекистан № УП-6079 от 05.10.2020 «Об утверждении Стратегии "Цифровой Узбекистан – 2030"».
12. Закон Республики Узбекистан «О персональных данных» от 02.07.2019 г.
13. Закон Республики Узбекистан «О кибербезопасности» от 15.04.2022 г.