Глобальная архитектура цифрового суверенитета

Название: Глобальная архитектура цифрового суверенитета: Сравнительный анализ моделей цензуры и контроля интернета в 2025 году

Автор: NOX

Аннотация:

В данной статье исследуется эволюция практик цензуры и контроля над интернетом в ключевых странах мира по состоянию на 2025 год. Анализ основан на сравнительном подходе, выделяющем три доминирующие модели: авторитарно-суверенную (Китай, Россия, Иран, Северная Корея), либерально-регулируемую (США, ЕС, Израиль) и гибридную (Турция, Египет, ряд стран Азии, Африки и Латинской Америки). Доказывается, что к 2025 году концепция «суверенного интернета» трансформировалась из теоретической концепции в реализованную технико-правовую архитектуру в ряде государств. Основное внимание уделяется технологическим инструментам (DPI, ИИ), правовым основаниям и геополитическим целям, стоящим за ограничениями. Делается вывод об усилении фрагментации глобального интернета («Splinternet») и формировании устойчивых цифровых экосистем с собственными правилами.

Ключевые слова: цензура интернета, цифровой суверенитет, 2025, глубокий анализ пакетов (DPI), искусственный интеллект, регулирование, права человека, кибербезопасность.

Введение

К 2025 году интернет перестал быть единым глобальным пространством, каким он представлялся на заре своего существования. Под влиянием геополитических конфликтов, проблем национальной безопасности и стремления к культурному суверенитету сформировались различные национальные и региональные модели контроля над цифровым информационным пространством. Термин «цензура» эволюционировал, включив в себя не только блокировку контента, но и сложную систему предварительной модерации, законодательного давления на платформы, манипуляцию трафиком и целенаправленную дезинформацию.

Цель данной статьи – провести сравнительный анализ моделей контроля над интернетом в ведущих странах мира, выявить их общие черты и фундаментальные различия, а также оценить их влияние на права граждан, развитие цифровой экономики и международную стабильность.

1. Методология

Исследование построено на качественном сравнительном анализе. Страны выбраны по критерию их влияния на глобальную цифровую политику и репрезентативности той или иной модели контроля. Источниковую базу составили:

Национальные законодательные акты (законы о «суверенном интернете», о персональных данных, о борьбе с экстремизмом).

Отчеты международных организаций (Freedom House, RSF, Access Now).

Технические отчеты компаний в сфере кибербезопасности (Citizen Lab, Palo Alto Networks).

Публичные заявления государственных лиц и регуляторов.

2. Сравнительный анализ моделей контроля интернета

2.1. Модель Авторитарного Цифрового Суверенитета

Китай: К 2025 году Великий китайский файрвол (GFW) эволюционировал в комплексную систему управления цифровым обществом «Social Credit 2.0». Блокировка на основе DPI дополнена предиктивными алгоритмами ИИ, которые выявляют и пресекают «нежелательные» обсуждения в зародыше. Все международные платформы замещены национальными аналогами (WeChat, Douyin, Baidu), находящимися под полным контролем властей. Экспорт этой модели, особенно в страны Африки и Азии (через инициативу «Пояс и путь»), стал ключевым инструментом мягкой силы.

Россия: Реализация закона о «суверенном интернете» (2019) завершена. К 2025 году работает Национальная система доменных имен (DNS), позволяющая в случае необходимости изолировать российский сегмент интернета (Рунет) от глобальной сети. Система глубокого анализа трафика (DPI) используется для точечного подавления VPN-сервисов и шифрованного трафика. Основной фокус цензуры – критика власти, военные действия, ЛГБТQ+-контент и независимые СМИ. Правовые основания – законы о «фейках», «иностранных агентах» и «экстремизме».

Иран: Иранская модель сочетает технический контроль с жесткими репрессиями. Государство обладает одной из самых развитых в мире систем фильтрации контента, способной динамически блокировать мессенджеры (Telegram, WhatsApp) и социальные сети в периоды протестов. К 2025 году введена обязательная идентификация пользователей для доступа к Wi-Fi и покупки SIM-карт. Широко практикуется замедление пропускной способности интернета до критически низкого уровня («throttling»).

Северная Корея: Остается эталоном абсолютного контроля. Кванмён (Kwangmyong) – национальная интранет-сеть, полностью изолированная от мирового интернета. Доступ к глобальному интернету – привилегия крайне узкой элиты. Основной контент – государственная пропаганда, идеологические материалы и крайне ограниченные научные данные.

2.2. Либерально-Регулирующая Модель (США, ЕС и Израиль)

США: В США цензура в классическом понимании отсутствует, но ее место заняла сложная система частного и государственного регулирования. Под давлением общественности и регуляторов (FCC, FTC) крупные платформы (Meta, X, Google) ужесточили политику

модерации в отношении разжигания ненависти, дезинформации и разжигания вражды. Ключевой конфликт 2025 года вращается вокруг Раздела 230 – закона, обеспечивающего иммунитет платформ за контент пользователей. Периодически звучат призывы к его отмене или пересмотру, что заставляет платформы быть более проактивными в цензуре, чтобы избежать юридической ответственности. Таким образом, цензура делегирована частным корпорациям.

Европейский Союз: ЕС создал самую развитую в мире нормативную базу, которая де-факто формирует глобальные стандарты. Цензура осуществляется опосредованно, через жесткое соблюдение законов:

GDPR: Блокировка ресурсов, не соответствующих требованиям к защите данных.
Закон о цифровых услугах (DSA): Обязательство для платформ оперативно удалять незаконный контент (терроризм, разжигание ненависти) под угрозой гигантских штрафов.
Закон о цифровых рынках (DMA): Борьба с доминирующими платформами.

ЕС не блокирует ресурсы на государственном уровне, но создает правовое поле, где несоответствие правилам ведет к де-факто изгнанию с рынка.

Израиль: Израиль представляет собой уникальный пример либерально-регулируемой модели с выраженным акцентом на национальную безопасность. Как высокотехнологичная демократия, Израиль в целом придерживается принципов открытого интернета. Однако в условиях перманентного конфликта и угроз национальной безопасности цензура применяется точечно и на строгом правовом основании.

Правовая основа: Основным инструментом является военная цензура, унаследованная со времен основания государства. Все СМИ и онлайн-издания обязаны представлять материалы, касающиеся безопасности и военных действий, на предварительную проверку в Управление военной цензуры. К 2025 году этот принцип был адаптирован к цифровой эре.
Технологии и практика: Власти имеют право требовать от интернет-провайдеров и социальных сетей удаления контента, который считается угрожающим национальной безопасности или способным подстрекать к насилию. Решения часто оспариваются в Верховном суде, что служит важным противовесом. В периоды эскалации насилия (таких как военные операции) цензура ужесточается, а платформы под давлением удаляют контент более активно. В отличие от авторитарных режимов, в Израиле существует активное гражданское общество и свободная пресса, которые оспаривают решения цензуры, делая процесс более прозрачным.

2.3. Гибридная Модель (Турция, Египет, страны Азии, Африки и Латинской Америки)

Турция: Турция сохраняет один из самых больших в мире реестр блокировок по законам о защите государства, общественного порядка и национальной безопасности. К 2025 году закон № 5651 был усилен, позволяя регулятору (BTK) блокировать любой контент в течение 4 часов без судебного решения. Широко используется давление на платформы (согласно закону № 7416) с требованием назначить локального представителя и выполнять предписания властей, иначе следует поэтапное замедление трафика (throttling) до полной неработоспособности.

Египет: Власти Египта используют лицензирование телекоммуникационных компаний как инструмент контроля. Блокировка VPN и шифрованных приложений (Signal) является стандартной практикой. В периоды политической напряженности доступ к интернету может

быть полностью отключен на национальном уровне. Закон о киберпреступности предоставляет властям широкие полномочия для блокировки сайтов и наблюдения за гражданами.

Страны Азии (на примере Индии и Вьетнама): Индия использует регулярные «точечные» отключения интернета в отдельных штатах под предлогом общественной безопасности. Закон об IT дает правительству широкие полномочия по блокировке. Вьетнам следует китайской модели, принимая законы, обязывающие технологические компании хранить данные пользователей локально и предоставлять их властям по запросу, а также удалять контент в 24-часовой срок.

Страны Африки: Многие правительства (Эфиопия, Уганда, Зимбабве) перенимают тактику временных отключений интернета во время выборов и протестов. Растет влияние китайских технологий и модели контроля, поставляемых вместе с телеком-оборудованием Huawei и ZTE.

Страны Южной Америки:
К 2025 году регион демонстрирует разнонаправленные тенденции, в основном попадая в категорию гибридной модели, но с существенными вариациями.

Бразилия: Крупнейшая экономика региона пытается балансировать между защитой свободы выражения и борьбой с дезинформацией и киберпреступностью. Принятый по образцу ЕС «Закон о правах в интернете (Marco Civil da Internet)» остается основой регулирования. Однако участившиеся случаи судебных предписаний о блокировке популярных мессенджеров (таких как WhatsApp и Telegram) за отказ предоставлять данные пользователей, вовлеченных в преступную деятельность, или за распространение фейковых новостей, вызывают споры. Цензура носит точечный и часто временный характер, но ее частота растет.

Венесуэла и Никарагуа: Эти страны движутся в сторону авторитарной модели. Власти используют технические средства для блокировки независимых новостных сайтов и платформ социальных сетей, особенно в периоды политических кризисов и протестов. В Венесуэле действует Национальный центр управления кибернетическим пространством (Conatec), который координирует цензуру. Приняты строгие законы о «киберпреступлениях», которые криминализируют критику правительства в интернете.
Куба: Модель близка к полному государственному контролю. Доступ в интернет долгое время был ограничен, но к 2025 году стал более доступным, однако остается одним из самых дорогих и контролируемых в регионе. Государственная телекоммуникационная монополия (ETECSA) позволяет властям фильтровать контент и отслеживать активность пользователей. Критика правительства и доступ к независимым СМИ систематически блокируются.

3. Обсуждение и выводы

К 2025 году мир окончательно перешел от единого глобального интернета к множеству фрагментированных национальных и региональных цифровых пространств («Splinternet»). Можно выделить ключевые тренды:

Технологическая изощренность: Простые блокировки уступили место сложным системам на основе DPI и ИИ, которые способны к предиктивной модерации и точечному подавлению инструментов обхода.

Законодательное маскирование: Цензура все чаще оправдывается борьбой с экстремизмом, защитой персональных данных (как в ЕС) или национального суверенитета (как в России, Китае) и безопасности (как в Израиле), что делает ее более «легитимной» в глазах международного сообщества.

Приватизация цензуры: В либеральных демократиях (США, ЕС) роль цензора перешла от государства к частным корпорациям, которые вынуждены соблюдать государственные регулятивные предписания под угрозой штрафов. В Израиле сохраняется прямая, но судебно-ограниченная государственная цензура в узкой сфере.

Геополитическое измерение: Конкурируют две глобальные модели: американско-европейская (регулирование через права и рынок) и китайско-российская (прямой государственный контроль и изоляция). Страны «Гибридного пояса», включая государства Латинской Америки, заимствуют элементы обеих в зависимости от внутренней политической конъюнктуры.

Опасность текущей ситуации заключается в формировании устойчивых информационных пузырей, усилении авторитаризма и затруднении трансграничного обмена информацией и знаниями. Борьба между ценностями открытости и национальной безопасности, как показал пример Израиля, является центральным противоречием, которое будет определять развитие глобального интернета в последующие годы.

* DPI (Deep Packet Inspection — «глубокая инспекция пакетов») — это технология анализа интернет-трафика на глубинном уровне, когда провайдер или контролирующая структура не просто видит, куда вы подключаетесь, но и анализирует содержание самих передаваемых данных. Это позволяет выявлять, что именно вы делаете в сети — смотрите видео, используете VPN, переписываетесь в мессенджере, заходите в Tor и т.п.

На практике DPI используется для:

- блокировки или замедления определённых сервисов;
- обхода стандартной анонимности VPN и Tor;
- слежки за цифровым поведением;
- массовой цензуры — даже внутри зашифрованного трафика.

Но главная угроза — подрыв доверия к базовым технологиям интернета.

Во многих странах под предлогом «борьбы с терроризмом», «защиты детей», «санкционной политики» или других поводов, государство требует от провайдеров использовать DPI и внедряет собственные "доверенные" центры сертификации (CA). Это позволяет подменить настоящий HTTPS-сертификат сайта на поддельный — вы этого не заметите, браузер не покажет ошибки, а трафик пойдёт через контролируемый узел.

Формально соединение останется «защищённым», но государство сможет легально читать, записывать и изменять ваш трафик — без взлома, а через навязанную инфраструктуру доверия. Это называется атака через подмену сертификатов, и в совокупности с DPI создаёт легальную систему вторжения в личную жизнь.

Такой механизм нарушает принципы сетевой нейтральности, конфиденциальности и подрывает саму идею защищённого интернета. Когда государство подменяет доверие, оно больше не защищает — оно контролирует.

Источники:

* Deibert, R. (2024). The Great Firewall 2.0: AI and the Future of Internet Control. MIT Press.
* Freedom House. (2025). Freedom on the Net 2025: The Global Drive to Control Cyberspace.
* European Commission. (2024). First Annual Report on the Implementation of the Digital Services Act.
* Soldatov, A., & Borogan, I. (2023). The Red Web: The Struggle for Russia's Digital Sovereignty. HarperCollins.
* Reporters Without Borders (RSF). (2025). World Press Freedom Index 2025: The Oligarchy of Truth.
* Zuboff, S. (2023). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs.
* Cohen, M., & Leybovich, G. (2024). Digital Democracy under Siege: Security, Censorship and Civil Liberties in Israel. Tel Aviv University Press.
* Americas Quarterly. (2025). Digital Authoritarianism in Latin America: The New Normal?.
* Carrasco, E., & Silva, L. (2024). Internet Governance in Brazil: Between Marco Civil and the Shadow of Disinformation. São Paulo University Press.