

WeChat и китайская модель цифрового суверенитета: эволюция политики конфиденциальности

Научный руководитель – Павлюченко Александра Андреевна

Дарчева Виктория Романовна

Студент (бакалавр)

Московский государственный университет имени М.В.Ломоносова, Факультет мировой политики, Кафедра информационного обеспечения внешней политики, Москва, Россия

E-mail: yakadsuna@gmail.com

Настоящее исследование обращается к проблеме трансформации цифрового суверенитета в условиях, когда частные технологические платформы превращаются в инструменты реализации государственной политики. Актуальность работы обусловлена двумя факторами: во-первых, глобальным усилением контроля над персональными данными и формированием альтернативных западным моделям интернет-управления; во-вторых, отсутствием в академическом дискурсе комплексных исследований, прослеживающих эволюцию конкретных цифровых платформ в контексте становления китайской модели киберсуверенитета. Цель исследования — проанализировать трансформацию политики конфиденциальности WeChat в контексте изменений законодательства КНР в сфере кибербезопасности и защиты персональных данных с 2011 по 2025 год.

Корпус анализа включает три типа источников: первичные (редакции политик конфиденциальности WeChat 2011–2025 гг., ключевые законы КНР о цифровом пространстве 2017–2025 гг. и связанные судебные решения); технические (отчёты независимой исследовательской организации Citizen Lab [1], фиксирующие аспекты цензуры и отслеживания в работе платформы); вторичные научные исследования, содержащие анализ кейсов интеграции WeChat в государственные сервисы и правоприменительной практики. В работе применяются сравнительно-правовой анализ, хронологический метод, а также анализ первичных источников (законодательных актов, официальных политик конфиденциальности и стратегических документов китайского правительства).

Анализ концептуальных основ китайской модели регулирования выявил принципиальное расхождение с западными подходами. Если в европейской традиции (GDPR) цифровой суверенитет трактуется через призму прав человека и контроля индивида над своей цифровой идентичностью [3], то введённый председателем Си Цзиньпином в 2015 году термин «киберсуверенитет» ([U+7F51] [U+7EDC] [U+4E3B] [U+6743]) закрепляет неотъемлемое право государства устанавливать правила функционирования интернета на своей территории исходя из национальной безопасности и социальной стабильности [7]. Эта концепция получила практическое воплощение в трёх ключевых законодательных актах: Законе «О кибербезопасности» (2017), вводящем локализацию данных и обязательства по сотрудничеству IT-компаний с органами госбезопасности [10]; Законе «О защите персональных данных» (2021), где защита информации подчинена интересам государства и допускает её обработку для выполнения государственных функций [3]; Законе «О безопасности данных» (2021), установившем категоризацию информации по степени важности [6]. Дальнейшее усиление контроля продолжилось в 2022–2023 годах через регулирование алгоритмических рекомендаций и генеративного ИИ, требующее соответствия всего контента социалистическим ценностям.

Хронологический анализ эволюции политики конфиденциальности WeChat позволил выделить три отчётливых этапа трансформации. На раннем этапе (2011–2016) политики носили преимущественно рыночный характер с фокусом на персонализацию сервисов, а

различия между внутренней и международной версиями были минимальны [4]. Переломным моментом стал этап адаптации (с июня 2017), когда после вступления в силу Закона «О кибербезопасности» в политиках впервые появились положения о возможности раскрытия данных компетентным органам без уведомления пользователя в целях национальной безопасности, а также началась систематическая дифференциация внутренней и международной версий [4]. На этапе системной интеграции (с 2021) принятие Закона «О защите персональных данных» [9] закрепило понятия «национальная безопасность» и «общественные интересы» как законные основания для обработки данных без согласия пользователя [4]. При этом статья 38 PIPL и статья 21 Закона о безопасности данных юридически оформили разделение версий: для внутренних пользователей данные хранятся исключительно на территории КНР, а для международных применяется дифференцированное регулирование [6].

Исследование демонстрирует, что WeChat превратился из коммерческого мессенджера в инструмент реализации государственной политики цифрового суверенитета. Компания Tencent выступает стратегическим партнёром государства в обеспечении внутренней стабильности: данные внутренней версии «Вэйсинь» хранятся в китайских ЦОДах и доступны госорганам по запросу; платформа интегрирована в систему цифрового госуправления (госуслуги, цифровая идентификация через WeChat Real-Name Authentication) [4]; контент-модерация осуществляется в соответствии с чёрными списками Государственной канцелярии интернет-информации КНР (САС) [1]. Реакция международного сообщества на такую интеграцию (попытки запрета в США [2], блокировка в Индии [5], рекомендации к неиспользованию в Австралии [8]) подтверждает, что граница между версиями WeChat становится не технической, а идентификационной: решающим фактором выступает «цифровая принадлежность» к КНР.

Источники и литература

- 1) Wang M., Lin P., Knockel J. Should We Chat? Privacy in the WeChat Ecosystem // The Citizen Lab. 2023. Режим доступа: <https://citizenlab.ca/2023/06/privacy-in-the-wechat-ecosystem-full-report/> (дата обращения: 07.03.2026);
- 2) Суд в США заблокировал решение об удалении WeChat с платформ Google и Apple // Коммерсантъ. 2020. 20 сент. Режим доступа: <https://www.kommersant.ru/doc/4500430> (дата обращения: 07.03.2026);
- 3) Гун Н. Защита персональных данных в Китае: законодательство в цифровую эпоху // Вестник Санкт-Петербургского университета. Право. 2023. Т. 14, № 1. Режим доступа: <https://lawjournal.spbu.ru/article/view/12724> (дата обращения: 05.03.2026);
- 4) WECHAT – Условия использования. 2025. 11 июн. Режим доступа: https://www.wechat.com/ru/service_terms.html (дата обращения: 05.03.2026);
- 5) В Индии запретили TikTok и WeChat // РИА Новости. 2020. 29 июня. 19:14. Режим доступа: <https://ria.ru/20200629/1573647699.html> (дата обращения: 06.03.2026);
- 6) Закон КНР о безопасности данных. 2021. 20 авг. Научно-технический центр ФГУП «ГРЧЦ». Режим доступа: https://rdc.grfc.ru/2021/08/zakon_o_bezopasnosti_knr/ (дата обращения: 07.03.2026);
- 7) Михалеви́ч А.А. Концепция киберсуверенитета Китайской Народной Республики: история развития и сущность // Вестник Российского университета дружбы народов. Серия: Политология. 2021. Режим доступа: <https://www.elibrary.ru/item.asp?id=46153801> (дата обращения: 06.03.2026);

- 8) Хакеры взломали учетную запись премьера Австралии в соцсети WeChat // РИА Новости. 2022. 24 янв. Режим доступа: <https://ria.ru/20220124/avstraliya-1769197961.html> (дата обращения: 07.03.2026);
- 9) Садовников Д. Обзор закона КНР О защите персональной информации (Personal Information Protection Law of the People's Republic of China (PIPL)) // zakon.ru. 2021. 17 сент. Режим доступа: https://zakon.ru/blog/2021/9/17/obzor_zakona_knr_o_zaschite_personalnoj_informacii_personal_information_protection_law_of_the_peoples (дата обращения: 06.03.2026);
- 10) Балакин Д.А., Аликберова А.Р. Особенности Закона о кибербезопасности Китайской Народной Республики 2017 г. И международная реакция на его принятие // Современные востоковедческие исследования. 2023.