УДК 316

В.Р. Дарчева

WeChat и китайская модель цифрового суверенитета: эволюция политики конфиденциальности

Аннотация:

Анализируется трансформация политики конфиденциальности мессенджера WeChat в контексте эволюции национального киберзаконодательства Китайской Народной Республики 2011-2025 гг. По мере усиления китайского законодательства в области кибербезопасности платформа Tencent все больше вписывается в архитектуру цифрового суверенитета, где индивидуальные права могут быть ограничены в пользу интересов национальной и социальной стабильности. Показано, как из коммерческого мессенджера WeChat превратился в многофункциональную платформу, глубоко интегрированную в систему цифрового управления, контроля и идентификации. В будущем подобный подход может быть экстраполирован и на другие сферы – от ИИ до финансовых технологий, – что делает актуальным его дальнейшее исследование в условиях глобального пересмотра норм цифрового управления.

Ключевые слова: WeChat, киберзаконодательство КНР, политика конфиденциальности, цифровой суверенитет, защита персональных данных, национальная безопасность, Tencent, социальная инженерия данных, китайская модель интернет-управления.

Об авторе: Дарчева Виктория Романовна, МГУ им. М.В. Ломоносова, студент факультета мировой политики; эл. почта: victoriadarceva@gmail.com

Научный руководитель: Павлюченко Александра Андреевна, МГУ им. М.В. Ломоносова, старший преподаватель кафедры информационного обеспечения внешней политики; эл. почта: alexa.pavlyuchenko@gmail.com

Введение

Цифровые платформы все чаще становятся не только инструментами коммуникации, но и акторами глобальной политики, формирующими новые режимы управления информацией и данными. В этой связи особое внимание заслуживает Китайская Народная Республика (далее – КНР), где государство последовательно реализует стратегию цифрового суверенитета, встраивая частные технологические компании в систему национального управления и обеспечения безопасности. Эта программа проявляется не только в законодательных инициативах, но и в самой архитектуре цифровых сервисов: один и тот же продукт может функционировать по разным правилам в зависимости от того, кому он адресован. Ярким примером служит мессенджер WeChat, разработанный компанией Tencent, – всемирно известной платформой, осуществляющей курс национальной защиты данных, их интеграции с государственными органами. Платформа существует в двух юрисдикционных форматах: как инструмент повседневной жизни внутри КНР, ставящий в приоритет национальную безопасность и государственный контроль, и как международное приложение для пользователей за пределами страны [12]. На фоне глобального усиления контроля над персональной информацией и защищенности от вмешательства «внешних» нарративов КНР формирует принципиально иной подход, в котором защита цифровых данных тесно связана с национальной безопасностью и стабильностью общества.

Правовые основы регулирования данных в КНР: от кибербезопасности к цифровому суверенитету

В последние годы КНР последовательно выстраивает собственную модель регулирования цифрового пространства, в центре которой национальный контроль над данными, информационной инфраструктурой и технологическим развитием. Эта стратегия, получившая название «китайского цифрового суверенитета», основана на приоритете государственных интересов над индивидуальными правами и принципиально отличается от западных подходов, номинально ориентированных на защиту личной автономии и приватности.

Понятие «цифровой суверенитет» впервые было введено во французском политическом дискурсе: в 2012 г. бизнесмен П. Белланжер определил его как «контроль над сегодняшним днем и нашей общей судьбой, которые являют себя и формируются через применение технологий и компьютерных сетей» [18]. В новейшем понимании термин означает способность государства защищать телекоммуникационную инфраструктуру,

персональные и корпоративные данные, а также самостоятельно определять направление информационной политики и развитие ключевых технологий в соответствии с национальными интересами [8].

В европейской традиции трактовка понятия «цифровой суверенитет» тесно связана с правами человека: акцент делается на контроле отдельного гражданина над своей цифровой идентичностью, защите от неконтролируемого сбора данных и манипуляции. Эта парадигма нашла отражение, в частности, в Общем регламенте по защите данных (GDPR), вступившем в силу в мае 2018 г. Закон закрепил за физическими лицами в ЕС расширенные права в отношении их персональных данных [9]. Среди них – право на доступ к своим данным, право на их исправление и удаление («право на забвение»), право на переносимость данных, а также право возражать против автоматизированного принятия решений, включая профилирование. Регламент требует от организаций получать четкое, информированное и добровольное согласие на обработку данных, обеспечивать прозрачность целей сбора и гарантировать безопасность хранения информации.

В Китае же сложился иной подход: в ноябре 2014 г. председателем Си Цзиньпином во время выступления на открытии Первой Всемирной интернет-конференции в Учжэне был употреблен термин «киберсуверенитет», впоследствии вошедший в академический и дипломатический дискурс. Согласно этой концепции, каждое государство имеет неотъемлемое право устанавливать правила функционирования интернета на своей территории, исходя из соображений национальной безопасности, социальной стабильности и культурных особенностей. Цифровое пространство рассматривается не как сфера реализации личных свобод, а как стратегическая зона, подлежащая государственному контролю и защите от внешнего влияния. Практическое воплощение этому нашлось в системе нормативного регулирования, формирование которой началось в 2016 г. и получило развитие в ключевых законодательных актах последующих лет.

Так, первым значимым шагом стало вступление в силу в 2017 г. Закона «О кибербезопасности», ставшего поворотным моментом в киберполитике КНР. Закон ввел обязательную локализацию критически важных данных на территории Китая и обязал операторов информационной инфраструктуры, включая крупные IT-компании, сотрудничать с органами государственной безопасности, предоставляя им доступ к данным в случае национальной угрозы [10; 5].

Следующий этап пришелся на 2021 г., когда были приняты два фундаментальных закона – Закон «О защите персональных данных» и Закон «О безопасности данных». Первый внешне схож с европейским GDPR, однако на деле имеет национальную специфику: защита данных напрямую подчинена интересам государства. Обработка персональной информации допускается без согласия субъекта, если она необходима для выполнения государственных функций или обеспечения национальной безопасности [15]. Второй закон, в свою очередь, установил категоризацию информации по степени важности и обязал организации проводить оценку связанных рисков [1].

В 2022 г. утверждены «Положения о регулировании алгоритмических рекомендаций», обязавшие платформы раскрывать принципы работы своих алгоритмов и запретившие рекомендации, способные подорвать социальную стабильность. В 2023 г. начали активно применяться положения об управлении службами генеративного ИИ, требующие соответствия инструмента коммунистическим ценностям и положениям национальной безопасности. Кроме того, в это же время вступили в силу меры по управлению безопасностью крупных моделей ИИ – обязательная государственная сертификация и аудит всех фундаментальных ИИ-моделей [11; 2].

Подобная законодательная динамика отражается соответствующими стратегическими государственными документами. В частности, «14-й пятилетний план социально-экономического развития Китайской Народной Республики на 2021-2025 годы и долгосрочные цели до 2035 года» закрепляет курс на «высококачественное развитие» цифровой экономики, технологическое самообеспечение и всестороннее укрепление базы собственных, особых нарративов, защищенных от влияния «извне» [11]. В документе освещается необходимость снижения зависимости от иностранных технологий в критических сферах – от полупроводников и операционных систем до искусственного интеллекта и квантовых вычислений. Иначе говоря, фокус смещается к формированию автономной цифровой инфраструктуры: развитию сетей 5G, центров обработки данных, облачных платформ и систем управления большими данными. Роль государства четко обозначена как гаранта информационной безопасности, регулятора потоков данных и барьера против внешнего вмешательства в цифровое пространство.

Реализация «китайской модели интернет-управления» обеспечивается не только законодательством, но и четкой институциональной архитектурой: главную роль в координации цифровой политики играет Государственная канцелярия интернет-

информации КНР (Cyberspace Administration of China, CAC), находящаяся под прямой юрисдикцией Руководящей группы ЦК КПК по информатизации и безопасности в Интернете. Именно эта структура отвечает за выработку стратегических директив, утверждение технических стандартов и контроль за исполнением решений на всех уровнях управления – от центральных органов власти до местных провинциальных управлений. Такая вертикаль обеспечивает высокую степень согласованности между идеологическими установками, нормативным регулированием и практическим контролем над цифровой экосистемой [13].

Эволюция политики конфиденциальности WeChat как элемента стратегии национальной безопасности

Изначально WeChat позиционировался как коммерческий продукт – мессенджер, разработанный Алленом Джаном и названный «Вэйсинем». Однако уже к середине 2010-х гг. платформа превратилась в «суперапп», интегрированный в повседневную жизнь миллионов граждан КНР. Сегодня WeChat объединяет функции мгновенных сообщений, электронных платежей, заказа такси, доступа к государственным услугам, бронирования билетов, а также выступает инструментом цифровой идентификации. В условиях пандемии COVID-19 платформа стала ключевым элементом системы общественного контроля – через специальные коды пользователи подтверждали свое здоровье и право на перемещение [7].

Уже с первых лет существования WeChat Tencent разделила его на две версии – внутреннюю (разработана для граждан КНР и оставила изначальное название «Вэйсин») и международную (WeChat для зарубежных рынков). Эта дифференциация изначально носила маркетинговый характер и была направлена на адаптацию интерфейса и функционала под локальные потребности. Однако с 2016-2017 гг., по мере укрепления регулирования в КНР, техническое и правовое размежевание между версиями стало систематическим и нормативно обусловленным [22]. Эта трансформация нашла отражение и в политике конфиденциальности платформы, которая прошла несколько четко различимых этапов эволюции в соответствии с меняющейся нормативно-правовой средой Китайской Народной Республики.

Так, в ранний период 2011-2016 гг. политики конфиденциальности носили преимущественно рыночный характер. Основное внимание уделялось сбору данных для персонализации сервисов, таргетированной рекламы и улучшения пользовательского опыта. Упоминания о взаимодействии с государственными органами либо отсутствовали,

либо были минимальными. Например, в версии политики 2012 г. отмечалось, что данные могут быть переданы «только в рамках деловых отношений с партнерами» и «только с согласия пользователя». В этот период различия между внутренней и международной версиями WeChat были минимальны: обе подчинялись общим корпоративным стандартам Tencent, направленным на глобальную экспансию.

Второй этап (июнь 2017 – конец 2020 гг.) связан с вступлением в силу Закона КНР «О кибербезопасности». Tencent, как материнская компания WeChat, была обязана пересмотреть подходы к обработке персональных данных. В политиках конфиденциальности с 2018 г. впервые появились положения, говорящие о возможности раскрытия персональных данных пользователя компетентным органам без предварительного уведомления в целях защиты национальной безопасности. Одновременно началась дифференциация политик: для пользователей внутри КНР формулировки стали строже и прямолинейнее, тогда как международная версия продолжала использовать более мягкие и «интернациональные» формулировки в соответствии с ожиданиями глобальных рынков.

Наконец, этап системной интеграции государственных интересов (с 2021 г.) характеризуется принятием Закона «О защите персональных данных», ставший катализатором глубокой перестройки корпоративных практик управления данными [15]. Политики WeChat были существенно скорректированы: в них все чаще стали фигурировать такие понятия, как «национальная безопасность», «общественные интересы» и «соблюдение законодательства» (как законные основания для обработки, хранения и передачи данных без получения специального согласия пользователя). Акцент на прозрачность и информированность пользователей постепенно ослабевает, однако сотрудничество с государственными структурами становится не просто допустимым, а нормативно предписанным элементом корпоративной ответственности. Начиная с 2021 г., Tencent официально закрепила разделение WeChat на две версии [14]. В частности, статья 38 Закона «О защите персональных данных» обязывает операторов, обрабатывающих данные граждан КНР, применять особые меры защиты и ограничивать трансграничную передачу информации, а статья 21 Закона «О безопасности данных» вводит требование дифференцированного регулирования в зависимости от юрисдикции пользователя [3; 19].

Таким образом, с 2011 по 2025 гг. автономия частного сектора в вопросах управления пользовательскими данными последовательно сокращается, иностранное

влияние всевозможно пресекается, а роль государства как конечного субъекта контроля над цифровой информацией неуклонно усиливается. Особенно показательны изменения в формулировках, касающихся передачи данных третьим лицам. Если в ранних редакциях речь шла преимущественно о партнерах, рекламодателях и сервис-провайдерах, то в актуальных версиях прямо и недвусмысленно указывается, что персональные данные могут быть предоставлены «органам государственной власти в соответствии с требованиями законодательства КНР» – без оговорок, условий или прозрачных процедур уведомления пользователя. Такая трансформация демонстрирует не столько формальную юридическую адаптацию, сколько более глубокую институциональную интеграцию цифровых платформ в систему государственного управления, что становится характерной чертой современной модели цифрового суверенитета в Китае.

WeChat как инструмент реализации государственной политики цифрового суверенитета

Компания Tencent, несмотря на частную форму собственности, оказывается одним из ключевых акторов в «национальной цифровой экосистеме» Китая. Государство рассматривает подобных технологических гигантов как стратегических партнеров в обеспечении внутренней стабильности и технологического суверенитета. Такая модель даже закреплена в законодательстве: согласно Закону КНР О кибербезопасности (2017 г.), все операторы критической информационной инфраструктуры, включая Tencent, обязаны хранить персональные данные пользователей исключительно на территории КНР и обеспечивать их доступность для уполномоченных государственных органов по запросу. Это требование напрямую повлияло на структуру WeChat: данные внутренней версии «Вэйсинь» хранятся в китайских ЦОДах, тогда как международная версия может использовать облачные ресурсы за пределами КНР, но при этом подлежит мониторингу на предмет соответствия «идеологическим нормам» в случае связи с китайскими пользователями [5].

WeChat активно интегрирован в систему цифрового государственного управления: с 2020 г. платформа используется для предоставления госуслуг через официальные аккаунты ведомств (например, Министерства общественной безопасности или Налоговой службы), а также для реализации программ цифровой идентификации – в частности, через систему WeChat Real-Name Authentication, которая обязывает пользователей проходить верификацию по паспорту КНР и доступна только в версии «Вэйсинь», что подчеркивает

границы между внутренним и внешним цифровыми пространствами. Следовательно, даже пользователи в ЕС или США могут подвергаться модерации, если их аккаунт исторически связан с китайским номером или IP-адресом. Это делает границу между версиями WeChat не технической, а идентификационной: решающим фактором становится не текущее местоположение, а «цифровая принадлежность» к КНР.

Контент-модерация в WeChat осуществляется в соответствии с требованиями Государственной канцелярии интернет-информации КНР (CAC): платформа автоматически блокирует или удаляет сообщения, содержащие ключевые слова, связанные с «подрывом государственной власти», «сепаратизмом» или «клеветой на руководство страны» [13]. По данным исследований Citizen Lab (2020, 2023 гг.), алгоритмы цензуры WeChat обучаются на основе черных списков, обновляемых государственными регуляторами, и применяются как внутри КНР, так и за ее пределами – в зависимости от регистрации аккаунта [21; 20].

Международное сообщество, особенно страны с иной моделью цифрового управления, воспринимает такую интеграцию как угрозу национальной безопасности, что приводит к соответствующим ограничительным мерам. В 2020 г. администрация президента США Д. Трампа попыталась запретить WeChat на основании указа о «недопустимом риске для национальной безопасности», связанным с возможной передачей данных китайским спецслужбам. Однако запрет так и не вступил в силу: федеральный суд приостановил его действие, а администрация Дж. Байдена отказалась от реализации в 2021 г. [16; 4]. В Индии приложение было заблокировано в 2020 г. вместе с 58 другими китайскими сервисами после обострения пограничного конфликта между двумя странами [6]. В Австралии парламентские комитеты рекомендовали чиновникам и военным не использовать WeChat из-за рисков утечки данных [17].

Вместе с тем внутри КНР платформа пользуется огромным спросом и полным доверием со стороны населения. С каждым годом число пользователей растет, а WeChat получает все больше возможностей для интеграции в повседневную жизнь граждан. Благодаря тесной координации с регуляторами и соблюдению национальных норм в области кибербезопасности, WeChat непрерывно укрепляет роль ключевого игрока цифровой трансформации Китая.

Таким образом, политика конфиденциальности платформы WeChat трансформировалась годами, однако не под давлением рыночной конкуренции или международных стандартов, а под прямым влиянием системных изменений в

киберзаконодательстве КНР. От коммерческого мессенджера WeChat превратился в многофункциональную платформу, глубоко интегрированную в систему цифрового управления, контроля и идентификации. Ключевым элементом этой трансформации послужило институциональное и юридическое закрепление дуальной структуры приложения – разделение на «Вэйсинь» для КНР и международную версию стало неотъемлемой частью национальной стратегии цифрового суверенитета. В отличие от западной модели, в которой конфиденциальность трактуется как право индивида, китайская модель рассматривает ее как условие стабильности, безопасности и суверенитета государства. WeChat служит ярким примером реализации этой логики на практике: платформа не просто подчиняется законодательству – она становится его инструментом.

Библиографический список:

1. Бажанов П. Закон КНР «О безопасности данных»: краткий обзор // CNLegal. 2021. URL: https://cnlegal.ru/china_economic_law/china_data_security_law_2021/ (дата обращения: 09.12.2025).

2. Бажанов П. Опубликованы правила регулирования генеративного ИИ в КНР // CNLegal. URL: https://cnlegal.ru/china_economic_law/china_generative_ai_2023/ (дата обращения: 10.12.2025).

3. Бажанов П. Сертификация охраны персональных данных в КНР // CNLegal. URL: https://cnlegal.ru/china_economic_law/personal_info_certification_2022/ (дата обращения: 08.12.2025).

4. Байден снял запрет с TikTok и WeChat в США. Таймлайн сложных отношений // РБК. URL: https://www.rbc.ru/quote/news/article/60c0f4029a79477f2057adcb (дата обращения: 08.12.2025).

5. Балакин Д.А. Особенности Закона о кибербезопасности Китайской Народной Республики 2017 г. и международная реакция на его принятие / Д.А. Балакин, А.Р. Аликберова // Современные востоковедческие исследования. 2023. Т. 5, № 2. С. 152-163.

6. В Индии запретили TikTok и WeChat // РИА Новости. URL: https://ria.ru/20200629/1573647699.html (дата обращения: 09.12.2025).

7. В Китае запускают «паспорта здоровья» для путешественников // CGTN. URL: https://russian.cgtn.com/n/BfJEA-cA-HAA/DaeHAA/index.html (дата обращения: 07.12.2025).

8. Володенков С.В. Цифровой суверенитет современного государства в условиях технологических трансформаций: содержание и особенности / С.В. Володенков, А.С. Воронов, Л.С. Леонтьева, М. Сухарева // Полилог/Polylogos. 2021. Т. 5, № 1. URL: https://polylogos-journal.ru/s258770110014073-2-1/ (дата обращения: 05.05.2026).

9. Гун Н. Защита персональных данных в Китае: законодательство в цифровую эпоху // Вестник Санкт-Петербургского университета. Право. 2023. Т. 14, № 1. URL: https://lawjournal.spbu.ru/article/view/12724 (дата обращения: 05.12.2025).

10. Закон КНР о безопасности данных // Научно-технический центр ФГУП «ГРЧЦ». URL: https://rdc.grfc.ru/2021/08/zakon_o_bezopacnocti_knr/ (дата обращения: 07.12.2025).

11. Кашин В.Б. Китайские эксперты о новом пятилетнем плане КНР: аналитическая записка / В.Б. Кашин, А.С. Пятачкова, В.А. Смирнова [и др.] // Центр комплексных европейских и международных исследований, НИУ ВШЭ, 2021. 25 с.

12. Михалевич Е.А. Концепция киберсуверенитета Китайской Народной Республики: история развития и сущность // Вестник Российского университета дружбы народов. Серия: Политология. – 2021. Т. 23, № 2. С. 254-264.

13. Мок Э. «Супердракон», укрощающий наводнение: почему Управление по вопросам киберпространства Китая стало играть глобальную роль / Э. Мок, Ц. Хао // Клуб «Валдай». URL: https://ru.valdaiclub.com/a/highlights/superdrakon-ukroshchayushchiy-navodnenie/ (дата обращения: 10.12.2025).

14. Сабанцев А. WeChat против Weixin // China Digital. 2023. URL: https://china-digital.com/blogs/wechat-vs-weixin-main-differences/ (дата обращения: 10.12.2025).

15. Садовников Д. Обзор закона КНР О защите персональной информации (Personal Information Protection Law of the People’s Republic of China (PIPL)) // Zakon.ru. URL: https://zakon.ru/blog/2021/9/17/obzor_zakona_knr_o_zaschite_personalnoj_informaciipersonal_information_protection_law_of_the_peoples (дата обращения: 09.12.2025).

16. Суд в США заблокировал решение об удалении WeChat с платформ Google и Apple // Коммерсант. URL: https://www.kommersant.ru/doc/4500430 (дата обращения: 07.12.2025).

17. Хакеры взломали учетную запись премьера Австралии в соцсети WeChat // РИА Новости. URL: https://ria.ru/20220124/avstraliya-1769197961.html (дата обращения: 07.12.2025).

18. Bellanger P. De la souveraineté numérique // Le Débat. 2012. Vol. 170, No. 3. P. 149-159.

19. Data Security Law of the People's Republic of China // The National People's Congress of the People's Republic of China. URL: http://www.npc.gov.cn (дата обращения: 10.12.2025).

20. Knockel J. We Chat, They Watch. How International Users Unwittingly Build up WeChat's Chinese Censorship Apparatus / J. Knockel, C. Parsons, L. Ruan (et al) // The Citizen Lab. URL: https://citizenlab.ca/2020/05/we-chat-they-watch/ (дата обращения: 06.12.2025).

21. Wang M. Should We Chat? Privacy in the WeChat Ecosystem / M. Wang, P. Lin, J. Knockel // The Citizen Lab. URL: https://citizenlab.ca/2023/06/privacy-in-the-wechat-ecosystem-full-report/ (дата обращения: 07.12.2025).

22. WECHAT – Условия использования. URL: https://www.wechat.com/ru/service_terms.html (дата обращения: 05.12.2025).

Darcheva V.R. **WeChat and the Chinese Model of Digital Sovereignty: the Evolution of Privacy Policy**

The transformation of the privacy policy of the WeChat messenger is analyzed in the context of the evolution of the national cyber legislation of the People's Republic of China 2011-2025. As Chinese cybersecurity legislation strengthens, the Tencent platform increasingly fits into the architecture of digital sovereignty, where individual rights can be limited in favor of the interests of national and social stability. It shows how WeChat has transformed from a commercial messenger into a multifunctional platform deeply integrated into a digital management, control and identification system. In the future, this approach may be extrapolated to other areas, from AI to financial technology, which makes it relevant to further explore it in the context of a global revision of digital governance standards.

Keywords: WeChat, Chinese cyber law, privacy policy, digital sovereignty, personal data protection, national security, Tencent, social data engineering, Chinese Internet governance model.