Мессенджер Max и статья 23 Конституции РФ: Конституционные проблемы и государственные цели

Прямой ответ на основной вопрос

Да, мессенджер Max нарушает или может нарушать статью 23 Конституции РФ по нескольким аспектам, хотя государство формально утверждает обратное. Критическим является не просто существование приложения, а его **архитектура, навязывание и интеграция с государственной инфраструктурой**, которые создают механизм для систематического контроля над коммуникациями граждан.

Текст статьи 23 и его требования

Статья 23 Конституции РФ гарантирует: «Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени... Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения».[1] [2]

Норма содержит два критических элемента: **безусловное право на секретность коммуникаций** и **ограничение этого права исключительно судебным решением**, а не административным или ведомственным приказом.

Анализ нарушений статьи 23

1. Проблема шифрования и доступа государства

Критическое отличие от международных стандартов: Max использует **сквозное шифрование только на уровне канала между пользователем и сервером**, но не между пользователями. Это означает, что сам сервер (контролируемый государством через VK) может в полной мере прочитать все сообщения.[3]

Для сравнения:

- **WhatsApp** использует сквозное шифрование по умолчанию (пользователь → пользователь)[4]
- **Signal** применяет end-to-end encryption с криптографическим "рачетингом" для каждого сообщения[4]
- **Telegram** предлагает сквозное шифрование в "секретных чатах" по выбору[4]

- **Max** нарушает этот стандарт и использует **FSB-одобренное шифрование**, которое оставляет сообщения доступными для государственных органов[5]

Как это нарушает статью 23: Статья 23 гарантирует тайну переписки. Если технически государство может прочитать любое сообщение без судебного решения (через архитектуру приложения), то тайна переписки фактически устранена, хотя формально право остается.

2. Сбор данных без надлежащего ограничения

Политика конфиденциальности Max явно предусматривает сбор:[6] [7]

- IP-адресов
- Геолокации
- Списков контактов
- Логов вызовов
- Поведенческих метрик
- Биометрических данных

Критически: политика **явно допускает передачу этих данных государственным органам и третьим лицам**.[7] [8] [6]

Нарушение статьи 23: Статья 24 Конституции (тесно связана со статьей 23) запрещает сбор информации о частной жизни без согласия. Max собирает данные в масштабах, превышающих необходимое, а его положения о передаче данных ослабляют правовую защиту.[9]

3. Отсутствие судебного контроля при доступе

Max интегрирован с **системой СОРМ-3** (Система оперативно-розыскных мероприятий). СОРМ-3 позволяет ФСБ и другим органам **автоматически и в реальном времени собирать данные о коммуникациях** без судебного решения в каждом конкретном случае.[10] [5]

Хотя Федеральный закон "Яровая" (№ 374-ФЗ) требует, чтобы провайдеры хранили данные и предоставляли ключи, **судебное решение должно быть выполнено в каждом отдельном случае**, а не в целом для платформы.[8]

Нарушение статьи 23: По буквальному тексту статьи, даже законная перлюстрация (выполнение судебного решения) не должна быть "встроена в архитектуру" приложения. Max создает систему, где государство имеет постоянный технический доступ без необходимости подтверждать судебное решение в каждом случае.

4. Деанонимизация через интеграцию с Госуслугами

Max связан с **цифровым ID** и порталом **Госуслуги**. Это означает, что каждое сообщение в Max может быть соединено с:[11] [12] [13]

- Реальным именем пользователя
- Паспортными данными
- Адресом проживания
- Другой идентификационной информацией

Нарушение статьи 23: Право на "личную и семейную тайну" предполагает возможность анонимной коммуникации или коммуникации без полной идентификации. Обязательная деанонимизация нарушает саму суть этого права.

5. Принудительная установка как нарушение права на выбор

С **1 сентября 2025 года Max должен быть предустановлен на все новые смартфоны, планшеты и компьютеры**, продаваемые в России. Государство **настоятельно рекомендует** (фактически требует) госслужащим и учителям его использование.[14] [15] [16]

Юрист Михаил Салкин прямо указал: **"Принуждение к установке приложения на личное устройство может квалифицироваться как нарушение конституционного права на неприкосновенность частной жизни — статья 23 Конституции РФ"**.[17] [18]

Нарушение статьи 23: Право на неприкосновенность частной жизни включает право **выбирать**, какие приложения устанавливать на своем устройстве. Принудительная предустановка нарушает это право.

Государственные цели в продвижении Max и запрете конкурентов

Официально заявленные цели

Государство объявило о следующих целях:

1. **Цифровой суверенитет** — избежать зависимости от иностранных технологических платформ. Сергей Боярский (глава комитета Госдумы) заявил, что Max закрывает "последний разрыв в цифровой безопасности".[19] [20]
2. **Национальная безопасность** — защита от использования иностранных мессенджеров в преступных целях и терроризме. Роскомнадзор мотивирует ограничения на WhatsApp и Telegram тем, что они используются для "организации террористических действий".[21]
3. **Консолидация государственных сервисов** — создание единой платформы для доступа к Госуслугам, цифровому ID и финансовым сервисам.[22] [11]

Скрытые и явные политические цели

Аналитики и правозащитники выявили более фундаментальные цели:

1. **Тотальный контроль коммуникаций**. Артем Козлюк из "Роскомсвободы" указал, что целью является **"централизовать и взять под контроль коммуникации и различные цифровые потоки: социальные, финансовые, информационные"**.[14]
2. **Подавление политического инакомыслия**. Max позволяет государству отслеживать всех граждан, их сетевые связи и убеждения через анализ коммуникаций.[5] [14]
3. **Социальный рейтинг** (по образцу Китая). Саркис Дарбинян из "Роскомсвободы" прямо назвал проект потенциальным "сумасшедшим экспериментом", который может привести к "системе социального рейтинга по китайскому образцу".[6]
4. **Миграция с зарубежных платформ**. State интенционально создает условия, при которых пользователи вынуждены переходить на Max. Ограничение работы WhatsApp и Telegram (падение скорости, блокировка звонков) — это технический механизм для миграции пользователей.[23] [16] [21]

Механизм запрета конкурентов

Правительство использует следующую стратегию:

Механизм	Примеры	Результат
Законодательные ограничения	ФЗ-41 (с 1 июня 2025) запрещает госорганам, банкам и операторам связи использовать иностранные мессенджеры для коммуникаций с клиентами[15] [24]	Крупные организации вынуждены уходить на отечественные платформы
Техническая блокировка	Роскомнадзор деградирует звонки в WhatsApp и Telegram, вводит постепенные ограничения[21] [25]	Пользователи испытывают неудобства и переходят на Max
Обязательная предустановка	Max обязателен на всех новых устройствах с 1 сентября 2025[14] [16]	Max становится "стандартным" приложением
Государственная интеграция	Max интегрирован с Госуслугами, электронными подписями, цифровым ID[11] [13]	Пользователи вынуждены использовать Max для доступа к государственным сервисам
Административное давление	Госорганам и учителям "рекомендовано" (фактически требуется) использовать Max[14] [15]	Бюджетные работники вынуждены устанавливать приложение на личные устройства

Международные примеры и сравнение

1. Китай: WeChat как модель тотального контроля

Сходства с Max: China использует мессенджер **WeChat** (более 1 млрд пользователей) как **инструмент государственного контроля и цензуры**.[26] [27] [28]

Характеристики WeChat:

- Все сообщения в групп-чатах **мониторируются правительством в реальном времени**[27] [26]
- Сообщения хранятся в течение **6 месяцев**, даже удаленные[27]
- **Встроенная цензура** фильтрует политически чувствительные ключевые слова и изображения[28] [26]
- **Социальный рейтинг**: WeChat интегрирована с системой социального кредита КНР[26]
- **Полная деанонимизация**: все пользователи связаны с реальными удостоверениями личности[28]

Различия: WeChat разработан частной компанией (Tencent), но **под строгим государственным контролем**. Max разработан государственной компанией VK, что дает еще больший прямой контроль.[20]

Вывод: Max следует **китайскому образцу** использования мессенджера как средства массовой слежки и контроля, хотя Россия заявляет иное.

2. Индия: SIM-привязка как альтернативный подход

Отличие от Max: In November 2025, India introduced **SIM-binding requirements** для WhatsApp, Telegram, Signal и других мессенджеров.[29] [30] [31]

Что требует Индия:

- Мессенджеры должны работать только с **активной SIM-картой**, введенной в момент регистрации[30] [29]
- **Web-версии должны разлогиниваться** каждые 6 часов[31] [29]
- Цель: **трассируемость** и **противодействие мошенничеству**[30]

Различие: Индия не **запрещает** иностранные мессенджеры, не создает государственный мессенджер и не внедряет шпионское ПО. Она требует **технической связи с физической SIM-картой**, что позволяет отследить географическое местоположение при необходимости.[30]

Оценка: Индийский подход нарушает права в меньшей степени, чем Max, так как:

- Не **запрещает** выбор платформы
- Не **собирает метаданные** в централизованную систему
- Требует **судебное решение** для доступа к данным (теоретически)
- Не интегрирует шпионаж в саму архитектуру приложения

3. Евросоюз: GDPR как противоположный подход

Регуляция мессенджеров в ЕС: EU не создает государственный мессенджер и не запрещает иностранные платформы. Вместо этого применяется **GDPR** (Регламент защиты данных).[32] [33]

GDPR-требования:

- Мессенджер **не должен читать адресную книгу** без явного согласия[32]
- Обязательно **сквозное шифрование** (end-to-end)[32]
- **Серверы только в ЕС**, не за границей[32]
- Данные **не могут использоваться** в рекламных целях[32]
- Нарушение: штрафы до **20 млн евро или 4% глобального оборота**[33]

Судебный контроль: ЕС через Европейский суд по правам человека (ЕСПЧ) опротестовал **российские требования** о передаче ключей шифрования. В деле *Podchasov v. Russia* (2024) ЕСПЧ признал, что требование России об отказе от ключей шифрования **нарушает право на приватность** (Статья 8 Европейской конвенции).[10]

Заключение: ЕС предпочитает **технологическую нейтральность** (допускает любые платформы) при условии соответствия стандартам защиты данных, а не государственный контроль.

4. Австралия: Другой тип государственного контроля

Различие подхода: Australia приняла серию **законов о полномочиях государственной слежки**, но не создает обязательный мессенджер.[34] [35]

Австралийские инструменты надзора:

- **Data Disruption Warrants** — позволяют полиции добавлять, копировать, удалять или изменять данные на устройствах[34]
- **Account Takeover Warrants** — позволяют выдавать себя за пользователя в течение 90 дней[34]
- **Network Activity Warrants** — позволяют получать доступ ко всему трафику в сети (например, ко всем сообщениям WhatsApp, если кто-то подозревается в преступлении)[34]
- **Emergency Authorization** — позволяет слежку без ордера в экстренных случаях[34]

Отличие от Max: Australia регулирует **доступ к мессенджерам** через судебные полномочия, но не создает **обязательный государственный мессенджер** и не прерывает пользователей работать с иностранными платформами.

Проблема: Even this approach was criticized by international observers as excessive. Australia in the top 5 for invasive surveillance powers.[36]

5. Сингапур: Цифровое правительство без тотального контроля

Подход: Singapore developing **Smart Nation 2.0** с цифровой трансформацией, включая цифровую идентификацию и e-gov сервисы.[37] [38] [39]

Отличие от Max: Singapore **не создает обязательный мессенджер**, **не запрещает иностранные платформы** и **не внедряет СОРМ-подобные системы** массовой слежки.[39] [37]

Фокус: Сингапур сосредоточена на **удобстве и включении** ("Trust, Growth, Community"), а не на контроле.[37]

Детальное юридическое обоснование нарушения статьи 23

Нарушение 1: Архитектура шифрования

Конституционный текст: "Ограничение этого права допускается только на основании судебного решения".[2] [1]

Интерпретация: Это означает:

1. Государство **может** при наличии судебного решения получить доступ к переписке
2. **Но** это должно быть исключением, а не правилом
3. **Архитектура** приложения не должна делать государство автоматическим "получателем" всех сообщений

Проблема Max: Использование FSB-одобренного шифрования означает, что **государство де факто "встроено" в каждое сообщение**. Никакое судебное решение не требуется для доступа на техническом уровне — ФСБ просто снимает данные из СОРМ-3 системы.[8] [5]

Вердикт: Нарушает статью 23, потому что превращает исключение (судебный доступ) в правило (автоматический доступ).

Нарушение 2: Сбор данных "по умолчанию"

Конституционный текст: Статья 24 (связана с 23): "Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются".[9]

Проблема Max:

- Сбор IP, геолокации, контактов, биометрических данных происходит **автоматически**[7] [6] [8]
- Пользователь **не может отказаться** от сбора без отказа от приложения в целом (что технически сложно, так как оно предустановлено)[12]
- Политика конфиденциальности **не требует** активного согласия на каждый элемент сбора[8]

Вердикт: Нарушает статью 23/24, потому что собирает данные о частной жизни без эффективного согласия.

Нарушение 3: Отсутствие судебного решения при системном доступе

Конституционный текст: "Ограничение этого права допускается только на основании судебного решения".[1] [2]

Проблема:

- **СОРМ-3** система позволяет ФСБ получать доступ к коммуникациям через технические каналы, встроенные в приложение[5]
- Технически, такой доступ не требует отдельного судебного решения — он "программно встроен"[5] [8]
- Хотя закон Яровая требует судебного решения для **декрипции данных**, Max не использует strong encryption, поэтому данные уже находятся в открытом виде на сервере[8] [5]

Вердикт: Нарушает статью 23, потому что создает механизм доступа, который **технически обходит** требование судебного решения.

Нарушение 4: Принудительная инсталляция и отсутствие выбора

Конституционный текст: Право на "неприкосновенность частной жизни" предполагает **свободу выбора** средств коммуникации.[1]

Проблема:

- Max **предустановлен на все новые устройства** с 1 сентября 2025[16] [14]
- Государство **активно поощряет** (фактически требует) его использование для государственных услуг[15]
- Отказ от использования на личных устройствах может привести к **невозможности доступа к Госуслугам**[13] [12]

Прецедент: Российский юрист Михаил Салкин прямо указал, что "принуждение к установке приложения на личное устройство может квалифицироваться как нарушение конституционного права на неприкосновенность частной жизни — статья 23 Конституции РФ".[18] [17]

Вердикт: Нарушает статью 23, потому что **уничтожает право на выбор**, что является стержнем права на неприкосновенность.

Государственные обоснования и их проблемы

Обоснование 1: "Цифровой суверенитет"

Аргумент государства: Russia должна иметь собственный мессенджер, чтобы не зависеть от иностранных корпораций.[19] [20]

Критика:

- **Противоречие**: Max использует open-source код из "недружественных" стран, включая Украину, что подрывает заявленную цель суверенитета[12] [5]
- **Частичная передача данных** на иностранные серверы опять же противоречит суверенитету[7] [5]
- **Реальная цель**: Не избежать зависимости, а **получить прямой контроль** над коммуникациями граждан

Обоснование 2: "Национальная безопасность"

Аргумент государства: WhatsApp и Telegram используются для террористических действий и мошенничества.[21]

Критика:

- Другие страны (ЕС, США, Австралия) борются с тем же, **не создавая обязательный государственный мессенджер**[35] [32] [34]
- **Избирательность**: Если безопасность — цель, почему Max должен быть обязательным **на личных устройствах граждан**, а не только для государственного использования? [17] [14]
- **Отсутствие пропорциональности**: Запрет на использование WhatsApp/Telegram гораздо более нарушает права, чем необходимо для безопасности

Обоснование 3: "Удобство государственных услуг"

Аргумент государства: Max объединит все государственные сервисы в одном приложении.[11] [22]

Критика:

- **Ложный выбор**: Государство могло бы интегрировать Госуслуги с **любым** мессенджером (WhatsApp, Telegram, Signal), но выбрало подконтрольный[11]
- **Деанонимизация**: Интеграция с Госуслугами и цифровым ID **уничтожает анонимность** коммуникаций, что нарушает основу права на неприкосновенность[13] [12]

Заключение: Пока еще нарушает или потенциально нарушает?

Текущее состояние (декабрь 2025)

Max уже нарушает статью 23 Конституции РФ по следующим аспектам:

1. **Архитектура шифрования** — встроенный доступ ФСБ для системного контроля
2. **Сбор данных** — сбор биометрических и поведенческих данных без эффективного согласия

3. **Отсутствие судебного контроля** — СОРМ-3 интеграция позволяет доступ без решения суда
4. **Принудительная установка** — нарушает право на выбор средств коммуникации

Будущие потенциальные нарушения

Если Max будет полностью интегрирован с государственной инфраструктурой и его использование станет де-факто обязательным (что разворачивается с 1 января 2026), то:[15]

5. **Деанонимизация** станет полной, что нарушит "местную и семейную тайну"[32]
6. **Социальный рейтинг** (по образцу Китая) будет техническим возможным[6]
7. **Политический контроль** — государство сможет отслеживать и подавлять инакомыслие через анализ коммуникаций

Обобщение международной позиции

Страна	Подход	Соответствие правам
Китай (WeChat)	Обязательный государственный мессенджер, тотальная слежка	Нарушает права, но формально "законно" в КНР
Россия (Max)	Обязательная предустановка, СОРМ-3 интеграция	**Нарушает статью 23 Конституции РФ**
Индия	SIM-привязка для существующих мессенджеров	Нарушает права в меньшей степени
ЕС	GDPR-регулирование без государственного контроля	Соответствует европейским стандартам прав
Австралия	Судебные полномочия доступа, но без государственного мессенджера	Нарушает права, но менее систематично
Сингапур	Цифровая трансформация без тотального контроля	Соответствует международным стандартам

Вывод: Российский подход к Max **ближайший к китайской модели**, что делает его одним из наиболее инвазивных в мире в отношении прав на приватность и статьи 23 Конституции.

⁂

1. https://base.garant.ru/10103000/74d7c78a3a1e33cef2750a2b7b35d2ed/
2. https://www.consultant.ru/document/cons_doc_LAW_28399/2573feee1caecac37c442734e00215bbf1c85248/
3. https://bbcrussian.substack.com/p/what-we-know-about-max-the-kremlin-backed-messenger
4. https://cybercitadel.com/signal-vs-telegram-a-detailed-comparison-of-security-and-privacy/
5. https://xpert.digital/en/max-messenger/
6. https://www.securitylab.ru/blog/personal/Bitshield/355756.php
7. https://mosregdata.ru/article/messenzher-max-pretenzii-i-problemy/

8. https://h2cked.com/russian-max-messenger-used-for-surveillance/
9. https://static.mskobr.ru/docs/laws/konst_23_24.pdf
10. https://www.dicopo.eu/russias-data-storage-laws-violate-privacy-rights/
11. https://www.it-world.ru/it-news/fd737zy3uio0c0kkok0g4go8so8c0co.html
12. https://www.themoscowtimes.com/2025/08/28/everything-you-need-to-know-about-max-russias-state-backed-answer-to-whatsapp-a90356
13. https://www.vedomosti.ru/economics/articles/2025/08/26/1134110-mintsifri-predlozhilo-krupnomu-biznesu-integrirovatsya-s-max
14. https://takiedela.ru/notes/max-v-plenu-u-fsb/
15. https://www.vedomosti.ru/politics/articles/2025/11/28/1158845-mintsifri-rekomendovalo-gosorganam-pereiti-na-max
16. https://www.aljazeera.com/news/2025/12/5/russia-continues-tech-crackdown-by-blocking-snapchat-facetime-access
17. https://news.ru/society/yurist-vyskazalsya-o-prinuzhdenii-rabotnikov-ustanavlivat-messendzher-max
18. https://myseldon.com/ru/news/index/333957521
19. https://www.aa.com.tr/en/europe/russia-unveils-national-messaging-app-to-reduce-reliance-on-whatsapp-telegram/3584707
20. https://jamestown.org/kremlins-new-moves-towards-internet-sovereignty/
21. https://tass.ru/ekonomika/25764077
22. https://interfax.com/newsroom/top-stories/112230/
23. https://www.svoboda.org/a/tselj---totaljnyy-kontrolj-vk-po-zakazu-kremlya-sozdast-edinyy-messendzher-dlya-rossiyan-/33449806.html
24. https://daydigital.ru/articles/day-digital/zapret-na-whatsapp-i-telegram-dlya-biznesa-s-1-iyunya-2025-kogo-kasaetsya-i-chto-delat/
25. https://www.vedomosti.ru/technology/news/2025/10/30/1151248-roskomnadzor-ne-blokiruet
26. https://www.monmouth.edu/magazine/the-dark-side-of-wechat/
27. https://en.wikipedia.org/wiki/Mass_surveillance_in_China
28. https://chinaobservers.eu/from-messaging-to-policing-wechats-role-in-maintaining-public-security/
29. https://www.moneycontrol.com/technology/sim-binding-in-india-what-it-means-for-whatsapp-telegram-users-and-why-the-government-wants-it-article-13702896.html
30. https://securityaffairs.com/185265/laws-and-regulations/india-mandates-sim-linked-messaging-apps-to-fight-rising-fraud.html
31. https://timesofindia.indiatimes.com/technology/tech-news/government-tells-whatsapp-telegram-and-others-to-link-services-to-sim-cards-what-it-means-for-users/articleshow/125673507.cms
32. https://chatwerk.de/en/blog/messenger-gdpr-you-have-to-keep-this-in-mind-when-it-comes-to-data-protection/
33. https://threema.com/en/use-cases/gdpr-compliant-messenger
34. https://digitalrightswatch.org.au/2021/09/02/australias-new-mass-surveillance-mandate/
35. https://www.abc.net.au/news/science/2022-09-21/internet-online-safety-act-industry-codes/101456902
36. https://www.comparitech.com/blog/vpn-privacy/gov-social-media-surveillance/
37. https://www.digitalgateway.gov.sg/about-sgdc/

38. https://www.pmo.gov.sg/newsroom/formation-smart-nation-and-digital-government-group-prime-ministers-office/
39. https://www.imda.gov.sg/about-imda/research-and-statistics/sgdigital
40. http://ng-74.ru/novosti/obschestvo/18722-eksperty-razoblachayut-mify-o-messendzhere-max-i-rasskazyvayut-kak-raspoznat-istinu-i-lozh.html
41. https://www.hse.ru/expertise/news/1078506823.html
42. https://up74.ru/articles/news/166493/
43. https://t-j.ru/news/max-pusti/
44. https://vc.ru/id2570483/2526213-messendzher-max-problemy-konkurentsiya-i-pravovye-voprosy
45. https://constitution.garant.ru/rf/chapter/74d7c78a3a1e33cef2750a2b7b35d2ed/
46. https://roskomsvoboda.org/ru/post/gov-services-to-integrate-into-max-messenger-for-tech-sovereignty/
47. https://www.ap.org/news-highlights/spotlights/2025/encrypted-messaging-apps-promise-privacy-government-transparency-is-often-the-price/
48. https://blog.cryptographyengineering.com/2024/08/25/telegram-is-not-really-an-encrypted-messaging-app/
49. https://dig.watch/updates/public-consultation-eu-clarifies-how-dma-and-gdpr-work-together
50. https://www.nytimes.com/2025/06/07/world/europe/russia-china-wechat-spying.html
51. https://tass.ru/obschestvo/24867953
52. https://www.leuropeista.it/en/russia-stop-whatsapp-and-telegram-calls-if-they-do-not-hand-over-user-data/
53. https://www.oaic.gov.au/about-the-OAIC/information-policy/information-policy-resources/messaging-apps-a-report-on-australian-government-agency-practices-and-policies
54. https://www.esafety.gov.au/newsroom/whats-on/online-safety-act
55. https://www.youtube.com/watch?v=uUOiknXHtNs
56. https://en.wikipedia.org/wiki/Internet_censorship_and_surveillance_by_country
57. https://www.bbc.com/news/articles/ce9rj2145jgo
58. https://www.amnesty.org.uk/which-countries-access-your-data-nsa-gchq-five-eyes-snowden-surveillance
59. https://www.mpg.de/25788438/chat-control-eu-client-side-scanning