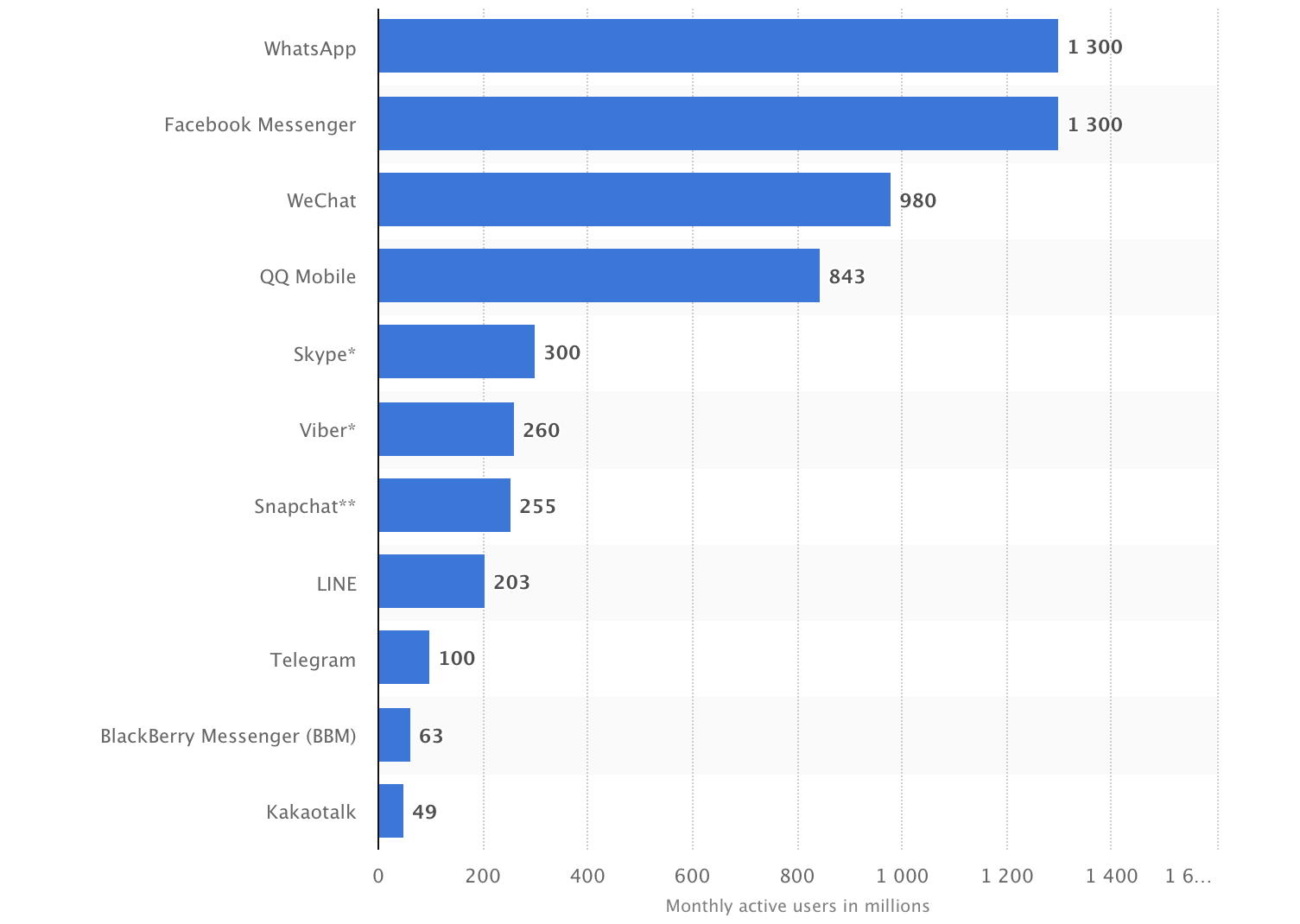
Как проблемами с Mail.ru и ФСБ ковалась репутация Павла Дурова и вера в «Телеграм»

* [Системы обмена сообщениями](https://habr.com/ru/hub/instant_messaging/),
* [История IT](https://habr.com/ru/hub/history/)

Запущенный в 2013 году на рынке, вроде бы и так не испытывающем дефицита в мессенджерах, «Телеграм» моментально начал менять правила игры, первым распознав, что рядовому юзеру хочется защиты приватности его коммуникаций — и открыв, тем самым, тогда ещё никем не занятую нишу для захвата, в которую, уже вслед за ним, после устремились и другие мессенджеры. А Telegram, тем временем, уже отбивал аудиторию у пабликов в соцсетях, и даже начал превращаться в медийную платформу, уводя землю из-под ног у других площадок — от блогов до традиционных медиа.  
  
В феврале 2016 года Дуров [заявил](https://ru.wikipedia.org/wiki/Telegram) о 100 миллионах пользователей «Телеграма», а 22 марта 2018 года мессенджер достиг «обитаемости» в 200 миллионов человек.  
  
И пусть это мизер на фоне миллиардных аудиторий других проектов, среди которых «Телеграм» лишь [девятый](https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/) по количеству активных юзеров — это не помешало ему стать трендесеттером среди других приложений.  
  


* WhatsApp давно не задаёт трендов, копируя лучшее у остальных — например, сквозное шифрование как раз у«Телеграма».
* Facebook Messenger, навязанный фактически силой пользователям соцсети без явного понимания, зачем и для чего, тем более не тянет на лидера — а в вопросах приватности, видимо, за всем «Фейсбуком», валится в аутсайдеры.
* Дальше рынок начинает потихоньку сегментироваться, и если кто-то ещё вызывает громкие эмоции, то это Skype: «Да когда ж он сдохнет-то!»
* …или Viber: «Смотрите, кто живой».

Как же Telegram дошёл до жизни такой?

Вера в защищённость «Телеграма», в какой-то мере — функция репутации самого Павла Дурова

Дуров постоянно артикулирует свою приверженность либертарианским взглядам, выступая, в числе прочего, за реформу российской образовательной системы, отмену налогов в сфере информации, отмену визовой системы, прописок и воинского призыва, снижение таможенных пошлин, предоставление регионам полной автономии, открытость суда присяжных etc. — причём, свои взгляды, как и основанные на них решения, Дуров не стесняется подавать в бескомпромиссном виде.

Старый завет: эпоха «Вконтакте»

Ещё во времена «Вконтакте» Дуров оказался втянут в корпоративную войну, когда крупный акционер соцсети, компания Mail.ru Group, попыталась её поглотить, купив 100% акций, чтобы объединить сайт с «Одноклассниками». В ответ на это Дуров буквально [показал](https://www.ridus.ru/news/30721) корпорации средний палец:  
  
  
  
Исход «войны» решило то, что Дуров сумел убедить сооснователей «ВКонтакте» не продавать свои акции. В апреле 2012 года «война» прекратилась.  
  
Примерно тогда же, в 2011 году, из-за отказа блокировать оппозиционные паблики во «Вконтакте» у Дурова начались проблемы и с российскими властями.  
  
8 декабря 2011 года этот конфликт стал публичным, когда на официальный запрос от ФСБ со списком групп, Дуров [ответил](https://twitter.com/durov/status/144775176742113281) картинкой, сразу ставшей мемом.  
  
  
  
Следующие два года, по мере ухудшения ситуации со свободами в России, давление на Дурова росло. О том, что стало последней каплей, он рассказал спустя два года после ответа с собачкой в худи.

13 декабря 2013 года ФСБ потребовала от нас выдать личные данные организаторов групп Евромайдана. Нашим ответом был и остаётся категорический отказ — юрисдикция России не распространяется на украинских пользователей ВКонтакте. Выдача личных данных украинцев российским властям была бы не только нарушением закона, но и предательством всех тех миллионов жителей Украины, которые нам доверились. В процессе мне пришлось пожертвовать многим. В частности, я продал свою долю ВКонтакте, так как её наличие могло помешать мне принимать правильные решения. Но я ни о чём не жалею — защита личных данных людей стоит этого и намного большего. С декабря 2013 года у меня нет собственности, но у меня осталось нечто более важное — чистая совесть и идеалы, которые я готов защищать.

За пределами России, находясь в менее уязвимом с точки зрения личной безопасности положении, Дуров занял ещё более категоричную позицию в отношении давления государства.  
  
«13 марта 2014 года прокуратура потребовала от меня закрыть антикоррупционную группу Алексея Навального под угрозой блокировки «Вконтакте». Но я не закрыл эту группу в декабре 2011 года и, разумеется, не закрыл сейчас», — написал Дуров на своей странице в соцсети.  
  
«Мы не будем удалять ни антикоррупционное сообщество Навального, ни сотни других сообществ, блокировки которых от нас требуют. Свобода распространения информации — неотъемлемое право постиндустриального общества. Это право, без которого существование «Вконтакте» не имеет смысла».

Новый завет: эпоха «Телеграма»

В [интервью New York Times](https://www.nytimes.com/2014/12/03/technology/once-celebrated-in-russia-programmer-pavel-durov-chooses-exile.html) Дуров рассказал, что идея создания мессенджера появилась в 2011 году, когда к нему пришли представители спецслужб России. Как только они покинули дом Павла, он осознал, что безопасного канала общения со своим братом, друзьями и коллегами у него просто нет. Если нет канала — значит нужно его создать. Что и было сделано.  
  
Первая версия софта появилась в 2013 году, изначально было представлено приложение для iOS, а затем — и для других платформ, включая Android, iOS, Windows Phone, Linux, Windows, OS X. Когда 14 августа 2013 года Telegram в качестве экспериментального мессенджера появился на AppStore, первый пункт его описания выглядел так:  
  
Безопасность. Передаваемые в Telegram сообщения не могут быть прослушаны третьими лицами вроде Вашего интернет-провайдера.  
  
Как следствие, «Телеграм» одним из первых громко и амбициозно заявил о своей сфокусированности именно на защите приватности.  
  
Фактически сразу после выхода мессенджера в свет было объявлено, что он защищён не только от обычных злоумышленников, но и от прослушивания со стороны государственных структур вроде ФСБ, АНБ и т.п., предложив даже такие оригинальные фичи, как секретные чаты.  
  
Секретные чаты в «Телеграм» были запущены ещё в октябре 2013 года, в то время как Facebook и WhatsApp предоставили пользователям такую возможность в 2016 году.  
  
Быть первым оказалось важно — повторение фишек «Телеграма», вроде сквозного шифрования, тем же «Ватсаппом», выглядело обычным приёмом конкурентной борьбы, ничего не говорящим о реальной мотивированности разработчиков защищать приватность юзеров.  
  
Разумеется, различные фичи сами по себе делали «Телеграм» защищённым мессенджером не более, чем зажигалка-граната и радиомаяк в каблуке делают из Джеймса Бонда адекватную замену роте ВДВ, например, при штурме укреплений противника.  
  
Свою устойчивость к штурмовым тактикам, подкопам и любым другим попыткам нанести «Телеграму» вред, команда приложения демонстрировала предложениями взломать их продукт за их же деньги. Разумеется, помимо каких-то крупных баунти, ведётся постоянная работа по отлову уязвимостей — и Telegram не жалеет денег на поиск слабых мест.  
  
Сами суммы вознаграждений по [двести](https://telegram.org/crypto_contest)-[триста тысяч долларов](https://telegram.org/blog/cryptocontest) привлекали внимание СМИ — и, как следствие, ещё больше разработчиков для тестирования уязвимостей мессенджера. Сейчас шумиха поугасла, поиск уязвимостей стал более рутинным, но никуда не пропал, периодически напоминая о себе разными публикациями очередных удачливых баг-хантеров.  
  
Благодаря своей репутации защищённого от взлома продукта, Telegram стал популярен, в числе прочего, в странах с авторитарными или чересчур любопытными режимами.  
  
В Иране, скажем, к концу 2017 года «Телеграмом» пользовалось более 40 млн человек — половина (!) всего восьмидесятимиллионного населения страны, — вскоре после чего был, в числе других массовых интернет-сервисов и ресурсов, [заблокирован властями](http://www.bbc.com/russian/features-42568058) в процессе подавления беспорядков.  
  
При всей декларируемой либеральности взглядов «капитанов индустрии» вроде Марка Цукерберга, Сергея Брина или Тима Кука, интересы акционеров заставляют их «прогибаться» под власть, например, в Китае, ставят их в неудобное положение, в котором они пытаются сохранить лицо, при этом не отказываясь от своего куска огромного китайского пирога.  
  
В сочетании с видимым презрением к финансовым рискам конфликтов с теми или иными государствами, какого бы размера рынок они не контролировали, Дуров завершает формирование образа чуть ли не современного Гая Фокса, кумира анархистов. И человека, которому веришь, что он не станет следить за вами или сливать ваши данные на сторону в своём приложении.  
  
В России «Телеграму» до подобного покрытия было далеко — в сентябре 2017 года Павел Дуров насчитал на родине 10 миллионов пользователей, — впрочем, достаточно, чтобы стать костью в горле ФСБ, в 2016 году пролоббировавшей принятие оруэлловского [пакета законов Яровой-Озерова](https://ru.wikipedia.org/wiki/%D0%97%D0%B0%D0%BA%D0%BE%D0%BD_%D0%AF%D1%80%D0%BE%D0%B2%D0%BE%D0%B9), дающего ей право требовать от любых работающих на территории России сервисов «золотые ключики» ко всем потайным дверкам — то есть дешифровку любых, на усмотрение наследников царской «охранки» и НКВД, проходящих через них коммуникаций.  
  
Регламент передачи ключей шифрования был сразу же опубликован ФСБ в приказе №432, а для демонстрации серьёзности настроя спецслужб, Роскомнадзор даже учинил показательную казнь ряда сервисов, самой громкой из которых стала до сих пор не снятая блокировка LinkedIn.  
  
  
  
Летом 2017 года на нескольких каналах вышли сюжеты, в которых Дурова называли анархистом и обвиняли в том, что многие теракты последних лет, в том числе взрыв в петербургском метро, координировались именно через Telegram. (Одновременно с этим, Первый канал призывал подписаться на него в Telegram).   
  
Дмитрий Киселёв в эфире «России 24» заявил, что Telegram «всё больше превращается в систему связи для террористов». Телеканал НТВ дал слово главе Роскомнадзора Александру Жарову, который призвал Павла Дурова «одуматься» и предоставить спецслужбам ключи дешифрации.   
  
26 июня Дуров [ответил](https://vk.com/durov?w=wall1_1840829) ему у себя на стене:

Это требование не только противоречит 23-й статье Конституции РФ о праве на тайну переписки, но и демонстрирует незнание того, как шифруется коммуникация в 2017 году. В 2017 году обмен секретной информацией построен на оконечном шифровании, к которому у владельцев мессенджеров нет и не может быть “ключей для дешифрации”. Эти ключи хранятся только на устройствах самих пользователей. Хотя Telegram был пионером этой технологии, сегодня оконечное шифрование используют все популярные мессенджеры, включая WhatsApp, Viber, iMessage и даже Facebook Messenger. Потенциальная блокировка Telegram никак не усложнит задачи террористов и наркодилеров — в их распоряжении останутся десятки других мессенджеров, построенных на оконечном шифровании (+VPN). Ни в одной стране мира не заблокированы все подобные мессенджеры или все сервисы VPN. Чтобы победить терроризм через блокировки, придется заблокировать интернет.

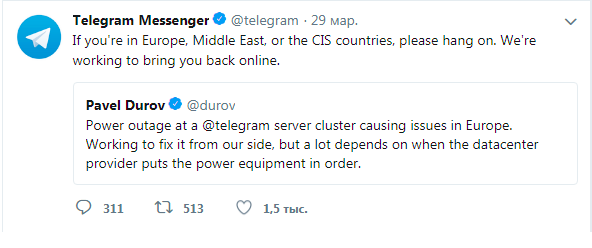
[Добавив](https://vk.com/wall1_1844194?w=wall1_1844194) в тот же день:

Время появления информации о том, что почти три месяца назад Telegram якобы использовался при подготовке теракта, вызывает вопросы. Печально, если спецслужбы России эксплуатируют подобную трагедию как предлог для усиления своего влияния и контроля над населением.  
  
К сожалению, средства коммуникации вроде Telegram или WhatsApp не могут стать небезопасными только для потенциальных террористов. Шифрование этих сервисов либо одинаково защищает всех пользователей, либо всех их ставит под удар. Отказ от оконечного шифрования в отдельно взятой стране сделает десятки миллионов людей беззащитными от атак хакеров и шантажа коррумпированных чиновников.   
  
Более того, ослабление шифрования во всех мессенджерах приведет к подрыву национальной безопасности страны в целом, так как в этом случае иностранные спецслужбы неизбежно тоже получат доступ к переписке граждан России. При этом риск терактов не исчезнет – как показали события в Париже, для проведения теракта достаточно одноразовых телефонов и обычных CMC без всякого шифрования.

Кроме медиа-атак, «Телеграму» пришлось [отбиваться](https://vk.com/id1?w=wall1_1860157) и от начавшего кружить вокруг него Роскомнадзора:

Telegram работает на единых принципах по всему миру: даже в консервативном Иране, где заблокированы Facebook и Twitter, и где у Telegram более 40 миллионов активных пользователей, правительство не получило от нас ни байта личных данных пользователей. Мы не будем делать исключений из наших принципов ради сохранения доли рынка в отдельных странах.

* В сентябре 2017 года ФСБ потребовала выдать ей «золотой ключик» уже от «Телеграма».
* «Телеграм» отказался, за что был в октябре оштрафован на 800 000₽.
* В декабре «Телеграм» обратился с иском о признании самого приказа 432 незаконным в Верховный суд Российской Федерации.
* 20 марта 2018 года Верховный суд [в иске отказал](https://www.gazeta.ru/tech/news/2018/03/20/n_11307739.shtml), оставив в силе законность приказа и требований ФСБ.
* В тот же день Роскомнадзор потребовал от «Телеграма» передать ключи шифрования в течение 15 дней, пригрозив блокировкой на территории России в случае неподчинения.
* Павел Дуров ответил в «Твиттере», что угрозы заблокировать Telegram не принесут результата.
* 13 апреля 2018 года Таганский суд Москвы вынес решение в пользу Роскомнадзора, тем самым позволив начать блокировку мессенджера на территории России.
* [1 февраля 2019 года Верховный суд РФ отклонил кассационную жалобу Telegram, поданную в рамках дела о блокировке мессенджера в России](https://ru.wikipedia.org/wiki/%D0%91%D0%BB%D0%BE%D0%BA%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_Telegram_%D0%B2_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8#%D0%A5%D1%80%D0%BE%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D1%8F_%D1%81%D0%BE%D0%B1%D1%8B%D1%82%D0%B8%D0%B9).

Незадолго до начала, 22 марта 2018 года, «Телеграм» перешагнул за двести миллионов пользователей, а 29 марта на 3,5 часа «лёг» на территории Европы и России из-за отключения электричества в одном из его дата-центров.   
  
  
  
Пользователи стали шутить о тренировочном отключении в России, а Роскомнадзор отшучивался, что он «[ни при чём](https://twitter.com/roscomnadzor/status/979284459504709632)».

Символы веры в пресвятую «Телегу»

* Личность основателя — взгляды и действия Павла Дурова.
* Последовательность политики «0 байтов данных пользователей третьим лицам» и при политическом, и при рыночном давлении.
* Резкость жестов, категоричность формулировок и даже какие-то намёки на неполиткорректность — это так желанная многими «новая откровенность».
* Первенство в установке на защищённость пользовательской коммуникации.
* Готовность «Телеграма» платить большие деньги за найденные уязвимости.
* Как показал 2018 год, даже выключенный рубильник «Телеграму» не помеха.

Пример сформированной таким путём веры в «Телеграм» продемонстрирует Брюс Сьюэлл, главный юрисконсульт Apple, в марте 2016 года заявивший, что Telegram — «абсолютно невзламываемый метод коммуникации».  
  
Но в этом проблема любой веры: не все готовы её принять.

Священные войны против «Телеграма»

В конце 2013 года на «Хабрахабре» появился [пост об уязвимости Telegram](https://habrahabr.ru/post/206900/), которая позволяла получить доступ к чатам любого пользователя, у которого отключена двухфакторная аутентификация, при помощи перехвата SMS с одноразовым кодом.  
  
Летом 2016 года на Gizmodo вышла статья «[Почему вы должны прекратить использовать Telegram прямо сейчас](https://gizmodo.com/why-you-should-stop-using-telegram-right-now-1782557415)», автор которой заявил, что мессенджер вовсе не так хорошо защищён, как это утверждает команда «Телеграма». Основной проблемой с безопасностью он назвал необходимость ручного включения шифрования чатов — по умолчанию эта функция была отключена, и, чтобы получить действительно защищённый канал связи, нужно было самостоятельно включить её в настройках.  
  
Но большинство проблем вокруг «Телеграма» были связаны с привязкой учётной записи к телефону пользователя. Так, в мае 2017 года неизвестные пользователи [смогли войти](https://www.vedomosti.ru/opinion/articles/2016/05/12/640689-zaschischen-telegram) в Telegram-аккаунты оппозиционных политиков Георгия Албурова и Олега Козловского. Они оба получили сообщения о входе с нового устройства, которое работало под управлением Linux и было подключено к сети через анонимную сеть Tor.  
  
После детального расследования (участие в нём приняли и разработчики Telegram) оказалось, что инцидент связан с перехватом SMS-сообщения с паролем для входа в мессенджер. Самое интересное заключается в том, что в ночь перехвата кодов, услуги передачи SMS-сообщений на телефонах пострадавших пользователей были отключены. Ещё одно совпадение заключается в том, что они оба были абонентами МТС, который Албуров и Козловский обвинили в содействии взломщикам.  
  
В конце 2017 года сомнения в неуязвимости мессенджера посеял Антон Розенберг, экс-сотрудник «Вконтакте» и «Телеграм». Он сообщил, что в ходе конфликта с братом Павла Дурова, Николаем, у него, Розенберга, в мессенджере «Телеграм» внезапно пропала история переписки с момента регистрации в 2013 году. «[Удалена она была только на сервере, так как сообщения, закешированные у меня в телефоне, никуда не делись. В общем, выглядело всё ровно так, будто кто-то сделал запрос delete\_first\_messages («удалить первые N сообщений пользователя») — такая функция была ещё в движке text-engine, разработанном в ВК и позднее выложенном в open source](https://medium.com/@anton.rozenberg/friendship-betrayal-claims-3f395bcc95fa)». Его пост наделал много шума, но его слова так и остались без подтверждения.  
  
В официальном [ответе «Телеграма» на статью Gizmodo](https://medium.com/@tglive/stop-reading-gizmodo-7fe0bb36afb1) говорилось, что автор путается в терминах, не различая, в частности, обычное и оконечное шифрование. По словам команды мессенджера, в нём шифруется всё: «Секретные чаты используют оконечное (end-to-end) шифрование, облачные чаты используют клиент-серверное шифрование для передачи данных и, конечно, хранятся в зашифрованном виде».  
  
Кроме того, для обеспечения безопасности данных, не имеющих end-to-end шифрования, Telegram использует распределённую инфраструктуру. В этом случае информация из облачных чатов хранится в большом количестве дата-центров по всему земному шару, находясь под различными юрисдикциями. Ключи дешифрования разбиты на части и не хранятся в том же месте, что и данные, зашифрованные этими ключами.   
  
В итоге, чтобы заставить Telegram выдать информацию любого рода, имеющую отношение к пользователям мессенджера, требуется получить несколько судебных предписаний из различных юрисдикций.   
  
В июне 2017 года команда мессенджера заявила следующее: «На сегодняшний день «Телеграм» передал 0 байтов данных пользователей третьим лицам, включая правительственные органы».  
  
Политики тоже, несмотря на ситуацию с Козловским и Албуровым, продолжают пользоваться «Телеграмом». Например, мессенджер использует штаб Алексея Навального.

Телеграм хороший сервис, я пользуюсь, штаб пользуется, утечек не было никогда. А были бы — ничего страшного, у нас нет никаких секретов; в отличие от власти, у нас нет такой ситуации, когда «про себя» мы обсуждали бы одно, а «в паблик» говорили бы другое.  
*— Леонид Волков, IT-специалист и руководитель штаба Алексея Навального*

В общем, до сих пор все сомнения, вопросы, блокировки и атаки шли дуровскому детищу только на пользу, упрочая его репутацию и укрепляя веру в защищённость «Телеграма».  
  
И это только одна сторона масштабного феномена «Телеграма», который включает, помимо технических, ещё и маркетинговые, медийные, культурные и идейные аспекты.  
  
P.S. Поддержать автора рублём можно, воспользовавшись функцией «Поддержать автора» или сервисом [QIWI](http://w.qiwi.com/n/EGORKOTKIN).