

## Дополнение к формуляру жалобы с более подробным описанием предмета жалобы

### Е. Изложение фактов

#### *О Заявителе*

1. Заявитель – компания Telegram Messenger Limited Liability Partnership (Telegram Messenger LLP), зарегистрированная в Великобритании, владеющая интернет-сервисом Telegram.
2. Telegram – бесплатный кроссплатформенный интернет-сервис обмена текстовыми сообщениями, изображениями, видеофрагментами и произвольными файлами. Он также поддерживает голосовые звонки в реальном времени. В настоящее время аудитория сервиса насчитывает более 180 миллионов человек по всему миру<sup>1</sup>. В России у сервиса по разным оценкам от 6 до 12 миллионов пользователей.
3. Серверная инфраструктура Telegram в целях безопасности имеет распределенную архитектуру, и включает в себя подсистемы, находящиеся на территории различных государств и управляемый различными юридическими лицами. Переписка пользователей при этом распределяется между различными подсистемами и никогда не хранится в одном месте.
4. Telegram предоставляет пользователям возможность использовать два вида каналов обмена сообщениями – «облачные чаты» и «секретные чаты». В секретных чатах используется алгоритм сквозного (end-to-end) шифрования, при котором регулярно изменяемые ключи шифрования генерируются на устройствах пользователей, а передаваемые сообщения не хранятся на серверах Telegram. При этом ни у кого, включая разработчика программного обеспечения и администратора сервиса, нет технической возможности получить или изготовить дубликаты этих ключей. Подобная архитектура является условием безопасности коммуникации, уменьшая риск получения третьими лицами несанкционированного доступа к переписке пользователей. Сообщения, передаваемые через «секретные чаты», никогда не сохраняются на серверах Telegram.
5. Telegram, наряду с Signal от Open Whispers Systems, одним из первых массовых интернет-сервисов начал предоставлять услуги безопасного обмена сообщениями, и в настоящее время большинство наиболее популярных мессенджеров, включая WhatsApp, Viber, WeChat, iMessage и другие, в той или иной степени используют сквозное шифрование, ставшее фактически «золотым стандартом» отрасли.
6. Также Telegram предоставляет возможность ведения публичных Telegram-каналов, ставших в авторитарных странах с сильной государственной цензурой, одним из немногих независимых и свободных источников распространения информации и обмена мнениями по общественно-политическим вопросам. Такой способ позволяет автору или группе авторов не только делиться

---

1

<https://www.bloomberg.com/news/articles/2017-12-12/cryptic-russian-crusader-says-his-5-billion-app-can-t-be-bought>

информацией с неограниченным кругом лиц с минимальной дистанцией между читателем и контентом, но и сохранять при этом анонимность.

7. При этом компания активно противодействует использованию сервиса для пропаганды насилия, самостоятельно ежемесячно удаляя сотни каналов, в которых распространяется террористический контент и детская порнография.

*Общая ситуация со свободой интернета и правом на приватность в России*

8. Ведущие неправительственные организации в сфере свободы выражения отмечают, что с 2013 года российские власти целенаправленно предпринимают шаги для расширения возможностей слежки и ограничения приватности и анонимности в интернете<sup>2</sup>.

9. 6 июля 2016 года в России был принят пакет законодательных поправок под предлогом противодействия терроризму, затронувших различные аспекты регулирования интернета, в том числе касающиеся приватности и анонимности (т.н. «пакет Яровой»). Так, в частности, онлайн-сервисы в течение шести месяцев обязаны хранить всю переписку пользователей, предоставляя эти данные по запросам Федеральной службы безопасности (ФСБ).

10. Сервисы, использующие шифрование, кроме того должны предоставить ФСБ ключи, позволяющие расшифровать любые передаваемые, принимаемые и обрабатываемые с их помощью сообщения. При этом, действующий закон не обязывает спецслужбы получать предварительное судебное разрешение на доступ к такой информации (см. п.48 настоящего Дополнения).

11. В настоящее время реестр компаний, на которые распространяется действие закона (Реестр организаторов распространения информации), насчитывает 98 сервисов, включая такие популярные платформы как Вконтакте, Одноклассники, Мэйл.ру, Яндекс, Threema, Badoo, а также СМИ, городские и профессиональные форумы и т.д. По заявлениям представителей российских телекоммуникационных властей, рассматривается вопрос о включении в реестр Apple, Twitter, Facebook и WhatsApp, Google, Microsoft, Viber<sup>3</sup>.

12. Российские суды по искам прокуратуры запрещают распространение инструкций по использованию VPN и средств обхода блокировок<sup>4</sup>. Представители правоохранительных органов и спецслужб регулярно выступают с призывами заблокировать сеть Tor и доступ к онлайн-анонимайзерам. Кроме того, с 1 января 2018 года в России вступает в силу закон, обязывающий интернет-мессенджеры идентифицировать пользователей, предоставляя соответствующую информацию властям.

2

Russia: Joint UPR Submission shows restrictive new laws on free expression. ARTICLE 19 // <https://www.article19.org/resources/russia-joint-upr-submission-shows-restrictive-new-laws-on-free-expression/>

3

<https://rg.ru/2017/07/06/oleg-ivanov-v-reestre-uzhe-85-organizatorov-rasprostraneniia-informacii.html>

4

<https://roskomsvoboda.org/11503/>

2

13. Согласно докладу Международной правозащитной группы Агора «Россия под наблюдением 2017», за последние 10 лет российские суды удовлетворяли более 98% запросов о разрешении прослушивания телефонных переговоров или снятия информации с каналов связи<sup>5</sup>.

14. После 2012 года, когда в России вступил в силу первый закон, позволяющий во внесудебном порядке ограничивать доступ к информации в интернете перечень запрещенной информации и круг органов власти, уполномоченных принимать решение о блокировке постоянно расширялся. В настоящее время в Реестр запрещенных сайтов внесено более 94 тысяч ссылок, а общее число заблокированных за все время действия механизма ресурсов приближается к 9 миллионам. В 2017 – 2018 годах Европейским судом по правам человека коммуницированы несколько обращений, охватывающих различные аспекты блокировки информации в интернете (дела *Kharitonov v. Russia*, no. 10795/14; *ООО Flavus and the Others v. Russia*, nos. 12468/15, 23489/15, 20159/15, 19074/16 and 61919/16; *FOND SODEYSTVIYA ZASHCHITE ZDOROVYA I SOTSIALNOY SPRAVEDLIVOSTI IMENI A. RYLKOVA against Russia*, 13439/14).

15. Отказ предоставить ФСБ полный доступ к переписке пользователей помимо значительного штрафа (от 800 тысяч до 1 миллиона рублей) также влечет за собой блокировку сервиса на территории России. Равным образом подлежит блокировке интернет-сервис, отказавшийся добровольно предоставить российским властям информацию, необходимую для включения в Реестр организаторов распространения информации. Так в 2017 году по этим основаниям были заблокированы интернет-мессенджеры BlackBerry Messenger, Imo, Line, Vchat, а также интернет-рация Zello.

#### *Взаимоотношения Заявителя с российскими властями*

16. В течение весны 2017 года Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) направляла запросы Заявителю о предоставлении данных о компании для включения ее в Реестр организаторов распространения информации в сети «Интернет».

17. 23 июня 2017 года руководитель Роскомнадзора обратился к руководству Telegram Messenger LLP и пользователям сервиса с открытым письмом, опубликованным на официальном сайте Роскомнадзора:

«Должен констатировать, что в настоящий момент все имеющиеся возможности официальной коммуникации с командой мессенджера Telegram исчерпаны.

Практически каждый день Роскомнадзор направляет по всем доступным адресам Telegram письма с разъяснениями требований российского закона об организаторах распространения информации.

Требование одно, и оно простое: заполнить присланную анкету сведениями о компании, которая управляет Telegram. И официально направить в Роскомнадзор для включения этих данных в реестр организаторов распространения информации. Однако до сих пор мы не получили от администрации мессенджера никакого ответа.

---

5

<https://opendemocracy.net/files/Agora-Russiaundersurveillance2017.pdf>

Включение мессенджера в данный реестр означает лишь готовность Telegram работать по российским законам. Действующий правовой статус Telegram в России не изменится.

Уже сейчас, в силу закона, а не факта внесения в соответствующий реестр, Telegram должен исполнять обязанности организатора распространения информации.

В случае фактического отказа от исполнения обязанностей организатора распространения информации, Telegram в России должен быть заблокирован. До тех пор, пока мы не получим требуемые сведения»<sup>6</sup>.

18. 25 и 26 июня 2017 года на центральных телеканалах и в других подконтрольных российскому правительству средствах массовой информации вышла серия однотипных репортажей, в которых утверждалось, что сервис Telegram – основной инструмент общения и самоорганизации террористов, а также канал продажи наркотиков. «Первый канал» в выпуске вечерних новостей сообщал:

«Почему же так любят «Телеграм» террористические ячейки? - спрашивает журналист.

«Телеграм» дает возможность террористам конспиративного общения, начиная от вербовки и обучения исполнителя, в том числе создания так называемых закрытых «спящих ячеек», - поясняет оперативный сотрудник антитеррористического подразделения ФСБ.

<...>

К тому же, помимо террористических ячеек, мессенджер давно облюбовали и торговцы наркотиками. Только в этом месяце МВД вскрыло десятки точек продаж через «Телеграм»<sup>7</sup>.

19. 28 июня 2017 года руководитель компании Павел Дуров на своей странице социальной сети «ВКонтакте» опубликовал заявление:

«Регистрационные данные о компании-издателе Telegram – не секрет и доступны любому желающему в открытых ... **Давая согласие на внесение в реестр, мы исходим из соответствия истине заявления главы Роскомнадзора («на этом точка») и не берем на себя каких-либо дополнительных обязательств. В рамках работы с российским регулятором мы можем обещать только тот уровень сотрудничества, который демонстрируем во всех остальных странах**, а именно – продолжать совместную работу по удалению публичных материалов, связанных с пропагандой терроризма, наркотиков, призывами к насилию и детской порнографией, а также продолжать работу по пресечению рассылок спама»<sup>8</sup>.

20. 28 июня 2017 года Роскомнадзор сославшись на публикацию Дурова, включил Заявителя в Реестр организаторов распространения информации под №90 (приложение 2).

21. 12 июля 2017 года ФСБ направила в адрес Заявителя запрос о предоставлении информации, «необходимой для декодирования сообщений за период, начиная с 12 июля 2017 года, по лицам, подозреваемым в причастности к террористической деятельности – пользователям интернет-мессенджера «Telegram». В частности, запрашивались общедоступный идентификатор

6

<https://rkn.gov.ru/news/rsoc/news46796.htm>

7

[https://www.1tv.ru/news/2017-06-25/327652-fsb\\_rf\\_telegram\\_daet\\_terroristam\\_vozmozhnost\\_konspirativnogo\\_obscheniya\\_i\\_sozdaniya\\_spyaschih\\_yacheek](https://www.1tv.ru/news/2017-06-25/327652-fsb_rf_telegram_daet_terroristam_vozmozhnost_konspirativnogo_obscheniya_i_sozdaniya_spyaschih_yacheek)

8

[https://vk.com/durov?w=wall1\\_1854483](https://vk.com/durov?w=wall1_1854483)

пользователя информационной системы; дата и время оказания услуги; IP-адрес; номер TCP/UDP порта; ключевой материал, необходимый и достаточный для декодирования сообщений. Информацию по 6 телефонным номерам требовалось предоставить до 19 июля 2017 года на адрес интернет-приемной службы [fsb@fsb.ru](mailto:fsb@fsb.ru) (приложение 3).

22. Запрос был доставлен Заявителю 21 июля 2017 года (приложение 4).

23. Заявитель отказался исполнить данный запрос, считая его незаконным и нарушающим права пользователей Telegram на уважение частной жизни и свободу выражения мнения. Так, генеральный директор Павел Дуров заявлял:

«Глава Роскомнадзора заявил, что Telegram должен выдать спецслужбам “ключи для дешифрации”, чтобы те могли читать переписку пользователей и ловить террористов. 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»<sup>9</sup>.

**«Стремление ФСБ получить доступ к личной переписке является попыткой расширить свое влияние за счет конституционного права граждан»<sup>10</sup>.**

«Во всем мире, включая Россию, Telegram обрабатывает запросы на удаление публично доступного противоправного контента, содержащего пропаганду терроризма, детскую порнографию и т. д. Вместе с тем, **ни в одной стране мы не выдаем личные данные пользователей государственным органам»<sup>11</sup>.**

24. 31 октября 2017 года в интернет-издании Republic были опубликованы результаты журналистского расследования, согласно которому, два из шести упомянутых в запросе ФСБ телефонных номеров принадлежали братьям Азимовым – предполагаемым организаторам взрыва в метро Санкт-Петербурга в апреле 2017 года:

«Впрочем, на момент, когда ФСБ отправляла запрос в Telegram, телефоны Азимовых уже три месяца находились в руках оперативников. Также из материалов дела следует, что для связи с куратором из террористического «Исламского государства» один из братьев использовал не Telegram, а WhatsApp»<sup>12</sup>.

#### *Дело об административном правонарушении в отношении Заявителя*

25. 14 сентября 2017 года старшим консультантом организационно-аналитического управления Научно-технической службы ФСБ России Овчинниковым в отношении Заявителя, в отсутствие представителя или защитника, был составлен протокол №137/2/2/3904 об административном правонарушении согласно которому по состоянию на 30 августа 2017 года Заявителем не исполнен запрос ФСБ, врученный ему 21 июля 2017 года, о предоставлении в срок до 19 июля 2017 года информации для декодирования.

9

[https://vk.com/durov?w=wall\\_1840829](https://vk.com/durov?w=wall_1840829)

10

[https://vk.com/durov?w=wall\\_2061401](https://vk.com/durov?w=wall_2061401)

11

[https://vk.com/durov?w=wall\\_2083400](https://vk.com/durov?w=wall_2083400)

12

Илья Рождественский. Шесть номеров. Из-за чего в России собираются заблокировать Telegram. Republic.ru, 31 октября 2017 года // <https://republic.ru/posts/87312>

Тем самым Заявителем совершено административное правонарушение, предусмотренное частью 2.1 статьи 13.31 Кодекса Российской Федерации об административных правонарушениях (КоАП) «неисполнение организаторов распространения информации в сети «Интернет» обязанности предоставлять в федеральный орган исполнительной власти в области обеспечения безопасности информацию, необходимую для декодирования принимаемых, передаваемых, доставляемых и (или) обрабатываемых электронных сообщений» (приложение 5).

26. 16 октября 2017 года мировой судья судебного участка №383 Мещанского района Москвы, в отсутствие представителя или защитника Заявителя, а также прокурора и представителя Федеральной службы безопасности, было вынесено постановление, которым Заявитель был признан виновным в совершении вышеуказанного административного правонарушения (приложение 6).

27. Мировая судья в постановлении указала, что бездействие Заявителя образует состав административного правонарушения по ч.2.1 ст. 13.31 КоАП, признала Заявителя виновным и назначила ему наказание в виде штрафа в сумме 800 000 рублей.

28. 26 октября 2017 года защита Заявителя подала в Мещанский районный суд Москвы жалобу на постановление по делу об административном правонарушении (приложение 7).

29. По мнению защиты, дело было рассмотрено с грубыми нарушениями норм материального и процессуального права. Доводы защиты в общем сводились к следующему:

*а) Незаконность требований ФСБ.*

а1 - Контроль переговоров может осуществляться лишь во исполнение и на основании судебного решения. В данном деле ФСБ России не представила ни компании, ни суду судебные решения, позволяющие убедиться в наличии законной цели, оснований и в соблюдении порядка ограничения конституционных прав граждан. При таких обстоятельствах Заявитель в силу профессиональных обязанностей по обеспечению тайны переписки пользователей, не имел права предоставлять ФСБ запрошенную информацию.

а2 - ФСБ не был соблюден установленный российским законодательством и Европейской конвенцией о взаимной правовой помощи по уголовным делам порядок запроса информации у иностранной компании.

а3 - Запрос не предполагал альтернативного способа контроля переговоров, интересующих ФСБ лиц, например, предоставления расшифрованной переписки, создавая серьезную угрозу безопасности коммуникаций всех пользователей сервиса. Фактически, ФСБ просила создать возможность декодирования сообщений пользователей, но безопасности коммуникаций угрожало бы не только предоставление ФСБ ключей декодирования, но даже самое существование такой таких ключей. При этом ФСБ в нарушение собственных регламентов просила передать запрошенную информацию по незащищенному каналу связи, отправив ее в интернет-приемную ФСБ на публичный адрес электронной почты [fsb@fsb.ru](mailto:fsb@fsb.ru). Передача Заявителем ключей шифрования

указанным в запросе способом нарушила бы нормативные акты самой ФСБ, создала бы условия для несанкционированного доступа к этим сведениям третьих лиц, не обладающих специальными познаниями и не уведомленными о значимости сведений.

a4 – Требование ФСБ было неисполнимым, поскольку используемый сервисом алгоритм end-to-end шифрования предусматривает, что лишь отправитель и получатель обладают общим ключом (end-to-end шифрование) для пересылаемых сообщений. Сообщения в секретных чатах не дублируются на сервере компании и не расшифровываются администратором сервера, история переписки сохраняется лишь непосредственно на тех двух устройствах, на которых был создан чат.

*b) Процессуальные нарушения*

b1 – Дело Заявителя, являющегося иностранной компанией, было рассмотрено судом с нарушением подсудности.

b2 – Органом, составившим протокол об административном правонарушении (приложение 5) и судом также были нарушены требования КоАП, касающиеся привлечения к ответственности иностранного юридического лица – к делу не был привлечен переводчик, уполномоченным органам власти Великобритании не был направлен запрос об оказании правовой помощи.

b3 – Суд принял на себя функции обвинения. Поскольку дело в отношении Заявителя затрагивало интересы не только частной компании, но и права миллионов пользователей сервиса Telegram, оно очевидно требовало поиска баланса между защитой публичных интересов и обеспечением гарантий на онлайн-безопасность пользователей. При таких обстоятельствах суд первой инстанции обязан был рассмотреть вопрос о привлечении прокурора и даче им заключения в части защиты прав неопределенного круга лиц, обеспечить обязательное участие представителя органа, составившего протокол, в целях всестороннего и полного выяснения всех обстоятельств дела. Тем не менее, дело затрагивающее интересы 100 млн. человек, в отношении иностранной компании с капитализацией свыше 1 млрд. долларов США, мировой судья рассмотрела единолично - в отсутствие защитника, представителя ФСБ, государственного обвинителя, переводчика.

30. В жалобе защита также просила суд второй инстанции обеспечить участие в рассмотрении жалобы органа, возбудившего дело об административном правонарушении, и прокурора.

31. 10 декабря 2017 года Мещанский районный суд Москвы рассмотрел жалобу защиты Заявителя, прокурор и представитель ФСБ России в судебное заседание не вызывались, по собственной инициативе не явились.

32. В начале судебного заседания защита Заявителя подала суду следующие ходатайства:

a) о ведении письменного протокола судебного заседания (приложение 8);

b) о вызове в суд для участия представителя ФСБ, как органа, составившего протокол по делу об административном правонарушении (приложение 9);

- с) о привлечении к участию в деле прокурора (приложение 10);
- d) о вызове для допроса в качестве свидетеля должностного лица ФСБ, направившего 12 июля 2017 года Заявителю запрос о предоставлении доступа к переписке (приложение 11);
- e) об истребовании в ФСБ либо Московском городском суде судебных решения, поименованные в запросе (приложение 11);
- f) о вызове для допроса переводчика (приложение 11);
- g) об истребовании в ФСБ нормативного акта, регламентирующего порядок использования почтового ящика [fsb@fsb.ru](mailto:fsb@fsb.ru);
- h) допросить в качестве свидетеля явившегося в суд уполномоченного при президенте Российской Федерации по защите прав предпринимателей в сфере интернете (интернет-омбудсмена);
- i) опросить явившегося в суд специалиста по техническим вопросам (приложение 11);
- j) в связи с необходимостью выявления конституционно-правового смысла применяемых в настоящем деле норм Федерального закона «Об информации, информационных технологиях и о защите информации» (п.48 Дополнения) и приказа ФСБ России № 432 от 19 июля 2016 года (п.50 Дополнения), направить в Конституционный Суд Российской Федерации запрос в целях получения разъяснений по соответствующему вопросу (приложение 12).

33. Все указанные ходатайства защиты были отклонены судом, указавшим, что не находит основания для из удовлетворения (приложение

34. Защитой также были представлены следующие доказательства:

- a) доклад уполномоченного при президенте Российской Федерации по защите прав предпринимателей в сфере интернете (интернет-омбудсмена), согласно которому Telegram является значимым сервисом для российских пользователей, использующих его в качестве важной коммуникационной среды, в том числе в предпринимательской деятельности. Компрометация используемых сервисом алгоритмов шифрования угрожает безопасности коммуникаций, утечкой личной информации и персональных данных, иногда – и физической безопасности пользователей. Поскольку в настоящее время end-to-end шифрование используется множеством популярных сервисом, дискредитация Telegram скорее всего приведет к тотальному отказу пользователей от сервиса в пользу конкурентов (приложение 14);
- b) заключение специалиста по техническим вопросам Щурова, согласно которому в случае использования end-to-end шифрования, как это реализовано в “секретных чатах” Telegram, ключи шифрования вырабатывается непосредственно на устройствах пользователей и никто, включая разработчика программного обеспечения сервиса и лиц, имеющих контроль над его серверной инфраструктурой не имеет технической возможности изготовить ключевую информацию, необходимую и достаточную для расшифровки сообщений. При этом, предложенный ФСБ в качестве канала связи адрес электронной почты [fsb@fsb.ru](mailto:fsb@fsb.ru) является уязвимым к перехвату и передавать по нему



конфиденциальную информацию небезопасно (приложение 15);

с) заключение специалиста по техническим вопросам Веснина, согласно которому, получение единого универсального ключа для расшифровки всего трафика Telegram невозможно технически и организационно, а электронная почта является ненадежным способом передачи конфиденциальной информации (приложение 15).

д) протоколы допроса в качестве подозреваемых по делу о взрыве в метро Санкт-Петербурга Акрама и Аброра Азимовых, где указывается, что они не пользовались мессенджером Telegram, а телефонные номера не использовали с апреля 2017 года (приложение 16).

35. Также в судебном заседании защитой были представлены дополнительные доводы по существу дела о том, что примененный в деле приказ ФСБ России №432 от 19 июля 2016 года (далее – «приказ ФСБ», п.50 Дополнения), не мог быть применен, поскольку принят неуполномоченным органом власти с превышением полномочий и прямо противоречит федеральному законодательству:

а) порядок взаимодействия организаторов распространения информации с уполномоченными государственными органами в сфере оперативно-розыскной деятельности или обеспечения безопасности, должен быть установлен не ФСБ, а Правительством России, которое до настоящего времени не приняло соответствующего нормативного акта;

б) приказ ФСБ вопреки требованиям законодательства не прошел общественное обсуждение;

с) приказ ФСБ противоречит уголовно-процессуальному законодательству, поскольку не содержит гарантий неприкосновенности частной жизни, поскольку не требует от ФСБ предоставлять судебные акты, разрешающие контроль переписки;

д) приказ ФСБ содержит неопределенные, трудновыполнимые и(или) обременительные требования к гражданам и организациям в том, что касается неопределенности срока и способа передачи информации, условий ее хранения, а также отсутствия гарантий секретности полученных ФСБ сведений (приложение 17).

36. В тот же день Мещанский районный суд Москвы вынес решение, которым полностью отказал в удовлетворении жалобы защиты и оставил постановление мирового судьи без изменения (приложение 18).

37. Суд указал, что факт совершения Заявителем административного правонарушения и вина Заявителя подтверждаются протоколом об административном правонарушении, копией письма-запроса ФСБ и сведениями о юридическом лице Заявителя, которым мировым судьей дана надлежащая оценка.

38. Суд оценил как несостоятельный довод жалобы о том, что дело было рассмотрено с нарушением подсудности, поскольку место совершения правонарушения в форме бездействия следует считать место, где должно было

быть совершено действие.

39. Также суд указал, что ссылки защиты на незаконность требования ФСБ, противоречащего ст.23 и 55 Конституции России и статье 8 Конвенции, основаны на неправильном толковании закона и не могут служить основанием для отмены постановления по делу, так как *«по общему смыслу положений Конвенции, административное наказание иностранного юридического лица на территории России, на право тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, допускается в тех случаях, когда оно необходимо в демократическом обществе и соразмерно публично-правовым целям»*<sup>13</sup>.

40. Иные доводы жалобы суд счел «голословными», указав, что они *«к существу вменяемого административного правонарушения не относятся, и не имеют правового значения для отмены или изменения обжалуемого постановления мирового судьи»*.

41. 5 декабря 2017 года защита Заявителя подала в Верховный Суд Российской Федерации административный иск к ФСБ о признании недействующим Приказа Федеральной службы безопасности Российской Федерации от 19 июля 2016 г. №432 «Об утверждении Порядка представления организаторами распространения информации в информационно-телекоммуникационной сети «Интернет» в Федеральную службу безопасности Российской Федерации информации, необходимой для декодирования принимаемых, передаваемых, доставляемых и (или) обрабатываемых электронных сообщений пользователей информационно-телекоммуникационной сети «Интернет» (приложение 19).

42. Доводы административного иска в целом повторяют в соответствующей части аргументацию, изложенную в жалобе на постановление по делу об административном правонарушении. Рассмотрение иска Верховным Судом назначено на 20 марта 2018 года.

## СООТВЕТСТВУЮЩЕЕ НАЦИОНАЛЬНОЕ ЗАКОНОДАТЕЛЬСТВО

### I. Право на уважение частной жизни и корреспонденции

#### 43. Конституция Российской Федерации

##### Статья 23

1. Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.
2. Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения.

##### Статья 24

1. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются.

---

13

Здесь и далее, цитаты из текстов официальных документов приводятся дословно с сохранением орфографии и пунктуации.

<...>

44. *Федеральный закон от 7 июля 2003 года N 126-ФЗ «О связи»*

Статья 63. Тайна связи

1. На территории Российской Федерации гарантируется тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и сетям почтовой связи.

Ограничение права на тайну переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и сетям почтовой связи, допускается только в случаях, предусмотренных федеральными законами.

2. Операторы связи обязаны обеспечить соблюдение тайны связи.

<...>

45. *Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 года N 174-ФЗ*

Статья 13. Тайна переписки, телефонных и иных переговоров, почтовых, телеграфных и иных сообщений

1. Ограничение права гражданина на тайну переписки, телефонных и иных переговоров, почтовых, телеграфных и иных сообщений допускается только на основании судебного решения.

<...>

46. *Федеральный закон от 12 августа 1995 г. N 144-ФЗ "Об оперативно-розыскной деятельности"*

Статья 9. Основания и порядок судебного рассмотрения материалов об ограничении конституционных прав граждан при проведении оперативно-розыскных мероприятий

Рассмотрение материалов об ограничении конституционных прав граждан на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, передаваемых по сетям электрической и почтовой связи, на неприкосновенность жилища при проведении оперативно-розыскных мероприятий осуществляется судом, как правило, по месту проведения таких мероприятий или по месту нахождения органа, ходатайствующего об их проведении.

<...>

47. *Уголовный кодекс Российской Федерации от 13 июня 1996 года №63-ФЗ*

Статья 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений

1. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан -

<...>

2. То же деяние, совершенное лицом с использованием своего служебного положения, -

<...>

II. Специальные положения законодательства, регулирующие обязанности и ответственность интернет-сервисов

48. *Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации»*

Статья 10.1. Обязанности организатора распространения информации в сети "Интернет"

1. Организатором распространения информации в сети "Интернет" является лицо, осуществляющее деятельность по обеспечению функционирования информационных систем и (или) программ для электронных вычислительных машин, которые предназначены и (или) используются для приема, передачи, доставки и (или) обработки электронных сообщений пользователей сети "Интернет".

<...>

3. Организатор распространения информации в сети "Интернет" обязан хранить на территории Российской Федерации:

1) информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков, видео- или иных электронных сообщений пользователей сети "Интернет" и информацию об этих пользователях в течение одного года с момента окончания осуществления таких действий;

2) текстовые сообщения пользователей сети "Интернет", голосовую информацию, изображения, звуки, видео-, иные электронные сообщения пользователей сети "Интернет" до шести месяцев с момента окончания их приема, передачи, доставки и (или) обработки. Порядок, сроки и объем хранения указанной в настоящем подпункте информации устанавливаются Правительством Российской Федерации.

3.1. Организатор распространения информации в сети "Интернет" обязан предоставлять указанную в пункте 3 настоящей статьи информацию уполномоченным государственным органам, осуществляющим оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации, в случаях, установленных федеральными законами.

<...>

4.1. Организатор распространения информации в сети "Интернет" обязан при использовании для приема, передачи, доставки и (или) обработки электронных сообщений пользователей сети "Интернет" дополнительного кодирования электронных сообщений и (или) при предоставлении пользователям сети "Интернет" возможности дополнительного кодирования электронных сообщений представлять в федеральный орган исполнительной власти в области обеспечения безопасности информацию, необходимую для декодирования принимаемых, передаваемых, доставляемых и (или) обрабатываемых

электронных сообщений.

<...>

Статья 15.4. Порядок ограничения доступа к информационному ресурсу организатора распространения информации в сети "Интернет"

1. В случае установленного вступившим в законную силу постановлением по делу об административном правонарушении неисполнения организатором распространения информации в сети "Интернет" обязанностей, предусмотренных статьей 10.1 настоящего Федерального закона, в его адрес (адрес его филиала или представительства) уполномоченным федеральным органом исполнительной власти направляется уведомление, в котором указывается срок исполнения таких обязанностей, составляющий не менее чем пятнадцать дней.

2. В случае неисполнения организатором распространения информации в сети "Интернет" в указанный в уведомлении срок обязанностей, предусмотренных статьей 10.1 настоящего Федерального закона, доступ к информационным системам и (или) программам для электронных вычислительных машин, которые предназначены и (или) используются для приема, передачи, доставки и (или) обработки электронных сообщений пользователей сети "Интернет" и функционирование которых обеспечивается данным организатором, до исполнения таких обязанностей ограничивается оператором связи, оказывающим услуги по предоставлению доступа к сети "Интернет", на основании вступившего в законную силу решения суда или решения уполномоченного федерального органа исполнительной власти.

<...>

*49. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. N 195-ФЗ*

Статья 13.31. Неисполнение обязанностей организатором распространения информации в сети "Интернет"

2.1. Неисполнение организатором распространения информации в сети "Интернет" обязанности предоставлять в федеральный орган исполнительной власти в области обеспечения безопасности информацию, необходимую для декодирования принимаемых, передаваемых, доставляемых и (или) обрабатываемых электронных сообщений, -

влечет наложение административного штрафа на граждан в размере от трех тысяч до пяти тысяч рублей; на должностных лиц - от тридцати тысяч до пятидесяти тысяч рублей; на юридических лиц - от восьмисот тысяч до одного миллиона рублей.

*50. Приказ ФСБ России от 19 июля 2016 г. №432 «Об утверждении Порядка представления организаторами распространения информации в информационно-телекоммуникационной сети "Интернет" в Федеральную службу безопасности Российской Федерации информации, необходимой для декодирования принимаемых, передаваемых, доставляемых и (или) обрабатываемых электронных сообщений пользователей информационно-телекоммуникационной сети "Интернет"»*

<...>

2. Уполномоченным подразделением Федеральной службы безопасности Российской Федерации по получению от организаторов распространения информации в сети "Интернет" информации для декодирования является Организационно-аналитическое управление Научно-технической службы Федеральной службы безопасности Российской Федерации (далее - уполномоченное подразделение).
3. Организатор распространения информации в сети "Интернет" осуществляет передачу информации для декодирования на основании запроса уполномоченного подразделения, подписанного начальником (заместителем начальника) уполномоченного подразделения.
4. Запрос направляется уполномоченным подразделением в письменном виде заказным почтовым отправлением с уведомлением о вручении.
5. В запросе указываются состав (формат) и адрес предоставления информации для декодирования.
6. Информация для декодирования передается организаторами распространения информации в сети "Интернет" на магнитном носителе по почте (в форме электронного сообщения по электронной почте) по адресу, указанному в запросе, либо по согласованию с уполномоченным подразделением организуется доступ уполномоченного подразделения к информации для декодирования.

***Г. Изложение имевших место нарушений Конвенции или протоколов к ней и подтверждающих доводов***

*Нарушение статьи 6 Конвенции*

51. Ссылаясь на «критерии Энгеля»<sup>14</sup>, Заявитель утверждает, что несмотря на то, что он был привлечен к административной ответственности в порядке, предусмотренном национальным законодательством об административных правонарушениях, по своей сути разбирательство в отношении него относилось к уголовной сфере.

52. Во-первых, Федеральный закон «Об информации, информационных технологиях и о защите информации» регулирует все отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации, а также применении информационных технологий. Примененные в отношении Заявителя положения закона, по утверждению властей, направлены на облегчение уполномоченным органам в сфере безопасности, расследования и предупреждения преступлений террористического характера. Таким образом, целью разбирательства была защита публичного интереса, что является чертой, свойственной уголовному праву.

53. Во-вторых, указанный закон применяется в отношении неограниченного круга как физических, так и юридических лиц, владеющих интернет-ресурсами, позволяющими обмениваться сообщениями, и не является узкоспециальным. Так, статьи 10.1 и 15.4 закона (п.48 настоящего Дополнения) распространяются

---

14

Engel and Others v. Netherlands, 8 June 1976, Series A, N 22, §82

на случаи применения интернет-сервисами («организаторами распространения информации» в терминологии закона) шифрования при передаче сообщений.

54. В настоящее время в соответствующий реестр включено 98 интернет-сервисов, однако Роскомнадзор ранее официально объявил о том, что обязанности, предусмотренные соответствующими положениям закона, должны исполнять все интернет-сервисы, вне зависимости от включения их в реестр. (п.17 настоящего Дополнения). При этом решение о включение интернет-сервиса в реестр принимается исключительно Роскомнадзором без учета мнения владельца сервиса.

55. В этой связи необходимо также учесть, что шифрование в том или ином виде в настоящее время применяется абсолютным большинством интернет-сервисов<sup>15</sup>, которые таким образом подпадают под действие указанного закона.

56. В-третьих, само по себе нарушение положений указанного закона влечет за собой исключительно суровые санкции в виде штрафа в размере от 800 тысяч до 1 миллиона рублей. Штраф такого размера несомненно является наказанием, налагаемым с целью недопущения повторного нарушения, аналогично ситуации, рассмотренной Судом в деле *Bendenoun v France* (Merits and just satisfaction), no. 12547/86, 24 February 1994, §47.

57. Учитывая изложенное Заявитель полагает, что к его делу применима статья 6 Конвенции, и утверждает, что судебное разбирательство в отношении него не было справедливым, поскольку дело было рассмотрено ненадлежащим судом.

58. Заявитель утверждает, что мировой судья Мещанского района города Москвы не имел права рассматривать дело в отношении иностранной компании, находящейся за пределами Российской Федерации.

59. В соответствии с частью 1 статьи 29.5 КоАП РФ дело об административном правонарушении рассматривается по месту его совершения. Согласно Постановлению Пленума Верховного Суда РФ от 24 марта 2005 г. № 5 «при определении территориальной подсудности дел об административных правонарушениях, объективная сторона которых выражается в бездействии в виде неисполнения установленной правовым актом обязанности, *необходимо исходить из...места нахождения юридического лица*». Таким образом, в данном случае местом совершения правонарушения является территория иностранного государства – Соединенного Королевства Великобритании и Северной Ирландии, с которой у Российской Федерации отсутствует международный договор, регулирующий вопросы подсудности подобных дел.

60. Рассматривая апелляционную жалобу Заявителя, Мещанский районный суд Москвы не дал оценки данному доводу защиты, однако, вероятно, счел местом совершения административного правонарушения место нахождения Федеральной службы безопасности. Однако даже в этом случае мировой суд Мещанского района Москвы не имел права рассматривать дело Заявителя, поскольку в силу статьи 29.1.6 КоАП РФ, в случае совершения административного правонарушения на территории Российской Федерации

---

15

По данным Mozilla Foundation в настоящее время почти 70% мирового интернет-трафика передается в зашифрованном виде // <https://letsencrypt.org/stats/#percent-pageloads>

иностранным юридическим лицом и невозможности производства процессуальных действий с его участием на территории Российской Федерации все материалы возбужденного и расследуемого дела об административном правонарушении передаются в Генеральную прокуратуру Российской Федерации, которая решает вопрос об их направлении в компетентные органы иностранного государства для осуществления административного преследования. Этого сделано не было.

61. Заявитель также утверждает, что национальные суды фактически возложили на себя функции обвинения, рассмотрев дело об административном правонарушении, в отсутствие представителя ФСБ (органа, составившего протокол об административном правонарушении) и прокурора, который должен был поддерживать обвинение. Соответствующее ходатайство защиты было отвергнуто и Мещанским районным судом Москвы, рассматривавшим жалобу защиты Заявителя.

62. Заявитель обращает внимание на то, что дело в отношении него является первым прецедентом такого рода, ставшим предметом рассмотрения российскими судами.

63. Заявитель утверждает, что с учетом сложности и значимости дела Заявителя не только для компании-владельца сервиса Telegram, но и для миллионов пользователей, суды, рассматривавшие дело об административном правонарушении должны были проявить максимальную степень осмотрительности и продемонстрировать свою независимость и беспристрастность. Привлечение к участию в деле представителя ФСБ и прокурора, несомненно укрепило бы уверенность как Заявителя, так и общественности в справедливости разбирательства.

64. Таким образом Заявитель утверждает, что национальные суды, рассматривавшие дело, не были беспристрастными, ссылаясь на позицию Суда, высказанную в постановлении по делу *Karelin v. Russia*, no.926/08, 20 September 2016, §72, о том, что *неучастие в деле прокурора повлияло на действие презумпции невиновности в ходе судебного разбирательства и, как следствие, на вопрос о беспристрастности суда и наоборот.*

65. Заявитель подчеркивает то, что на всем протяжении своего участия в рассмотрении дела защита Заявителя требовала привлечь к участию прокурора и представителя ФСБ, в чем ей было отказано, то есть суд второй инстанции не устранил явно выявленное нарушение справедливости, допущенное мировым судьей.

#### *Нарушение статьи 10 Конвенции*

66. Заявитель утверждает, что привлечение его к административной ответственности в виде штрафа за отказ предоставить Федеральной службе безопасности России доступ к конфиденциальной переписке пользователей является вмешательством в его право свободно распространять информацию и идеи без какого-либо вмешательства со стороны публичных властей и независимо от государственных границ, гарантированное статье 10 Конвенции.



67. Заявитель утверждает, что такое вмешательство не было предусмотрено законом и не являлось необходимым в демократическом обществе.

Вмешательство не было основано на законе.

68. Европейский Суд неоднократно отмечал, что любое вмешательство в пользование правом на свободу выражения должно быть «предусмотрено законом», при этом норма может рассматриваться как «закон», только в том случае, если она сформулирована с достаточной точностью, чтобы позволить гражданину предвидеть, в той степени, какая целесообразна в данных обстоятельствах, последствия, которые может повлечь за собой определенное действие (см. *Editorial Board of Pravoye Delo and Shtekel v. Ukraine*, no. 33014/05, 5 May 2011, §51). В этой связи Заявитель ссылается на следующие обстоятельства.

69. Примененная в отношении Заявителя статья 10.1 Федерального закона «Об информации, информационных технологиях и о защите информации» (п. 48 настоящего Дополнения) не содержит четкого и исчерпывающего описания условий, при которых уполномоченному органу власти Российской Федерации должен быть предоставлен доступ к конфиденциальной переписке пользователей интернет-сервиса.

70. Приказ ФСБ России от 19 июля 2016 г. №432 (п.50 настоящего Дополнения) не содержит четкой описанной процедуры передачи конфиденциальной информации, разглашение которой серьезно угрожало бы онлайновой безопасности всех пользователей сервиса, а также не устанавливает срок, в течение которого запрос ФСБ должен быть выполнен.

71. 5 декабря 2017 года, то есть уже после того как Заявитель был привлечен к административной ответственности, ФСБ подготовила и выложила для общественного обсуждения проект приказа о внесении изменений в приказ №432 в части установления 10-дневного срока предоставления информации<sup>16</sup>. Таким образом, на момент привлечения Заявителя к ответственности срок исполнения подобного требований ФСБ российским законодательством установлен не был.

72. Положения указанной нормы федерального закона, а также приказ ФСБ сформулированы в чрезвычайно общих словах, допускающих произвольное толкование и применение, и не позволяющих администрации интернет-сервиса объективно оценить законность требований и последствия их исполнения или неисполнения.

73. Заявитель в этой связи ссылается на существовании фундаментального противоречия между положениями национального законодательства об обязанности операторов связи обеспечить тайну связи и соблюдение прав граждан при оказании услуг (п.43 – 46 настоящего Дополнения) и обязанностью организаторов распространения информации передать спецслужбам информацию, позволяющую декодировать переписку пользователей (п.48 и 50 настоящего Дополнения).

---

16

<http://regulation.gov.ru/projects#npa=75929>

74. Заявитель обращает внимание на то, что примененные в отношении него положения ст.10.1 Федерального закона «Об информации, информационных технологиях и о защите информации (п.48 настоящего Дополнения) не содержит требования предварительно получить судебное разрешение на доступ к переписке пользователей.

75. Сотрудники компании, выполнившей подобный запрос российских спецслужб подвергались бы постоянной угрозе привлечения к уголовной ответственности по ст.138 УК РФ об ответственности за нарушение неприкосновенности частной жизни в отсутствие судебного разрешения (п.47 настоящего Дополнения).

76. Также Заявитель обращает внимание на то, что примененный в его деле приказ ФСБ противоречит требованиям федерального законодательства и был принят неуполномоченным органом власти с нарушением установленного порядка. Детальное обоснование этого защита Заявителя представила при рассмотрении апелляционной жалобы Мещанский районным судом Москвы (п. 35 настоящего Дополнения, приложение 18), однако все соответствующие аргументы были оставлены без внимания судом.

77. Таким образом, вмешательство не было предусмотрено законом.

*Вмешательство не было необходимым в демократическом обществе.*

78. Заявитель утверждает, что в его деле российские власти даже не пытались установить баланс между необходимостью противодействия терроризму и обеспечения общественной безопасности и защитой прав граждан на уважение частной жизни и права Заявителя на распространение информации.

79. ФСБ требовала от Заявителя предоставить неограниченный по времени доступ к конфиденциальной переписке шести возможных пользователей сервиса Telegram, не предоставив судебных актов, разрешающих такой доступ.

80. Кроме того, ФСБ не давала гарантий безопасности запрошенных ключей шифрования, предложив направить ей критически важную информацию по незащищенному каналу связи на адрес интернет-приемной Службы, доступ к которому, вероятно, имеется у значительного числа сотрудников, что очевидно, не позволяет полностью исключить возможность несанкционированного доступа посторонних лиц к охраняемой законом информации (п.21 настоящего Дополнения).

81. В соответствии с информацией, размещенной на сайте, адрес данной электронной почты является одним из каналов обращения граждан в Службу, по которым **запрещено** передавать сведения ограниченного распространения<sup>17</sup>, к которым, безусловно, относится запрошенная ФСБ информация о дешифровании переписки между пользователями мессенджера Telegram.

82. У Заявителя не имелось возможности предоставить запрошенную информацию, поскольку в силу технических особенностей архитектуры сервиса,

---

17

<http://www.fsb.ru/fsb/supplement.htm>

ключи шифрования секретных чатов генерируются непосредственно на устройствах пользователей, и администратор сервиса не имеет к ним доступа. При таких обстоятельствах требование предоставить ключи шифрования фактически означает требование создать бэкдор (т.н. дефект алгоритма, который намеренно встраивается в него разработчиком и позволяет получить несанкционированный доступ к данным).

83. Заявитель в этой связи ссылается на позицию Специального докладчика ООН по вопросу о праве на свободу убеждений и их свободное выражение, указывающего: *«все технические специалисты единодушны во мнении о том, что не существует особого доступа, который можно было бы открыть только для органов власти, даже для тех из них, кто в принципе руководствуется интересами населения. В существующей технологической среде намеренная компрометация ключей шифрования, даже в предположительно законных целях, подрывает онлайн-безопасность всех пользователей»* (см. Доклад Совету по правам человека ООН А/НRC/29/32).

84. Заявитель дополнительно ссылается на заключение Суда о том, что *российские правовые нормы, регулирующие перехват сообщений, не предусматривают адекватных и эффективных гарантий против произвола и риска злоупотребления, который присущ любой системе тайного наблюдения, и который является особенно высоким в системе, где спецслужбы и полиция обладают прямым доступом, с помощью технических средств, ко всем мобильным телефонным переговорам* (см. *Roman Zakharov v. Russia*, no.47143/06, 4 December 2015, §302), полагая что указанное в полной мере относится к принятым впоследствии положениям российского законодательства об организаторах распространения информации и «пакету Яровой» (пп. 9, 48 и 50 настоящего Дополнения).

85. Заявитель также обращает внимание на представленные в ходе рассмотрения апелляционной жалобы доказательства того, что ФСБ намеренно вводила суд в заблуждение относительно получения информации по запрошенным телефонным номерам. В частности, двое подозреваемых в совершении террористической атаки в Санкт-Петербурге в апреле 2017 года, которым принадлежат как минимум два из перечисленных в запросе ФСБ телефонных номера, дали показания, что они никогда не использовали сервис Telegram, а телефонными номерами не пользовались с апреля 2017 года, поскольку находились с следственным изолятором (п. 34(d) настоящего Дополнения, приложение 17).

86. Как следует из материалов журналистского расследования издания Republic (п.24 настоящего Дополнения), на которые также ссылалась защита Заявителя, лишь три из запрошенных номеров были привязаны к аккаунтам в сервисе Telegram.

87. При таких обстоятельствах, когда отсутствовали какие бы то ни было доказательства возможности достижения декларируемых российскими властями целей противодействия терроризму, а в ходе рассмотрения дела было выявлено возможное предоставление ФСБ недостоверной информации, привлечение Заявителя к административной ответственности за отстаивание прав пользователей на приватность и конфиденциальность, сопровождающееся

реальной угрозой блокировки сервиса на территории Российской Федерации, представляется явно неадекватной реакцией. Следовательно, вмешательство не было необходимым в демократическом обществе.

*Нарушение статьи 13 Конвенции*

88. В соответствии со статьей 13 Конвенции каждый, чьи права и свободы, признанные в настоящей Конвенции, нарушены, имеет право на эффективное средство правовой защиты в государственном органе, даже если это нарушение было совершено лицами, действовавшими в официальном качестве.

89. Привлечение Заявителя к административной ответственности и реальная угроза блокировки сервиса на территории Российской Федерации право нарушило его право свободно распространять информацию без какого-либо вмешательства со стороны публичных властей, и независимо от государственных границ. Между тем национальные суды фактически отказались рассматривать жалобу Заявителя по существу с точки зрения гарантий, установленных статьей 10 Конвенции.

90. Заявитель был привлечен к административной ответственности на том основании, что им не была исполнена обязанность по предоставлению в Управление ФСБ России запрошенной информации. При этом доводы защиты Заявителя о том, что у него не имелось технической возможности предоставить информацию для декодирования сообщений конкретных пользователей, а создание бэкдора угрожало бы безопасности всех пользователей сервиса, а самое требование ФСБ было незаконным даже не рассматривались, соответствующие ходатайства защиты были отклонены без мотивировки (пп. 32 и 33 настоящего Дополнения, приложение 13).

91. Вместо того, чтобы по существу оценить аргументы Заявителя, национальные суды лишь формально проверили действия Федеральной службы безопасности на соответствие статье 10.1 Федерального закона «Об информации...» и приказа ФСБ №432.

92. Таким образом, Заявитель, несмотря на соблюдение формальной процедуры рассмотрения дела об административном правонарушении, фактически был лишен возможности предоставлять доказательства и приводить аргументы в свою защиту, то есть лишен права на эффективное средство правовой защиты.

---

Дамир Гайнутдинов