EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

ТРЕТЬЯ СЕКЦИЯ

ДЕЛО «ПОДЧАСОВ ПРОТИВ РОССИИ»

(Заявление №33696/19)

РЕШЕНИЕ

Статья 8 • Частная жизнь • Корреспонденция • Законодательное требование для «организаторов Интернет-коммуникаций» собирать и хранить Интернет-сообщения и связанные с ними данные, предоставлять правоохранительным органам или службам безопасности доступ к этим данным и расшифровывать зашифрованные сообщения • Законодательство, предусматривающее чрезвычайно широкую обязанность по хранению данных, тем самым делая вмешательство чрезвычайно обширным и серьезным • Недостаточные и неадекватные гарантии против злоупотреблений, связанных с доступом правоохранительных органов к хранимым Интернет-сообщениям и связанным с ними данным • Законодательное требование расшифровывать сквозное шифрование несоразмерно • Оспариваемое законодательство не «необходимо в демократическом обществе» • Превышение пределов усмотрения

Подготовлено Секретариатом. Не является обязательным для Суда.

СТРАСБУРГ

13 Февраля 2024 ГОДА

ОКОНЧАТЕЛЬНОЕ

13/05/2024

Настоящее решение стало окончательным в соответствии со статьей 44 § 2 Конвенции.
Оно может подлежать редакционной правке.

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

В деле «Подчасов против России»,

Европейский Суд по правам человека (Третья секция), заседая в составе Палаты, состоящей из:

Пер Пастор Виланова, *Председатель*,
Джолиен Шуккинг,
Йонко Грозев,
Георгиос А. Сергхидес,
Пеетер Роосма,
Иоаннис Ктистакис,
Оддни Мьолль Арнардоттир, *судьи*,

и Ольги Чернышевой, *заместителя Секретаря секции*,

рассмотрев:

заявление (№ 33696/19) против Российской Федерации, поданном в Суд в соответствии со статьей 34 Конвенции о защите прав человека и основных свобод («Конвенция») гражданином России г-ном Антоном Валерьевичем Подчасовым («заявитель») 18 июня 2019 года;

решение уведомить российское правительство («Правительство») о заявлении;

замечания, представленные Правительством, и замечания в ответ, представленные заявителем;

комментарии, представленные Европейским институтом информационного общества и Privacy International, которым было предоставлено разрешение на участие Президентом секции;

решение Председателя секции назначить одного из действующих судей Суда для выполнения функций *ad hoc* судьи, применяя по аналогии правило 29 § 2 Регламента Суда (см. объяснение в деле «*Кутаев против России*», № 17912/15, §§ 5-8, 24 января 2023 года);

Рассмотрев дело в закрытом заседании 9 января 2024 года,

Провозглашает следующее решение, которое было принято в этот день:

ВВЕДЕНИЕ

1. Дело касается законодательного требования к «организаторам распространения информации в сети Интернет» хранить все данные о сообщениях в течение одного года и содержимое всех сообщений в течение шести месяцев, а также предоставлять эти данные правоохранительным органам или службам безопасности в установленных законом случаях, вместе с информацией, необходимой для расшифровки электронных сообщений, если они зашифрованы.

ФАКТЫ

2. Заявитель родился в 1981 году и проживает в Барнауле. Его представлял адвокат из Москвы, господин С. Дарбинян.

3. Правительство первоначально представлял г-н А. Федоров, бывший представитель Российской Федерации в Европейском суде по правам человека, а позже его преемник на этом посту, г-н М. Виноградов.

4. Обстоятельства дела могут быть изложены следующим образом.

5. Заявитель является пользователем Telegram, мессенджера, который можно использовать бесплатно на различных устройствах, таких как мобильные телефоны, планшеты или компьютеры. Этим приложением пользуются миллионы людей в России и по всему миру. Согласно официальному сайту Telegram, по умолчанию в «облачных чатах» не используется сквозное (клиент-клиент) шифрование, а вместо этого применяется собственная схема шифрования сервер-клиент. Однако можно переключиться на сквозное шифрование, активировав функцию «секретного чата». На официальном сайте говорится, в частности:

> «Все сообщения в секретных чатах используют сквозное шифрование. Это означает, что только вы и получатель можете читать эти сообщения – никто другой не может их расшифровать, включая нас здесь, в Telegram».

6. 28 июня 2017 года Telegram Messenger LLP был внесен в специальный публичный реестр как «организатор Интернет коммуникации» (*организатор распространения информации в сети Интернет* – далее «ОКИ»). Это влекло за собой обязательство Telegram хранить все данные о сообщениях в течение одного года и содержимое всех сообщений в течение шести месяцев, а также предоставлять эти данные правоохранительным органам или службам безопасности в установленных законом случаях, вместе с информацией, необходимой для расшифровки электронных сообщений, если они зашифрованы (см. пункты 17-25 ниже).

7. 12 июля 2017 года Федеральная служба безопасности («ФСБ») потребовала от Telegram Messenger LLP раскрыть техническую информацию, которая способствовала бы «расшифровке сообщений с 12 июля 2017 года в отношении пользователей Telegram, подозреваемых в террористической деятельности». Запрос на раскрытие ссылался на статью 10.1(4.1) Закона об информации и Приказ № 432 от 19 июля 2016 года (см. пункты 20 и 24 ниже). В нем было указано шесть номеров мобильных телефонов, связанных с учетными записями Telegram Messenger, и шесть судебных решений, вынесенных 10 июля 2017 года. Требовалось, чтобы Telegram Messenger LLP предоставил, среди прочего, IP-адрес, номер TCP/UDP порта и «данные, относящиеся к [шифровальным] ключам» (*ключевой материал*), которые были бы «необходимы и достаточны» для расшифровки сообщений. Информация должна была быть направлена до 19 июля 2017 года на адрес электронной почты ФСБ.

8. Telegram Messenger LLP отказался выполнить запрос на раскрытие, аргументируя это тем, что технически невозможно выполнить его без создания «бэкдора», который ослабил бы механизм шифрования для всех пользователей. Компания объяснила, в частности, что шесть пользователей, указанных в запросе на раскрытие, включили функцию «секретного чата» и, следовательно, использовали сквозное шифрование. 12 декабря 2017 года Компания была оштрафована Мещанским районным судом Москвы. Впоследствии, решением Таганского районного суда Москвы от 13 апреля 2018 года было принято решение о блокировке приложения Telegram в России. Оба решения были подтверждены в апелляционном порядке.

9. 12 марта 2018 года заявитель вместе с тридцатью четырьмя другими лицами оспорил запрос на раскрытие в суде. Истцы утверждали, что предоставление шифровальных ключей, как того требует ФСБ, позволит расшифровывать сообщения всех пользователей. Это, по их мнению, нарушит их право на уважение частной жизни и на конфиденциальность их сообщений. После получения ключей шифрования ФСБ получит возможность технического доступа ко всем сообщениям без санкции суда, требуемого по российскому законодательству. Они указывали на широкий охват статьи 10.1 Закона об информации (см. пункты 16-23 ниже) как на правовое основание для вмешательства и отсутствие гарантий против потенциально необоснованного раскрытия их личной информации.

10. 22 марта 2018 года Мещанский районный суд отказал в иске установив, что оспариваемый запрос на раскрытие не затрагивает права истцов. Решение об отказе не содержало дальнейших доводов.

11. 22 мая 2018 года Московский городской суд подтвердил в апелляционном порядке решение об отказе.

12. 10 сентября 2018 года судья Московского городского суда отказал в передаче кассационной жалобы, поданной заявителем, для её рассмотрения в Московском городском суде, установив отсутствие значительных нарушений материального или процессуального права, повлиявших на исход дела.

13. Дальнейшая кассационная жалоба заявителя была отклонена 16 января 2019 года Верховным судом Российской Федерации.

14. Приложение Telegram Messenger все еще доступно и функционирует в России.

СООТВЕТСТВУЮЩАЯ ПРАВОВАЯ БАЗА

15. Для краткого изложения национальных положений о тайном наблюдении за линиями связи, включая соответствующие положения Уголовно-процессуального Кодекса и Закона об оперативно-розыскной деятельности, см. дело «*Роман Захаров против России*» ([GC], no. 47143/06, §§ 15-138, ECHR 2015).

16. Статья 10.1 Федерального закона № 149-ФЗ от 27 июля 2006 года «Об информации, информационных технологиях и защите информации» («Закон об информации») была введена в этот закон в 2014 году. Она определяет ОКИ и перечисляет его установленные законом обязанности.

17. ОКИ определяется как лицо или организация, обеспечивающие функционирование информационных систем и/или программ для электронных устройств с целью получения, передачи, доставки и/или обработки электронных сообщений в Интернете (статья 10.1(1) Закона об информации).

18. В июле 2016 года для ОКИ были введены следующие обязательства.

19. ОКИ должен хранить на территории России все данные о сообщениях пользователей Интернета в течение одного года и содержимое всех сообщений в течение шести месяцев. Это обязательство касается голосовых, текстовых, визуальных, звуковых, видео или других электронных сообщений, отправленных, полученных, переданных или обработанных пользователями Интернета (статья 10.1(3)).

20. ОКИ должен предоставить информацию, упомянутую в статье 10.1(3), правоохранительным органам или службам безопасности в установленных законом случаях (статья 10.1(3.1)). Также он должен предоставить любую информацию, необходимую для расшифровки электронных сообщений, если они зашифрованы (статья 10.1(4.1)).

21. Оборудование, установленное ОКИ, должно соответствовать техническим требованиям, установленным правительством, и позволять

правоохранительным органам и службам безопасности выполнять свои задачи (статья 10.1(4)).

22. В контексте предоставления услуг мгновенного обмена сообщениями, ОКИ должен, помимо вышеуказанных требований, идентифицировать пользователей таких услуг по их номерам мобильных телефонов (статья 10.1(4.2)(1)).

23. Объем информации, которой необходимо хранить в соответствии с статьей 10.1(3), место и условия хранения, порядок предоставления информации правоохранительным органам и службам безопасности и порядок надзора за ОКИ должны быть установлены правительством Российской Федерации (статья 10.1(6)).

24. Приказ ФСБ № 432 от 19 июля 2016 года предусматривает, что ОКИ должен предоставить любую информацию, необходимую для расшифровки электронных сообщений, в течение десяти дней после запроса компетентного подразделения служб безопасности. Запрос должен уточнять содержание (формат) запрашиваемой информации и почтовый или электронный адрес, на который необходимо отправить информацию.

25. Постановление Правительства РФ №743 от 31 июля 2014 года, с изменениями от 18 января 2018 года, предусматривает, что ОКИ должен предоставить службам безопасности удаленный доступ к своей информационной системе, чтобы они могли получить информацию, указанную в пунктах 3 и 4.1 статьи 10.1 Закона об информации (пункт 8).

26. Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации № 571 от 29 октября 2018 года предусматривает, что ОКИ должен установить оборудование, которое способно, среди прочего, искать, обрабатывать и передавать в центр управления ФСБ – по запросу этого центра или автоматически – следующие данные: личные данные зарегистрированных пользователей; получение, отправку, доставку или обработку голосовых, текстовых, визуальных, звуковых, видео или иных электронных сообщений пользователей Интернета; содержимое голосовых, текстовых, визуальных, звуковых, видео или иных электронных сообщений; и информацию, необходимую для расшифровки электронных сообщений, если они зашифрованы (пункт 4). Центр управления служб безопасности должен иметь круглосуточный удалённый доступ к оборудованию и возможность управления им (пункт 14).

27. Постановление Правительства Российской Федерации № 1526 от 23 сентября 2020 года предусматривает, что ОКИ должен предоставлять данные о сообщениях правоохранительным органам и службам безопасности в течение тридцати дней с момента запроса или в течение трёх дней в неотложных случаях (пункты 8 и 9). Запрос должен

включать конкретные идентификаторы информации, которые будут использоваться в качестве критериев поиска, такие как номер телефона, адрес электронной почты, информация, содержащаяся в заголовке протокола связи, или другие идентификаторы (пункт 7).

МЕЖДУНАРОДНЫЕ ДОКУМЕНТЫ

I. ОРГАНИЗАЦИЯ ОБЪЕДИНЁННЫХ НАЦИЙ

28. В Докладе о праве на неприкосновенность частной жизни в цифровую эпоху, подготовленном Управлением Верховного комиссара ООН по правам человека и опубликованном 4 августа 2022 года (A/HRC/51/17), содержатся следующие положения, имеющие отношение к делу (сноски опущены):

«B. Ограничения шифрования

…

21. Шифрование является ключевым элементом обеспечения права на неприкосновенность частной жизни и безопасности в Интернете и необходимо для защиты прав, включая права на свободу мнений и их выражение, свободу объединений и мирных собраний, безопасность, здоровье и недискриминацию. Шифрование гарантирует, что люди могут свободно обмениваться информацией, не опасаясь, что их данные станут известны другим, будь то государственные органы или киберпреступники. Шифрование необходимо, чтобы люди чувствовали себя в безопасности при свободном обмене информацией по широкому кругу вопросов, включая чувствительные данные о здоровье или финансовую информацию, знания о гендерной идентичности и сексуальной ориентации, художественное самовыражение и информацию, связанную с принадлежностью к меньшинству. В условиях повсеместной цензуры шифрование позволяет людям сохранять пространство для отстаивания, выражения и обмена мнениями с другими. В определенных случаях журналисты и правозащитники не могут выполнять свою работу без защиты надежного шифрования, защищающего их источники и укрывающего их от влиятельных акторов, находящихся под расследованием. Шифрование обеспечивает женщин, которые сталкиваются с особыми угрозами наблюдения, преследования и насилия в Интернете, важным уровнем защиты от непреднамеренного раскрытия информации. В условиях вооруженных конфликтов зашифрованные сообщения необходимы для обеспечения безопасной связи между гражданскими лицами. Примечательно, что за два месяца после начала вооруженного конфликта в Украине 24 февраля 2022 года количество загрузок зашифрованного мессенджера Signal в Украине увеличилось более чем на 1000 процентов по сравнению с предыдущими месяцами.

…

23. Несмотря на преимущества, Правительства иногда ограничивают использование шифрования, например, для защиты национальной безопасности и борьбы с преступностью, в частности, для выявления материалов сексуального насилия над детьми. Ограничения включают запреты на зашифрованные

коммуникации и уголовную ответственность за предложение или использование средств шифрования, а также обязательную регистрацию и лицензирование средств шифрования. Аналогично, в некоторых случаях от поставщиков услуг шифрования требуется обеспечивать, доступ правоохранительных органов или других государственных органов ко всем сообщениям по запросу, что фактически может означать всеобщее ограничение шифрования, которое может требовать или по крайней мере поощрять создание своего рода «бэкдора» (встроенного пути обхода шифрования, обеспечивающего тайный доступ к данным в текстовом виде). Еще одной формой вмешательства в использование шифрования является требование о создании и поддержки системы эскроу ключей, а также передачи всех частных ключей, необходимых для расшифровки данных, Правительству или назначенной третьей стороне. Введение требований по отслеживанию, согласно которым поставщики должны иметь возможность отслеживать любое сообщение до предполагаемого отправителя, также может потребовать ослабления стандартов шифрования. В последнее время различные государства начали вводить или рассматривать возможность введения для поставщиков цифровой связи общих обязанностей по наблюдению, включая тех, кто предлагает услуги зашифрованных коммуникаций. Такие обязанности могут фактически вынудить этих поставщиков отказаться от надежного сквозного шифрования или найти крайне проблематичные обходные пути (см. пункты 27-28 ниже).

24. Несомненно, что широко используемые возможности шифрования, которые общественность требовала в ответ на массовое слежение и киберпреступность, создают дилемму для Правительств, стремящихся защитить население, особенно его наиболее уязвимых членов, от тяжких преступлений и угроз безопасности. Однако, как указал Специальный докладчик по вопросу о поощрении и защите права на свободу мнений и их выражения, регулирование шифрования рискует подорвать права человека. Правительства, стремящиеся ограничить шифрование, часто не могут доказать, что предлагаемые ими ограничения необходимы для достижения конкретного законного интереса, учитывая наличие других различных инструментов и подходов, которые предоставляют необходимую информацию для конкретных целей правоохранительных органов или других законных целей. Такие альтернативные меры включают улучшенную, более оснащенную традиционную полицию, операции под прикрытием, анализ метаданных и углубленное международное полицейское сотрудничество.

25. Более того, влияние большинства ограничений использования шифрования на право на неприкосновенность частной жизни и связанные с ним права является непропорциональным, часто затрагивая не только лиц представляющих интерес, но и всё население. Прямые запреты Правительств или уголовная ответственность за шифрование, в частности, не могут быть оправданы, поскольку они лишают всех пользователей в их юрисдикциях возможности безопасного общения. Системы эскроу ключей имеют значительные уязвимости, поскольку они зависят от целостности хранилища и подвергают хранимые ключи кибератакам. Более того, обязательные «бэкдоры» в средствах шифрования создают уязвимости, которые выходят далеко за рамки их полезности в отношении конкретных пользователей, идентифицированных как подозреваемые в совершении преступлений или как угроза безопасности. Они ставят под угрозу право на неприкосновенность частной жизни и безопасность всех пользователей и подвергают их незаконному вмешательству не только со стороны государств, но и со стороны негосударственных акторов, включая преступные сети. Лицензионные и регистрационные требования имеют аналогичные

непропорциональные последствия, поскольку требуют, чтобы программное обеспечение для шифрования содержало эксплуатационные уязвимости. Такие неблагоприятные последствия не обязательно ограничиваются юрисдикцией, вводящей ограничения; скорее всего, что «бэкдоры», однажды установленные в юрисдикции одного государства, станут частью программного обеспечения, используемого в других частях мира.

26. …Поскольку содержимое сообщений, после их шифрования, не может быть доступно никому, кроме отправителя и получателя, любое общее обязательство по наблюдению вынудило бы поставщиков услуг либо отказаться от транспортного шифрования, либо получать доступ к сообщениям до их шифрования ...»

II. СОВЕТ ЕВРОПЫ

29. Приложение к Рекомендации Комитета министров Совета Европы о защите прав человека в отношении услуг социальных сетей (CM/Rec(2012)4, принято 4 апреля 2012 года) гласит следующее:

15. В сотрудничестве с частным сектором и гражданским обществом государства-члены, в дополнение к мерам, изложенным в разделе I этого приложения, должны принять соответствующие меры для обеспечения защиты права пользователей на частную жизнь, в частности, взаимодействуя с поставщиками услуг социальных сетей для выполнения следующих действий:

...

– обеспечить применение наиболее подходящих мер безопасности для защиты персональных данных от незаконного доступа третьих лиц. Это должно включать меры по сквозному шифрованию связи между пользователем и сайтом социальной сети ...»

30. Резолюция Парламентской ассамблеи Совета Европы 2045 (2015) о массовом слежении, принятая 21 апреля 2015 года, гласит следующее, в той мере, в какой это имеет отношение к делу:

«5. Ассамблея глубоко обеспокоена угрозами безопасности Интернета со стороны практик некоторых разведывательных служб, раскрытых в документах Сноудена, систематически ищущих, использующих и даже создающих «бэкдоры» и другие уязвимости в стандартах безопасности и при их внедрении, которые могут быть легко использованы террористами и кибер-террористами или другими преступниками.

6. Ассамблея также обеспокоена сбором большого объема персональных данных частными компаниями и риском того, что эти данные могут быть использованы для незаконных целей государственными или негосударственными акторами. ...

8. Высокотехнологичные средства слежения уже используются в ряде авторитарных режимов для отслеживания оппонентов и подавления свободы информации и выражения мнений. В этом отношении Ассамблея глубоко обеспокоена недавними законодательными изменениями в Российской

Федерации, которые создают возможности для усиленного массового наблюдения через социальные сети и интернет-сервисы.

9. В нескольких странах сформировался мощный «промышленный комплекс слежения», подпитываемый культурой секретности вокруг операций наблюдения, их высокой технической сложностью и тем фактом, что серьезность предполагаемых угроз и необходимость конкретных контрмер и их затраты и выгоды сложно оценить лицам принимающим политические и бюджетным без опоры на информацию от заинтересованных групп. Существует риск, что эти мощные структуры могут выйти из-под демократического контроля и подотчетности и угрожать свободному и открытому характеру наших обществ ...

11. Ассамблея признает необходимость эффективного, целенаправленного наблюдения за подозреваемыми террористами и другими организованными преступными группами. Такое целенаправленное наблюдение может быть эффективным инструментом для правоохранительных органов и предотвращения преступлений. В то же время она отмечает, что, согласно независимым обзорам, проведенным в Соединенных Штатах, массовое наблюдение не способствовало предотвращению террористических атак, вопреки ранним заявлениям высокопоставленных разведывательных чиновников. Вместо этого ресурсы, которые могли бы предотвратить атаки, направляются на массовое наблюдение, оставляя потенциально опасным лицам свободу действий ...

19. Ассамблея, таким образом, призывает государства-члены и государства-наблюдателей Совета Европы:

19.1 обеспечить, чтобы их национальные законы разрешали сбор и анализ персональных данных (включая так называемые метаданные) только с согласия соответствующего лица или на основании судебного приказа, выданного на основе разумного подозрения в причастности цели к совершению преступления; незаконный сбор и обработка данных должны быть наказуемы так же, как и нарушение традиционной тайны переписки; создание «бэкдоров» или любых других техник для ослабления или обхода мер безопасности либо использования их существующих уязвимостей должно быть строго запрещено; все учреждения и компании, хранящие персональные данные, должны быть обязаны применять наиболее эффективные доступные меры безопасности;

19.2 обеспечить, для реализации такой правовой основы, чтобы их разведывательные службы были подчинены адекватным судебным и/или парламентским механизмам контроля …

19.5 содействовать дальнейшему развитию удобных для пользователя (автоматических) технологий защиты данных, способных противостоять массовому слежению и любым другим угрозам Интернет-безопасности, включая угрозы, исходящие от негосударственных акторов …»

III. ЕВРОПЕЙСКИЙ СОЮЗ

31. В решении, вынесенном Судом Справедливости Европейского Союза (CJEU) 8 апреля 2014 года по объединенным делам Digital Rights

Ireland и Seitinger и другие (C-293/12 и C-594/12, EU:C:2014:238), Директива о хранении данных 2006/24/ЕС была признана недействительной. Директива устанавливала обязаность для поставщиков общедоступных услуг электронной связи или публичных сетей связи хранить все данные о трафике и местоположении в течение периода от шести месяцев до двух лет, для обеспечения доступности этих данных в целях расследования, выявления и преследования за тяжкие преступления, определенные каждым государством-членом в его национальном законодательстве. Для обзора этого постановления и дальнейших развитий в судебной практике CJEU см. дело *Big Brother Watch и другие против Соединенного Королевства* [GC], № 58170/13 и 2 другие, §§ 209-41, 25 мая 2021 года.

32. CJEU также постановил в своем решении от 6 октября 2015 года по делу Максимилиан Шремс против Уполномоченного по защите данных (C-362/14, EU:C:2015:650), следующее:

> «94. В частности, законодательство, разрешающее на общем основании доступ государственных органов к содержимому электронных сообщений, должно рассматриваться как подрывающего сущность основного права на уважение частной жизни, гарантированного статьей 7 Хартии ...»

33. Совместное заявление Европола и Агентства Европейского Союза по кибербезопасности (ENISA) от 20 мая 2016 года о правомерном расследовании преступлений, соблюдающих требования защиты данных XXI века, гласит:

> «Перехват зашифрованного сообщения или взлом цифрового сервиса могут считаться пропорциональными в отношении конкретного подозреваемого, но взлом криптографических механизмов может вызвать побочный ущерб. Фокус должен быть направлен на получение доступа к сообщению или информации, а не на взлом механизма защиты Хорошая новость заключается в том, что информация в какой-то момент должна быть расшифрована, чтобы быть полезной для преступников. Это создает возможности для таких альтернатив, как операции под прикрытием, внедрение в преступные группы и получение доступа к устройствам связи за пределами точки шифрования, например, с помощью реальной криминалистики на захваченных устройствах или законного перехвата этих устройств, пока они используются подозреваемыми. Более того, криминалистические методы, использующие физические отпечатки устройств, могут не помочь перехватить содержимое сообщения, но могут предоставить другие важные улики для следователя. Тем не менее, существуют случаи, когда таких альтернатив нет, и доступ к скрытому содержимому можно получить только путем расшифровки.
>
> Хотя ни один механизм шифрования на практике не является совершенным по своему дизайну и реализации, расшифровка становится все менее и менее реализуемой для целей правоохранительных органов. Это привело к предложениям ввести обязательные бэкдоры или хранение ключей для ослабления шифрования. Хотя это и предоставило бы следователям законный

доступ в случае серьезных преступлений или террористических угроз, это также увеличило бы пространство злонамеренного использования, что, следовательно, имело бы гораздо более широкие последствия для общества. Более того, преступники могут легко обойти такие ослабленные механизмы и воспользоваться существующими знаниями о криптографии для разработки (или покупки) собственных решений без бэкдоров или эскроу-ключей ...

Решения, целенаправленно ослабляющие в технические механизмы защиты для поддержки правоохранительных органов, по своей сути ослабляют и защиту от преступников, что делает легкое решение невозможным ...

Когда обход невозможен, но доступ к зашифрованной информации крайне необходим для обеспечения безопасности и отправления правосудия, тогда должны предлагаться осуществимые решения по расшифровке без ослабления механизмов защиты, как в законодательстве, так и в ходе непрерывной технической эволюции. В последнем случае, настоятельно рекомендуется стимулирование тесного сотрудничества с промышленными партнерами, а также с научным сообществом, обладающими опытом в криптоанализе для взлома шифрования, в случаях предусмотренных законом. Мы убеждены, что можно найти решение, которое найдет разумный и рабочий баланс между личными правами и защитой интересов безопасности граждан ЕС. В этом отношении развитие европейских инструментов НИОКР может стимулировать это сотрудничество, в то время как агентства ЕС могут тесно сотрудничать в установлении лучших практик."

34. 28 июля 2022 года Европейский совет по защите данных (EDPB) и Европейский инспектор по защите данных (EDPS) приняли Совместное мнение 4/2022 по предложению Регламента Европейского Парламента и Совета по установлению правил для предотвращения и борьбы с сексуальным насилием над детьми. В нем говорится следующее (сноски опущены):

«Резюме

... меры, позволяющие государственным органам получать доступ к содержимому сообщений на общем основании для выявления случаев вовлечения детей, скорее всего, затрагивают сущность прав, гарантированных статьями 7 и 8 Хартии ...

EDPB и EDPS также выражают сомнения в эффективности мер блокировки и считают, что требование к поставщикам интернет-услуг расшифровывать онлайн-сообщении для блокировки касающихся материалов сексуального насилия над детьми (МСНД) будет непропорциональным.

Более того, EDPB и EDPS подчеркивают, что технологии шифрования вносят фундаментальный вклад в уважение частной жизни и тайны связи, свободу выражения мнений, а также в инновации и рост цифровой экономики, которые зависят от высокого уровня доверия и уверенности, предоставляемого такими технологиями. Пункт 26 Преамбулы к Предложению не только предоставляет выбор технологий обнаружения, но также и технических мер для защиты

конфиденциальности сообщений, таких как шифрование, с оговоркой, что этот выбор технологий должен соответствовать требованиям предлагаемого Регламента, т.е. он должен обеспечивать возможность обнаружения. Это поддерживает идею, статей 8(3) и 10(2) Предложения, что поставщик не может отказаться от выполнения приказа об обнаружении на основании технической невозможности. EDPB и EDPS считают, что должен быть найден лучший баланс между общественной потребностью в защищенных и частных каналах связи и борьбой с их злонамеренным использованием. В Предложении должно быть четко указано, что ничто в предлагаемом Регламенте не следует толковать как запрещающее или ослабляющее шифрование ...

4.10 Влияние на шифрование

96. Европейские органы по защите данных последовательно выступают за широкое использование сильных инструментов шифрования и против бэкдоров любого типа. Это связано с тем, что шифрование важно для обеспечения соблюдения всех прав человека как офлайн, так и онлайн. Более того, технологии шифрования вносят фундаментальный вклад как в уважение частной жизни, так и в тайну связи ...

97. В контексте межличностного общения сквозное шифрование (E2EE) является важнейшим инструментом для обеспечения конфиденциальности электронных сообщений, поскольку оно предоставляет сильные технические гарантии против доступа к содержимому сообщений кем-либо, кроме отправителя и получателей, включая поставщика. Предотвращение или препятствование в любом виде использования E2EE, возложение на поставщиков услуг обязательства обрабатывать данные электронных сообщений для целей, отличных от предоставления их услуг, или обязательства передавать электронные сообщения третьим лицам, создадут риск того, что поставщики будут предлагать менее зашифрованные услуги для лучшего соответствия обязательствам, что в целом ослабит роль шифрования и подорвет уважение к фундаментальным правам европейских граждан. Следует отметить, что хотя E2EE является одной из наиболее часто используемых мер безопасности в контексте электронных средств связи, другие технические решения (например, использование других криптографических схем) могут быть или стать столь же важными для обеспечения и защиты конфиденциальности цифровых сообщений. Таким образом, их использование также не должно предотвращаться или препятствовать.

98. Развертывание инструментов для перехвата и анализа межличностных электронных сообщений принципиально противоречит E2EE, поскольку последнее направлено на техническую гарантию того, что сообщение останется конфиденциальным между отправителем и получателем ...

100. Влияние деградации или препятствования использования E2EE, которое может возникнуть из-за принятия Предложения, должно быть оценено надлежащим образом. Каждый из методов обхода сохраняющего конфиденциальный характер E2EE, представленных в отчете об оценке воздействия, сопровождающем Предложение, приведет к появлению лазеек в системе безопасности. Например, сканирование на стороне клиента, вероятно, приведет к значительному, неограниченному доступу и обработке незашифрованного содержимого на устройствах конечных пользователей ... В то же время сканирование на стороне сервера также принципиально несовместимо с парадигмой E2EE, поскольку однорангово зашифрованный канал связи, будет необходимо взломать, что приведет к массовой обработке персональных данных на серверах поставщиков.

> 101. Хотя в Предложении говорится, что оно «оставляет за соответствующим поставщиком право выбора технологий, которые будут использоваться для эффективного выполнения приказа об обнаружении, и не должно пониматься как поощрение или препятствование использования той или иной технологии», структурная несовместимость некоторых приказов об обнаружении с E2EE фактически становится сильным сдерживающим фактором для использования E2EE. Неспособность получить доступ и использовать сервисы с использованием E2EE (которая представляет собой текущий уровень развития техники с точки зрения технической гарантии конфиденциальности) может иметь сдерживающий эффект на свободу выражения и законное использование услуг электронной связи частными лицами...».

ПРАВО

I. ПРЕДВАРИТЕЛЬНЫЕ ВОПРОСЫ

35. Жалоба заявителя касаются непрерывного хранения ОКИ Интернет-сообщений и связанных с ними данных, потенциального доступа властей к этим данным и обязательства ОКИ расшифровывать их, если они зашифрованы, в соответствии с Законом о информации и его подзаконными актами. Суд рассмотрит соответствие оспариваемого закона Конвенции на дату рассмотрения допустимости жалоб заявителя (см. *«Big Brother Watch и другие против Соединенного Королевства»* [GC], №№ 58170/13 и 2 других, §§ 268-70, 25 мая 2021 года). Суд постановляет, что он имеет юрисдикцию рассматривать настоящее заявление в той мере, в какой факты, лежащие в основе предполагаемых нарушений Конвенции, имели место до 16 сентября 2022 года – даты, когда Российская Федерация перестала быть стороной Конвенции (см. *«Федотова и другие против России»* [GC], №№ 40792/10 и 2 других, §§ 68-73, 17 января 2023 года; *«Пивкина и другие против России»* (дек.), № 2134/23 и 6 других, § 61, 6 июня 2023 года; и *«Н.Ф. и другие против России»*, № 3537/15 и 8 других, § 30, 12 сентября 2023 года).

II. ЗАЯВЛЕННОЕ НАРУШЕНИЕ СТАТЬИ 8 КОНВЕНЦИИ

36. Заявитель обжалует законодательное требование к ОКИ хранить содержание всех Интернет-сообщений и связанных с ними данных, а также предоставлять эти данные правоохранительным органам или службам безопасности по их запросу вместе с информацией, необходимой для расшифровки электронных сообщений, если они зашифрованы. Он ссылался на статью 8 Конвенции, которая гласит следующее:

> «1. Каждый имеет право на уважение его частной и семейной жизни, его жилища и его корреспонденции.

2. Не допускается вмешательство со стороны публичных властей в осуществление этого права, за исключением случаев, когда такое вмешательство предусмотрено законом и необходимо в демократическом обществе в интересах национальной безопасности, общественной безопасности или экономического благосостояния страны, в целях предотвращения беспорядков или преступлений, для охраны здоровья или нравственности или защиты прав и свобод других лиц.»

A. Приемлемость

37. Суд отмечает, что эта жалоба не является явно необоснованной или недопустимой по любым другим основаниям, перечисленным в статье 35 Конвенции. Следовательно должна быть признана допустимой.

B. Существо дела

1. Аргументы сторон

(a) Заявитель

38. Заявитель утверждал, что законодательное требование к ОКИ хранить содержание всех онлайн-сообщений, в сочетании с требованием предоставлять ключи шифрования по запросу правоохранительных органов, представляет собой вмешательство в право заявителя на уважение его частной жизни и корреспонденции. Более того, технически невозможно предоставить властям ключи шифрования, связанные с конкретными пользователями приложения для обмена сообщениями Telegram. Любое раскрытие ключей шифрования, таким образом, затрагивало бы конфиденциальность корреспонденции всех пользователей Telegram.

39. Заявитель также утверждал, что положения национального законодательства, требующие хранения содержания всех онлайн-сообщений и предоставления ключей шифрования правоохранительным органам, не были предсказуемыми в их применении и не содержали эффективных гарантий против произвола. В частности, национальным властям не требовалось судебного разрешения для запроса ключей шифрования. Хотя в постановлении о раскрытии информации от 12 июля 2017 года упоминалось, что были получены судебные решения в отношении шести телефонных номеров, эти судебные решения никогда не были показаны компании Telegram Messenger, судам, рассматривавшим дело компании или заявителя, или общественности.

(b) Правительство

40. Правительство утверждало, что не имело места вмешательство в права заявителя. Заявитель не смог продемонстрировать, что существует "обоснованная вероятность" того, что службы безопасности собирали и хранили информацию о его личной жизни. Что касается ключей шифрования Telegram, то Приказ № 432 (см. выше, пункт 24) не содержал требования предоставлять ключи шифрования для расшифровки всего трафика. Ключи шифрования должны были предоставляться по запросу в отношении конкретных данных. Запрос на ключи шифрования от 12 июля 2017 года, оспариваемый заявителем, касался сообщений, связанных с шестью телефонными номерами, принадлежащими подозреваемым в терроризме, и для него было получено судебное разрешение. Таким образом, утверждения заявителя о том, что службы безопасности имели доступ ко всем сообщениям пользователей, не были подтверждены.

41. В качестве альтернативы Правительство утверждало, что заявленное вмешательство имеет основание в национальном законодательстве. Положения национального законодательства были доступны и предсказуемы по своим последствиям. Любой перехват сообщений должен был быть санкционирован судом. Перехват сообщений мог проводиться только после получения информации о том, что было совершено, совершается или замышляется уголовное преступление; о лицах, замышляющих совершить, совершающих или совершивших уголовное преступление; или о событиях или действиях, угрожающих национальной, военной, экономической или экологической безопасности Российской Федерации. Только преступления средней тяжести, тяжкие и особо тяжкие преступления могли послужить основанием для приказа о перехвате, и только лица, подозреваемые в таких преступлениях, или лица, которые могли обладать информацией о таких преступлениях, могли быть подвергнуты мерам перехвата. Записи перехваченных сообщений должны были храниться в условиях, исключающих любую возможность их прослушивания или копирования несанкционированными лицами (правительство сослалось на положения национального законодательства, изложенные в решении Большой Палаты Европейского Суда по делу «*Роман Захаров против России*», № 47143/06, §§ 31-33 и 51, ЕСПЧ 2015). Процедуры, которым необходимо следовать при рассмотрении, использовании, хранении и уничтожении полученных данных, содержат необходимые гарантии против злоупотребления властью.

42. Правительство также утверждало, что предоставление ключей шифрования ФСБ не означало, что информация, необходимая для расшифровки зашифрованных электронных сообщений, станет доступной всему персоналу службы. Руководители соответствующих

служб несут ответственность за обеспечение того, чтобы их персонал действовал в пределах установленных обязанностями требований. В любом случае, сотрудники ФСБ обязаны сохранять конфиденциальность в отношении информации о частной жизни, ставшей им известной в ходе исполнения служебных обязанностей. Ключи шифрования используются для расшифровки сообщений, в отношении которых было получено судебное решение на перехват.

43. Наконец, Правительство утверждало, что вмешательство было "необходимым в демократическом обществе" для достижения законной цели борьбы с терроризмом. Например, в апреле 2017 года в Санкт-Петербурге произошел террористически акт. Впоследствии, в декабре 2017 года, был предотвращен еще один акт. В обоих случаях атаки координировались из-за рубежа через секретные чаты в Telegram.

(c) Третьи лица

(i) Институт европейского информационного общества (EISI)

44. EISI объяснил, что сквозное шифрование является математическим инструментом, который работает следующим образом: с помощью "публичного" ключа любое сообщение ("открытый текст") переводится в, казалось бы, случайную комбинацию букв, цифр или символов («зашифрованный текст»). Только отправители и получатели могут видеть открытый текст, в то время как посторонние видят только зашифрованный текст. Сообщение в зашифрованном тексте не может быть переведено обратно в открытый текст без «приватного» ключа, который хранится надежно на устройстве получателя. Преобразование в открытый текст происходит непосредственно на устройстве получателя. Сквозное шифрование гарантирует, что оператор службы обмена сообщениями никогда не имеет доступа ни к приватному ключу, ни к исходному сообщению в открытом тексте, предотвращая любой доступ к передаваемому содержимому.

45. EISI также утверждал, что требование ФСБ о раскрытии информации Telegram равносильно «приказу о предоставлении бэкдора», который касается всех пользователей Telegram без ограничений. Выполнение этого приказа фактически означало бы, что Telegram должен централизованно хранить «приватные» ключи, то есть, он не смог бы легально предоставлять услуги сквозного шифрования своим пользователям.

46. EISI утверждал, что шифрование, используемое службами обмена сообщениями, является механизмом самозащиты от слежения. Оно играет важную роль в обеспечении целостности и безопасности сообщений во время передачи. Оно обеспечивает существенную защиту уязвимым лицам, таким как журналисты, оппозиционные лидеры или жертвы кибертравли. Таким образом, существует сильная связь между

шифрованием и правами человека, в частности, статьями 8 и 10 Конвенции. Введение «бэкдоров» в зашифрованные линии связи ослабило бы этот механизм защиты и создало бы риски для безопасности.

47. EISI оспорил необходимости и пропорциональности требования доступа ко всем зашифрованным сообщениям через «бэкдор», поскольку это подрывает приватность всех пользователей ради небольшой группы подозреваемых. Это делает всех пользователей уязвимыми для несанкционированного государственного наблюдения, киберпреступной деятельности и других злонамеренных действий. Даже если эти риски не реализуются, знание таких угроз создает сдерживающий эффект, делая авторов, исследователей, журналистов и оппозиционных активистов менее склонными к высказываниям или общению со своими источниками. EISI также утверждал, что существуют менее инвазивные целевые альтернативы для борьбы с преступностью и защиты национальной безопасности, такие как использование реальной криминалистики на изъятых устройствах, отгадывание или получение приватных ключей, хранящихся у участников связи, использование уязвимостей в программном обеспечении цели или отправка закладок на целевые устройства. Хотя неизбирательные «бэкдоры» могут быть дешевле для государства, чем альтернативные методы следствия, они обходятся дорого обществу в целом из-за создаваемых рисков для безопасности. Тот факт, что альтернативные методы значительно сложнее использовать в больших масштабах из-за их трудоемкости, стоимости и логистической сложности, следует рассматривать как положительное препятствие, заставляющее приоритизировать и направлять меры.

(ii) Privacy International

48. Privacy International дал аналогичное описание того, как работает сквозное шифрование. Поскольку шифрование и дешифрование отправленных и полученных сообщений, происходит на устройствах пользователей, сквозное шифрование гарантирует, что только предполагаемые получатели, а даже не поставщик услуг связи, имеют доступ к содержимому сообщения. «Приватный» ключ, используемый для расшифрования сообщения получателем, хранится на устройстве получателя и не передается никому.

49. Privacy International также утверждал, что меры, требуемые оспариваемым законодательством, включающие хранение и дешифрование зашифрованных сообщений, противоречат обязательствам национальных властей по защите конфиденциальности, приватности, безопасности и целостности систем связи и информационных технологий. Реализация таких мер заставила бы поставщиков услуг, таких как Telegram, вносить радикальные

изменения в свое программное обеспечение и ослабить используемые схемы шифрования. Обязательство расшифровывать зашифрованные сообщения вынуждает поставщиков услуг связи модифицировать свои существующие сервисы, создавая «бэкдоры», которые, однажды найденные, могут быть легко использованы как легитимными, так и преступными акторами. Иными словами, в случае сквозного шифрования единственный способ для поставщика услуг связи выполнить обязательство по дешифровке сообщений — это выпустить обновление программного обеспечения, которое не может быть нацелено на конкретных пользователей и поэтому без разбора влияет всех пользователей приложения или услуги. Требование поставщиков телекоммуникационных услуг создать «бэкдоры» для неизбирательного доступа к зашифрованным сообщения не может быть ограничено тем, что «необходимо в демократическом обществе».

2. Оценка Суда

(a) Наличие вмешательства и его пределы

50. Суд отмечает, что настоящее дело касается законодательных требований для ОКИ хранить содержание всех Интернет-сообщений и связанных данных, предоставлять правоохранительным органам или службам безопасности доступ к этим данным по запросу и расшифровывать электронные сообщения, если они зашифрованы.

51. Что касается хранения ОКИ Интернет-сообщений и соответствующих данных, Суд повторяет, что простое хранение данных, относящихся к частной жизни человека, является вмешательством в смысле статьи 8. Последующее использование сохраненной информации не имеет значения для данного вывода. Однако, при определении того, затрагивает ли хранимая органами личная информация какой-либо из аспектов частной жизни, Суд будет учитывать конкретный контекст, в котором информация была зафиксирована и сохранена, природу записей, способ их использования и обработки, а также результаты, которые могут быть получены (см. *S. и Marper против Соединенного Королевства*, № 30562/04 и 30566/04, § 67, ECHR 2008).

52. Суд считает, что хранение ОКИ заявителя содержания всех его Интернет-сообщений и соответствующих данных нарушает его право на уважение частной жизни и корреспонденции (см. пункт 19 выше о национальных положениях; сравните *Breyer против Германии*, № 50001/12, § 81, 30 января 2020 года, и *Ekimdzhiev и другие против Болгарии*, № 70078/12, §§ 372 и 373, 11 января 2022 года). Это хранение составляет вмешательство в его права предусмотренные статьей 8, независимо от того, имели ли власти доступ к сохраненным данным. Хранение, хотя и осуществляемое частными лицами – ОКИ – требуется

по закону; следовательно, вмешательство можно отнести к действиям российского государства (см. *Ekimdzhiev и другие*, цитируемые выше, §§ 372 и 375).

53. Суд далее отмечает, что вмешательство, на которое подано заявление, касается не только хранения описанных данных, но и возможности национальных властей получить доступ к этим данным (для сравнения *Breyer*, § 61, и *Ekimdzhiev и другие*, § 376, оба цитируемые выше).

54. Действительно, нет доказательств того, что власти получили доступ к данным заявителя, хранимым Telegram. Поскольку невозможно, чтобы физическое или юридическое лицо знало наверняка, был ли осуществлен доступ к их данным, следует анализировать вопрос о том, может ли заявитель утверждать, что он является жертвой вмешательства в свои права предусмотренные статьей 8 из-за простого существования законов, разрешающих властям это делать, исходя из тех же критериев, что и для тайного наблюдения (см. *Ekimdzhiev и другие,* цитируемые выше, § 376).

55. В деле *Романа Захарова* (цитируемого выше) Суд изучил российское законодательство о тайном наблюдении и пришел к выводу, что, учитывая тайный характер мер наблюдения, широкие пределы их применения, затрагивающего всех пользователей сетей связи, и отсутствие эффективных средств для оспаривания предполагаемого применения мер тайного наблюдения на национальном уровне, само существование законодательства, допускающего тайное наблюдение, представляет собой вмешательство в частную жизнь пользователя (см. *Роман Захаров*, цитируемый выше, §§ 170-79). Суд не находит оснований считать иначе в данном случае, поскольку Правительство подтвердило, что доступ к сохраненным Интернет-сообщениям и связанным данным регулируется тем же правовым режимом, что и рассмотренный в деле *Романа Захарова*. Следовательно, само существование оспариваемого законодательства является вмешательством в осуществление заявителем своих прав по статье 8 (для сравнения *Ekimdzhiev и другие*, цитируемые выше, §§ 383-84).

56. Наконец, что касается законодательного требования ОКИ расшифровывать сообщения, если они зашифрованы (см. пункты 20 и 24 выше), Суд отмечает, что наблюдения сторон по этому вопросу ограничиваются сообщениями с сквозным шифрованием, то есть в случае Telegram — общением через «секретные чаты» (см. пункт 5 выше). Стороны не представили никаких данных о схеме шифрования, используемой в «облачных чатах», и по этой причине Суд не будет их рассматривать.

57. Заявитель утверждал, что технически невозможно предоставить властям ключи шифрования, связанные с конкретными пользователями мессенджера Telegram. Чтобы обеспечить расшифровку сообщений с

сквозным шифрованием, необходимо ослабить технологию шифрования, используемую мессенджером Telegram. Однако, поскольку эти меры не могут быть ограничены конкретными лицами, они затронут всех без исключения. Этот аргумент основан на доводах компании Telegram в национальных судебных разбирательствах (см. пункт 8 выше). Позиция заявителя подкрепляется третьими сторонами (см. пункты 44, 45, 48 и 49 выше) и также поддерживается международными материалами (см. в частности пункты 28 и 34 выше). Правительство, напротив, не представило никаких аргументов или информации, способной опровергнуть утверждения заявителя о том, что меры, которые ОКИ должны предпринять для выполнения законодательного требования по расшифровке сообщений со сквозным шифрованием, затронут всех пользователей их услуг. Соответственно, Суд принимает, что заявитель был затронут оспариваемыми законодательными положениями.

58. Суд приходит к выводу, что непрерывное хранение Интернет-сообщений заявителя и связанных данных Telegram, потенциальный доступ властей к этим данным и обязанность Telegram расшифровывать их, если они зашифрованы, в соответствии с Законом об информации и его нормативными актами, составляет вмешательство в права заявителя по статье 8.

59. Суд также отмечает, что в данном деле персональные данные хранятся с целью предоставления компетентным национальным органам возможности проводить целевое тайное наблюдение за Интернет-коммуникациями. Следовательно, вопросы, касающиеся хранения персональных данных и тайного наблюдения тесно связаны в данном деле.

(b) Обоснование вмешательства

(i) Общие принципы

60. Суд находит, что, хотя дело должно быть рассмотрено в первую очередь с точки зрения хранения персональных данных заявителя, его следует также рассматривать, где это уместно, в свете прецедентного права Суда по тайному наблюдению (см. пункт 59 выше). Применимые средства защиты в любом случае схожи по сути и должны предлагать эффективные гарантии против присущего риска злоупотреблений и ограничивать вмешательство в права, защищаемые статьей 8, до уровня «необходимого в демократическом обществе» (см. *Ekimdzhiev и другие*, цитируемые выше, §§ 291-93 и 395, с дальнейшими ссылками).

61. Суд повторяет, что любое вмешательство может быть оправдано по статье 8 § 2 только если оно соответствует закону, преследует одну или несколько законных целей, указанных в пункте 2 статьи 8, и является необходимым в демократическом обществе для достижения

этих целей. Формулировка "в соответствии с законом" требует, чтобы оспариваемая мера имела основу в национальном праве. Она также должна быть совместима с принципом верховенства права, который прямо упомянут в Преамбуле Конвенции и присущ объекту и цели статьи 8. Закон должен быть доступен заинтересованному лицу и предсказуем в отношении его последствий (см. *Роман Захаров,* цитируемый выше, §§ 227-28).

62. Защита персональных данных имеет фундаментальное значение для осуществления человеком права на уважение частной и семейной жизни, гарантированным статьей 8 Конвенции. Национальное законодательство должно обеспечивать соответствующие гарантии для предотвращения любого такого использования персональных данных, которое может быть несовместимо с гарантиями этой статьи. Необходимость таких гарантий тем больше, когда речь идет о защите персональных данных, подвергаемых автоматической обработке, особенно когда такие данные используются в интересах полиции (см. *S. и Marper*, цитируемые выше, § 103, и, в контексте массового перехвата сообщений, *Big Brother Watch и другие*, цитируемые выше, § 330), и особенно в условиях, когда доступная технология становится все более совершенной (см. в контексте хранения персональных данных *Uzun против Германии*, № 35623/05, § 61, ECHR 2010 (выдержки); *Catt против Соединенного Королевства,* № 43514/15, § 114, 24 января 2019 года; и *Gaughran против Соединенного Королевства*, № 45245/15, § 86, 13 февраля 2020 года; см. также, в контексте тайного наблюдения, *Роман Захаров*, § 229, и *Big Brother Watch* и другие, § 333, оба цитируемые выше). Защита, предоставляемая статьей 8 Конвенции, была бы недопустимо ослаблена, если использование современных технологий в системе уголовного правосудия было бы разрешено на любых условиях и без тщательного установления баланса между потенциальными выгодами от широкого использования таких технологий и важными интересами частной жизни (см. *mutatis mutandis, S. и Marper*, процитировано выше, § 112).

63. В контексте сбора и обработки персональных данных необходимо иметь четкие, подробные правила, регулирующие объем и применение мер, а также минимальные гарантии, касающиеся, *inter alia,* срока, хранения, использования, доступа третьих лиц, процедур сохранения целостности и конфиденциальности данных и процедур их уничтожения, обеспечивая тем самым достаточные гарантии против риска злоупотреблений и произвола (там же, § 99; см. также *P.N. против Германии*, № 74440/17, § 62, 11 июня 2020 г.). Национальное законодательство должно, в частности, обеспечить, чтобы сохраняемые данные были актуальными и не чрезмерными по отношению к целям, для которых они хранятся, и сохранялись в форме, позволяющей идентифицировать субъектов данных, не дольше, чем это требуется для

целей, для которых эти данные хранятся. Национальное законодательство также должно предоставлять адекватные гарантии того, что сохраненные персональные данные будут эффективно защищены от злоупотреблений и неправомерного использования (см. *S. и Marper*, процитировано выше, § 103). Основные принципы защиты данных требуют, чтобы хранение данных было соразмерным по отношению к цели их сбора, и требует ограниченных сроков хранения (там же, § 107).

64. В контексте тайного наблюдения, когда полномочия, которыми наделена исполнительная власть, осуществляются в тайне, риск произвола очевиден. Чтобы соответствовать требованию «предсказуемости», национальное законодательство должно быть достаточно четким, чтобы граждане могли получить адекватное представление о том, при каких обстоятельствах и на каких условиях государственные органы вправе прибегать к любым подобным мерам. Более того, поскольку осуществление мер по тайному наблюдению за сообщениями на практике не подлежит проверке со стороны заинтересованных лиц или общественности в целом, было бы противоречием верховенству права, если бы дискреционные полномочия, предоставленные исполнительной власти или судье, были выражены в терминах неограниченной власти. Следовательно, закон должен указывать объем любых таких дискреционных полномочий, предоставленных компетентным органам, и порядок их осуществления с достаточной ясностью, чтобы обеспечить человеку адекватную защиту от произвольного вмешательства (см. *Роман Захаров,* процитированный выше, §§ 229-30). Подробное описание гарантий, которые должны быть закреплены в законе, чтобы он отвечал требованиям «качества закона» и обеспечивал применение мер тайного наблюдения только в тех случаях, когда это «необходимо в демократическом обществе», см. в *Роман Захаров,* §§ 231-34, и *Big Brother Watch и другие*, §§ 335-39, оба цитируются выше.

65. Наконец, Суд повторяет, что конфиденциальность сообщений является существенным элементом права на уважение частной жизни и корреспонденции, закрепленного в Статье 8. Пользователи телекоммуникационных и Интернет-услуг должны иметь гарантию того, что их частная жизнь и свобода выражения мнения будут уважаться, хотя такая гарантия не может быть абсолютной и должна иногда уступать другим законным императивам, таким как предотвращение беспорядков или преступлений или защита прав и свобод других лиц (см. дело «*K.U. против Финляндии*», № 2872/02, § 49, ECHR 2008, и дело «*Delfi AS против Эстонии* [GC], № 64569/09, § 149, ECHR 2015).

(ii) Применение вышеуказанных принципов в настоящем деле

66. Суд считает, что в настоящем деле вопросы законности и существования законной цели не могут быть отделены от вопроса о том, было ли вмешательство «необходимым в демократическом обществе» (см., в отношении хранения персональных данных, *S. и Marper*, § 99; *Breyer*, § 85; и *Ekimdzhiev и другие*, § 420, все цитируются выше; см. также, в отношении тайного наблюдения, *Роман Захаров*, § 236, и *Big Brother Watch* и другие, § 334, оба цитируются выше). Поэтому они будут рассматриваться вместе ниже.

67. Сбор и сохранение Интернет-сообщений и связанных данных в настоящем деле имели правовую основу в Законе об информации (см. пункт 19 выше), который должен читаться в совокупности с правовыми положениями, регулирующими доступ правоохранительных органов к хранимым данным и их дальнейшее использование, как это установлено в Законе об информации, Уголовно-процессуальном кодексе и Законе об оперативно-розыскной деятельности (см. пункты 15 и 25 выше; см. также, для аналогичного рассуждения, *Breyer*, цитируемый выше, §§ 85 и 97).

68. Суд также отмечает, что, хотя технологические возможности значительно увеличили объем сообщений, проходящих через глобальный Интернет, угрозы, с которыми сталкиваются государства-участники и их граждане, также значительно возросли. Эти угрозы включают, но не ограничиваются, глобальный терроризм, наркоторговлю, торговлю людьми и сексуальную эксплуатацию детей. Многие из этих угроз исходят от международных сетей враждебных акторов, имеющих доступ ко все более совершенным технологиям, позволяющим им коммуницировать незамеченными (см. *Big Brother Watch* и другие, цитируемые выше, § 323). Суд убежден, что оспариваемые правовые положения преследуют законные цели защиты национальной безопасности, предотвращения беспорядков и преступности и защиты прав и свобод других лиц.

69. Поэтому остается рассмотреть, содержало ли внутреннее законодательство адекватные и эффективные гарантии и защиты, чтобы соответствовать требованиям «качества закона» и «необходимости в демократическом обществе».

(α) Хранение интернет-сообщений и данных сообщений

70. Суд отмечает, что в нынешнюю, все более цифровую эпоху, технологические возможности значительно увеличили объем Интернет-сообщений, так что значительная часть связи принимает цифровую форму. Оспариваемое законодательство требует непрерывного автоматического хранения и сохранения содержания всех Интернет-сообщений в течение шести месяцев и связанных данных сообщений в

течение одного года. Оно применяется ко всем услугам Интернет-сообщений, используемым для передачи голосовых, текстовых, визуальных, звуковых, видео или других электронных сообщений (см. пункт 19 выше). Это затрагивает всех пользователей Интернет-связи, даже при отсутствии разумных подозрений в их причастности к преступной деятельности или деятельности, угрожающей национальной безопасности, или других причин полагать, что сохранение данных может способствовать борьбе с тяжкими преступлениями или защите национальной безопасности. Оно охватывает содержание всех сообщений и все данные сообщений без каких-либо ограничений по территориальному или временному применению или категориям лиц, чьи персональные данные могут быть сохранены. Суд поражен чрезвычайно широкой обязанностью хранения, предусмотренной оспариваемым законодательством, и приходит к выводу, что вмешательство является исключительно масштабным и серьезным (для сравнения *Ekimdzhiev и другие*, цитируемые выше, § 394, касающиеся только хранения данных связи).

71. Учитывая серьезность вмешательства, Суд будет особенно внимательно рассматривать вопрос, содержит ли национальное законодательство адекватные и достаточные гарантии против злоупотреблений, связанных с доступом правоохранительных органов к Интернет-сообщениям и связанным данным, хранимым ОКИ в соответствии с Законом об информации.

(β) Потенциальный доступ к сохраненным данным для целей направленного тайного наблюдения

72. Что касается законодательного требования предоставлять правоохранительным органам или службам безопасности доступ к сохраненным данным по их запросу, Суд повторяет, что доступ к данным в отдельных случаях должен сопровождаться, *mutatis mutandis*, теми же гарантиями, что и тайное наблюдение (см. *Екимджиев и другие*, цитируемые выше, § 395). Суд принимает во внимание аргумент Правительства о том, что доступ должен быть санкционирован судом. Однако он отмечает, что в России правоохранительные органы не обязаны по национальному законодательству предъявлять судебное разрешение поставщику услуг связи до получения доступа к сообщениям лица. Действительно, в соответствии с распоряжениями правительства, ОКИ обязаны установить оборудование, предоставляющее службам безопасности прямой доступ к сохраненным данным (см. пункты 24-26 выше). Таким образом, правоохранительные органы имеют прямой удаленный доступ ко всем Интернет-сообщениям и связанным данным связи.

73. Суд считает, что требование предъявлять разрешение поставщику услуг связи до получения доступа к сообщениям лица

является важной гарантией против злоупотреблений со стороны правоохранительных органов, обеспечивающей получение надлежащего разрешения во всех случаях тайного наблюдения. В России порядок доступа к сохраненным данным предоставляет службам безопасности технические средства обхода разрешительных процедур и получения доступа к сохраненным Интернет-сообщениям и данным связи без получения предварительного судебного разрешения. Хотя возможность недобросовестных, небрежных или рьяных действий со стороны должностных лиц никогда нельзя полностью исключить в любой системе, Суд считает, что система, наподобие российской, позволяющая службам безопасности напрямую получать доступ к Интернет-сообщениям каждого гражданина без необходимости предъявлять разрешение на перехват поставщику услуг связи или кому-либо еще, особенно подвержена злоупотреблениям. Следовательно необходимость гарантий против произвола и злоупотреблений является особенно высокой (см. *Роман Захаров*, цитируемый выше, §§ 269-70).

74. Правительство подтвердило, что доступ к сохраненным Интернет-сообщениям и связанным данным связи регулируется тем же правовым режимом, который был рассмотрен в деле *Романа Захарова* (цитируемое выше) в контексте перехватов мобильной телефонной связи. В этом деле Суд пришел к выводу, что российские правовые положения, регулирующие меры тайного наблюдения, не соответствуют требованию «качества закона», поскольку они не предоставляют адекватных и эффективных гарантий против произвола и риска злоупотреблений. Следовательно, они не могут ограничить «вмешательство» до уровня «необходимого в демократическом обществе». В частности, Суд установил, что обстоятельства, при которых государственные органы были уполномочены прибегать к мерам тайного наблюдения для целей выявления, предотвращения и расследования преступлений или защиты национальной, военной, экономической или экологической безопасности России, не были определены с достаточной ясностью. Разрешительные процедуры не могли гарантировать, что меры тайного наблюдения будут применяться только тогда, когда это «необходимо в демократическом обществе». Надзор за перехватом не соответствовал требованиям независимости, наличия полномочий и компетенций, достаточных для осуществления эффективного и непрерывного контроля, общественного надзора и реальной эффективности. Эффективность средств правовой защиты была подорвана отсутствием уведомления о тайном наблюдении на любом этапе или адекватного доступа к документам, относящимся к тайному наблюдению (см. *Роман Захаров*, цитируемый выше, §§ 243-305).

75. Суд не видит оснований для иного вывода в настоящем деле. Следовательно он считает, что национальное законодательство не

предоставляет адекватных и достаточных гарантий против злоупотреблений, связанных с доступом правоохранительных органов к Интернет-сообщениям и связанным данным, хранимым ОКИ в соответствии с Законом об информации.

(γ) Законодательное требование расшифровывать сообщения

76. Наконец, что касается требования предоставлять службам безопасности информацию, необходимую для расшифровки электронных сообщений, если они зашифрованы, Суд отмечает, что международные органы утверждали, что шифрование предоставляет сильные технические гарантии против незаконного доступа к содержимому сообщений и поэтому широко используется как средство защиты права на уважение частной жизни и тайны корреспонденции в Интернете. В цифровую эпоху технические решения для обеспечения и защиты конфиденциальности электронных сообщений, включая меры по шифрованию, способствуют обеспечению других фундаментальных прав, таких как свобода выражения мнений (см. пункты 28 и 34 выше). Кроме того, шифрование помогает гражданам и бизнесу защищаться от злоупотреблений информационными технологиями, таких как хакерство, кража идентификационных и персональных данных, мошенничество и неправильное раскрытие конфиденциальной информации. Это должно быть учтено при оценке мер, которые могут ослабить шифрование.

77. Как отмечалось выше (см. пункт 57), для того чтобы расшифровать сообщения, защищенные сквозным шифрованием, например, сообщения в «секретных чатах» Telegram, необходимо ослабить шифрование для всех пользователей. Эти меры, по-видимому, не могут быть ограничены конкретными лицами и затронут всех без разбора, включая лиц, не представляющих угрозы законным интересам правительства. Ослабление шифрования путем создания бэкдоров, по всей видимости, сделает технически возможным выполнение рутинного, общего и неограниченного наблюдения за личными электронными сообщениями. Бэкдоры также могут быть использованы преступными сетями и серьезно нарушат безопасность электронных коммуникаций всех пользователей. Суд принимает во внимание опасности ограничения шифрования, описанные многими экспертами в данной области (см. в частности, пункты 28 и 34 выше).

78. Суд признает, что шифрование также может использоваться преступниками, что может осложнить уголовное расследование (см. *Yüksel Yalçınkaya против Турции* [GC], № 15669/20, § 312, 26 сентября 2023 года). Однако, он отмечает в этой связи призывы к альтернативным «решениям для расшифровки без ослабления защитных механизмов, как в законодательстве, так и через постоянное техническое развитие» (см. о возможностях альтернативных методов расследования

Совместное заявление Европола и Агентства Европейского союза по кибербезопасности, цитируемое в пункте 33 выше, и пункт 24 Доклада о праве на частную жизнь в цифровую эпоху Управления Верховного комиссара ООН по правам человека, цитируемого в пункте 28 выше; см. также объяснение третьих лиц, выступающих в пункте 47 выше).

79. Суд приходит к выводу, что в настоящем деле законодательная обязанность ОКИ расшифровывать сообщения, защищенные сквозным шифрованием, рискует превратиться в требование к поставщикам таких услуг ослабить механизм шифрования для всех пользователей; следовательно, оно не является пропорциональным преследуемым законным целям.

(δ) Заключение

80. Исходя из вышеизложенного, Суд приходит к выводу, что оспариваемое законодательство, предусматривающее хранение всех Интернет-сообщений всех пользователей, прямой доступ служб безопасности к хранимым данным без адекватных гарантий против злоупотреблений и требование расшифровывать зашифрованные сообщения, применительно к сообщениям, защищенным сквозным шифрованием, не может считаться необходимым в демократическом обществе. В той мере, в какой это законодательство позволяет государственным органам получать доступ на общем основании и без достаточных гарантий к содержимому электронных сообщений, оно нарушает саму сущность права на уважение частной жизни предусмотренного статьей 8 Конвенции. Таким образом, государство-ответчик превысило допустимые пределы усмотрения в этом вопросе.

81. Соответственно, имело место нарушение статьи 8 Конвенции.

III. ПРЕДПОЛАГАЕМОЕ НАРУШЕНИЕ СТАТЬИ 13 КОНВЕНЦИИ

82. Заявитель жаловался на нарушение статьи 13 Конвенции на отсутствие у него эффективного внутригосударственного средства правовой защиты в отношении его заявления по статье 8. Учитывая факты дела, представления сторон и свои выводы по статье 8, Суд считает, что нет необходимости отдельно рассматривать приемлемость и сущность жалобы по статье 13 (см. Решение Европейского суда по правам человека, принятое Большой палатой, «*Центр юридических ресурсов от имени Валентина Кымпеану против Румынии*», № 47848/08, § 156, ECHR 2014 г.).

IV. ПРИМЕНЕНИЕ СТАТЬИ 41 КОНВЕНЦИИ

83. Статья 41 Конвенции гласит:

«Если Суд установит нарушение Конвенции или Протоколов к ней, а внутреннее право соответствующей Высокой Договаривающейся Стороны допускает лишь частичное устранение последствий этого нарушения, Суд, в случае необходимости, присуждает справедливую компенсацию потерпевшей стороне».

A. Ущерб

84. Заявитель потребовал 10 000 евро в качестве компенсации нематериального вреда.

85. Правительство сочло, что заявитель не может претендовать на возмещение морального вреда, так как его права не были нарушены.

86. Суд считает, что установление факта нарушения само по себе является достаточной справедливой компенсацией за любой нематериальный вред, причиненный заявителю (см. Решение Европейского суда по правам человека «*Роман Захаров против России*», цитируемое выше, § 312).

B. Судебные издержки и расходы

87. Заявитель не представил никаких требований в отношении судебных издержек и расходов.

ПО ЭТИМ ОСНОВАНИЯМ СУД

1. *Постановляет* единогласно, что он обладает юрисдикцией для рассмотрения жалоб заявителя в части, касающейся фактов, имевших место до 16 сентября 2022 года;
2. *Объявляет* единогласно жалобу, касающуюся предполагаемого нарушения права на уважение частной жизни и переписки, приемлемой;
3. *Постановляет* единогласно, что имело место нарушение статьи 8 Конвенции;
4. *Постановляет* пятью голосами против двух, что нет необходимости рассматривать жалобу по статье 13 Конвенции;
5. *Постановляет* шестью голосами против одного, что установление факта нарушения само по себе является достаточной справедливой компенсацией за любой моральный вред, причиненный заявителю;
6. *Отклоняет* шестью голосами против одного требование заявителя о справедливой компенсации.

Составлено на английском языке и объявлено в письменном виде 13 февраля 2024 года в соответствии с правилами 77 §§ 2 и 3 Регламента Суда.

Ольга Чернышова
Заместитель Секретаря

Пере Пастор Виланова
Председатель

В соответствии со статьей 45 § 2 Конвенции и правилом 74 § 2 Регламента Суда, к настоящему постановлению прилагается особое мнение судьи Сергхидеса.

П.П.В.
О.Ч.

ЧАСТИЧНО ОСОБОЕ МНЕНИЕ СУДЬИ СЕРГХИДЕСА

1. Жалоба заявителя заключалась в том, что его право на уважение частной жизни и переписки было нарушено из-за законодательного требования к «организаторам интернет-коммуникаций» (ОКИ) хранить содержание всех Интернет-сообщений и связанные с ними данные, а также предоставлять эти данные правоохранительным органам или службам безопасности по их запросу, вместе с информацией, необходимой для расшифровки электронных сообщений, если они были зашифрованы.

2. Хотя я согласен с пунктами 1-3 резолютивной части постановления, я с уважением не согласен с пунктами 4-6.

3. В частности, я не согласен с (a) пунктом 82 постановления и пунктом 4 его резолютивной части в том, что, установив нарушение статьи 8 в данном деле, нет необходимости отдельно рассматривать приемлемость и сущность жалобы по статье 13; (b) пунктом 86 постановления и пунктом 5 его резолютивной части, в которых установлено, что установление факта нарушения само по себе является достаточной справедливой компенсацией за любой моральный вред, причиненный заявителю; и (c) пунктом 6 резолютивной части, отклоняющим требование заявителя о справедливой компенсации.

4. Что касается решения Суда о том, что нет необходимости рассматривать жалобу по статье 13, я утверждаю, что, поскольку эта жалоба была подана заявителем, Суд обязан ее рассмотреть, иначе право заявителя на эффективное средство правовой защиты не будет обеспечено Судом. Как и любое другое право по Конвенции, которое якобы было нарушено, право по статье 13 должно быть рассмотрено и обеспечено Судом в соответствии с принципом эффективности и неделимости прав, а также правом на индивидуальное заявление, которое является краеугольным камнем Конвенции. Однако Суд не может обеспечить заявителю эффективную защиту, если он решает, как в данном случае, не рассматривать соответствующую жалобу.

5. Переходя к вопросу о моральном вреде, заявитель требовал 10 000 евро (см. пункт 84 постановления), в то время как Правительство утверждало, что он не может претендовать на возмещение нематериального вреда, так как его права не были нарушены (см. пункт 85 постановления). Однако Суд установил, что в данном деле имело место нарушение статьи 8 – нарушение, которое, по моему мнению, было серьезным. Я также утверждаю, что заявитель понес моральный вред в данном деле и поэтому должен был получить денежное возмещение в этом отношении по статье 41 Конвенции. У меня была возможность в ряде особых мнений критиковать решение Суда об отклонении требований о возмещении морального вреда по статье 41, просто полагавшегося на стандартную фразу, а именно «установление

факта нарушения само по себе является достаточной справедливой компенсацией за любой моральный вред, причиненный заявителю». Для меня будет достаточным сослаться на три таких мнения, критикующих этот стандартный способ отклонения денежных требований в отношении нематериального вреда, что избавляет меня от необходимости повторять те же аргументы здесь снова: см., таким образом, пункты 3-16 моего частично особого мнения в деле «*Тингаров и другие против Болгарии*», № 42286/21, 10 октября 2023 года; пункты 22-38 моего частично совпадающего, частично особого мнения в деле «Юксел Ялчынайа против Турции [Большая палата]», № 15669/20, 26 сентября 2023 года; и пункты 4-10 совместного частично особого мнения, которое я подготовил вместе с судьей Феличи в деле «*Гржеда против Польши* [Большая палата]», № 43572/18, 15 марта 2022 года.