МЕЖДУНАРОДНОЕ И ИНТЕГРАЦИОННОЕ ПРАВО. ЕВРОПЕЙСКОЕ ПРАВО

DOI: 10.12737/jfcl.2020.045

Комментарий к постановлению Европейского суда по правам человека по делу «Брейер против Германии»*

ДЕДОВ Дмитрий Иванович, судья Европейского суда по правам человека, доктор юридических наук
Франция, F-67075, г. Страсбург
E-mail: Dmitry.Dedov@echr.coe.int

ГАДЖИЕВ Ханлар Иршадович, заведующий отделом судебной практики и правоприменения Института законодательства и сравнительного правоведения при Правительстве Российской Федерации, судья Европейского суда по правам человека в 2003—2017 гг., доктор юридических наук
Россия, 117218, г. Москва, ул. Большая Черемушkinsкая, 34
E-mail: khanlar9999@gmail.com

Стремительное развитие цифровых технологий сопровождается ростом осуществления массовых наблюдений, что непосредственно касается проблемы сбора, обработки и хранения персональных данных. Сторонники расширения использования массового наблюдения утверждают, что, хотя оно и сопряжено с вмешательством в частную жизнь граждан, но в то же время служит эффективным средством обеспечения необходимого уровня безопасности и предотвращения преступности. Вместе с тем очевидно, что государство обязано поддерживать разумные ожидания неприкосновенности частной жизни, обеспечивая эффективную и полную защиту основных прав и свобод человека и, в частности, защиту персональных данных, основанную на требованиях Европейской конвенции о защите прав человека и основных свобод. Европейский суд по правам человека в деле «Брейер против Германии» решил, что юридически необходимое неизбирательное хранение абонентской информации поставщиками телекоммуникационных услуг не нарушает ст. 8 указанной Конвенции. Суд установил, что рассматриваемое вмешательство было довольно ограниченным по своему характеру, сославшись при этом на рассмотренные как самим Судом, так и Судом ЕС дела, которые подтверждают его вывод об отсутствии нарушения. Однако согласно особому мнению судьи К. Ранзони гарантии по защите персональных данных в рассмотренном деле нельзя считать эффективными, поскольку доступ к личным данным может быть получен с легкостью, автоматически, и закон не предусматривает каких-либо ограничений против возможного злоупотребления. Кроме того, законодатель не предоставил эффективных средств защиты, включая судебный контроль за доступом к персональным данным. Суд проявил избирательный подход при обосновании своих выводов, не обратив внимания на все критерии, выработанные как им самим, так и Судом ЕС.

Ключевые слова: цифровые технологии, защита данных, частная жизнь, хранение информации, вмешательство, баланс интересов.

Для цитирования: Дедов Д. И., Гаджиев Х. И. Комментарий к постановлению Европейского суда по правам человека по делу «Брейер против Германии» // Журнал зарубежного законодательства и сравнительного правоведения. 2020. № 5. С. 112—123. DOI: 10.12737/jfcl.2020.045

Введение. Дело «Брейер против Германии»¹ посвящено проблеме баланса между частными и публичными интересами на современном этапе развития передачи данных в электронном виде. В более конкретном виде проблема касается защиты тайны переписки, когда такая информация сохраняется операторами связи за определенный период времени и может быть получена компетентными органами власти для достижения общественно значимых целей. Эта тема актуальна для российской практики, ей посвя-

щены так называемые законы Яровой², вменяющие в обязанность операторов связи создавать электронные хранилища информации. Операторы связи выступили против такой обязанности, так как она повлечет огромные затраты и неизбежно приведет к увеличению тарифов за оказание услуг связи. При этом проблема защиты тайны переписки и телекоммуникаций

² В составе пакета законов, принятых по инициативе депутата И. Яровой, центральное место занимает Федеральный закон от 6 июля 2016 г. № 374-ФЗ «О внесении изменений в Федеральный закон “О противодействии терроризму” и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности».

* Статья написана в рамках гранта РФФИ № 18-29-16051 «Основные тенденции в правовом регулировании цифровых технологий. Сравнительно-правовое исследование».

¹ Breyer v. Germany, no. 50001/12, 30 January 2020.

и права на личную жизнь в современных условиях цифровизации передачи данных остается открытой.

Прежде чем приступить к комментированию данного дела, отметим, что проблема защиты частной жизни является, вероятно, наиболее актуальной темой современности и требует от исследователей постоянно отслеживать изменения в законодательстве — как в международном, так и национальном, происходящие сдвиги в судебной практике, пытающейся динамично развиваться в поисках наиболее эффективных методов обеспечения гарантий неприкосновенности личной жизни.

В юридической литературе придается большое значение концепции частной жизни, при этом указывается, что право на ее неприкосновенность охватывает и другие права: на индивидуальную автономию, уединение, личную жизнь, контроль информации о себе, ограничение доступности, исключительный контроль доступа к частным сферам, конфиденциальность, секретность и др.³

Рассматриваемое право, предусмотренное ст. 8 Конвенции о защите прав человека и основных свобод (далее — Конвенции), не касается непосредственно неприкосновенности частной жизни, поскольку изложенное в ней определение относится лишь к частной и семейной жизни, жилищу и переписке. В то же время очевидно, что неприкосновенность частной жизни не ограничивается упомянутыми сферами. Сам Европейский суд по правам человека (далее — Суд, ЕСПЧ) характеризует ее как широкий термин, не поддающийся исчерпывающему определению⁴. Осознавая сложности с точным и окончательным установлением содержания этого права, Суд в деле “Niemietz v. Germany” по существу признал, что невозможно и не нужно пытаться дать определение понятия частной жизни, значение которого довольно широкое⁵. Отношение к Конвенции как к живому инструменту, в соответствии с которым она должна интерпретироваться в свете существующих условий, позволяет Суду реагировать на многие вызовы в век стремительного развития цифровых технологий. Изложенное касается и защиты персональных данных, о чем Конвенция умалчивает, и можно сделать вывод, что это право не защищено, как это предусмотрено в Хартии ЕС об основных правах, ст. 8 которой непосредственно регламентирует вопросы защиты данных личного характера. Доктрина защиты данных развивалась благодаря эволюции законодательства ЕС, включая

практику Суда ЕС, а также вследствие новых подходов в решениях ЕСПЧ и в первую очередь интерпретации ст. 8 Конвенции. Она стала рассматриваться как составная часть названного положения Конвенции. Суд в деле “Z. v. Finland” аргументировал, что защита медицинских данных имеет основополагающее значение для осуществления права на уважение семейной и частной жизни⁶. Как видно из анализа вынесенных Судом постановлений, он последовательно расширял пределы усмотрения судей в национальном правотворчестве, рекомендуя новые подходы, и в числе знаковых хотелось бы отметить решения по делам “Biriuk v. Lithuania”, “S. and Marper v. The United Kingdom”, “Peck v. The United Kingdom”.

Рассмотрим тенденции в развитии практики Европейского Суда по правам человека, которые прослеживаются в данном деле.

Поиск баланса интересов: теория и реальность.

Начнем с позиции национальных властей, и в данном случае — с мнения Конституционного суда Германии (далее — КС Германии), который рассмотрел нормы национального законодательства, регулирующие условия доступа к информации, представляющей собой переданные сообщения и иные контакты абонентов связи через мобильные телефоны с помощью оплаченных сим-карт. Конституционный суд Германии считается самым авторитетным судом стран — участниц Европейской конвенции о защите прав человека и основных свобод. Поэтому рассмотренное далее дело представляет огромный интерес с точки зрения судебного диалога между ЕСПЧ и КС Германии. Примеры такого диалога высочайшего профессионального уровня и на такую актуальную тему в свете решения проблем развития современных технологий в практике ЕСПЧ встречаются не часто.

Заявители являются активистами общественной организации — союза в защиту гражданских свобод против хранения персональной информации. Они подали соответствующий иск в Конституционный суд Германии для рассмотрения вопроса о конституционности соответствующих норм германского законодательства. Таким образом, дело не касается конкретного случая истребования персональной информации органами власти для выполнения определенных задач, связанных, например, с расследованием уголовного дела против заявителей; оно связано с традиционным конституционным нормоконтролем. Если такой контроль является обычным в компетенции конституционного суда, то для ЕСПЧ такой абстрактный контроль, вне связи с конкретным вмешательством в фундаментальные права и свободы, уже сам по себе является неординарным событием. В таких случаях ЕСПЧ принимает на себя компе-

³ См.: Flaherty D. H. Protecting Privacy in Surveillance Societies. The Federal Republic of Germany, Sweden, France, Canada and the United States. Chapel Hill, 1989. P. 8.

⁴ См.: Peck v. The United Kingdom, постановление от 28 января 2003 г., № 44647/98, § 57.

⁵ См.: Niemietz v. Germany, постановление от 16 декабря 1992 г., № 13710/88, § 29.

⁶ Z. v. Finland, постановление от 25 февраля 1997 г., № 22009/93, § 95.

тенцию по осуществлению абстрактного контроля в исключительных случаях, когда этого требует защита фундаментальных прав и свобод, поскольку в самом национальном праве предусмотрена возможность вмешательства в основные права со стороны органов власти. В сфере защиты персональных данных от прослушивания телефонных переговоров и контроля за передачей информации ЕСПЧ использовал такой подход к рассмотрению жалобы в виде абстрактного изучения качества национального законодательства в деле «Роман Захаров против властей Российской Федерации»⁷.

Отметим, что ЕСПЧ провел различие между делом Брейера и делом Р. Захарова на основании природы вмешательства в частную жизнь. В деле Р. Захарова это вмешательство происходило в виде секретного слежения за гражданином во время его переговоров по мобильному телефону, что представляет собой более серьезное и глубокое вмешательство в частную жизнь, чем в деле Брейера, которое касается доступа к файлам. Поэтому ЕСПЧ в этом деле не придавал такого серьезного значения вопросам судебного разрешения на вмешательство и системы независимого контроля и надзора за использованием, хранением и уничтожением полученной информации, поскольку эти элементы являются важными, но не имеющими решающего значения для определения пропорциональности при сборе и хранении персональных данных. На наш взгляд, такое различие лишено основания, поскольку доступность частных разговоров для прослушивания или частной переписки для прочитывания третьими лицами, независимо от того, в какой момент происходит такой доступ — в момент разговора или позже, расценивается как вмешательство в частную жизнь, и эта проблема является одинаково серьезной и глубокой. От того, в какой момент осуществляется прослушивание разговора, происходит оно непосредственно в живом эфире или в записи — содержание разговора и его значение для его участников от этого не меняется. Эти и другие различия в подходах и оценке дела Брейера и дела Р. Захарова, о которых пойдет речь далее, дают основания сделать вывод о двойных стандартах в практике ЕСПЧ.

В своих решениях Конституционный суд Германии анализирует в основном положения ст. 111—113 Закона о связи (the Telecommunications Act), которые неоднократно изменялись в связи с необходимостью реагировать на вызовы в реальном времени. Так, в июле 2016 г. ст. 111 Закона о связи была дополнена обязанностью оператора проверять данные личности абонента, так как анонимность пользователей не позволяла найти и получить переписку таких абонентов среди другой информации, которая была со-

хранена оператором связи. Более того, во избежание фальсификации личных сведений, предоставляемых операторам, которая на тот момент носила массовый характер, пользователи должны были предъявить удостоверение личности для получения услуг мобильной связи при покупке сим-карты. Эти данные регистрировались оператором связи в привязке к конкретному коммуникационному адресу (номеру телефона и карты), чтобы позже при необходимости идентифицировать пользователя и его переписку, даже если на момент заключения договора об услугах связи абонент не находился под подозрением в совершении преступления.

Оценка ситуации как фальсификации личных сведений, т. е. противоправное поведение, которое вменялось абонентам со стороны властей, является важным моментом для понимания развития ситуации с защитой права на личную жизнь в данной сфере. В этом случае наблюдается расхождение между либеральным и консервативным взглядами на проблему. Либеральный подход стоит на стороне абонента, который защищен презумпцией добросовестности, не стремится нарушить закон и избежать ответственности. Абонент не называет своего настоящего имени, если такая обязанность отсутствует, стремится обеспечить конфиденциальность своей переписки. Сторонники консервативного подхода, напротив, считают, что, согласившись на обработку своих данных цифровым способом, абонент таким образом соглашается на утрату конфиденциальности. Такие крайние подходы характерны для развития этих отношений в США, где крайне либеральный подход был продемонстрирован компанией Apple в 2016 г., когда после массового убийства в церкви в Сан-Бернардино один из преступников был убит и следователям понадобилась информация о его контактах из его личного телефона. Компания отказалась предоставить такую информацию, несмотря на разрешение суда, ссылаясь на защиту конфиденциальности данных своих абонентов как политику компании. Такая демонстративная и чрезмерная забота о своих абонентах в очевидной ситуации похожа на фарс. В результате репутация компании пострадала еще больше, так как следователи получили помощь одного из хакеров, который взломал защиту телефона, получив приличное вознаграждение.

На самом деле истина находится посередине. Добросовестный пользователь в нормальном демократическом обществе не выдает в публичное пространство (даже если это частный разговор или переписка) сведения, за которые ему было бы стыдно или которые могут носить признаки нарушения закона; такая информация, если только она не касается личных сведений о здоровье или личных отношений с близкими людьми, не может нанести никому ущерб. Однако это возможно лишь в идеальном мире, поскольку характер информации, которой об-

⁷ Roman Zakharov v. Russia [GC], no. 47143/06, 4 December 2015.

мениваются люди в частных беседах, может быть разнообразным и очень чувствительным для других людей: от политических анекдотов и интриг до сплетен и слухов — иначе жизнь кажется многим пресной и неинтересной. С другой стороны, личные разговоры обычно не преследуют цель нанесения ущерба другим людям, поэтому они не должны быть автоматически доступны для постороннего наблюдателя. Другими словами, даже теоретическая доступность личных контактов или вероятность их утечки должна постепенно изменить природу современного человека, сделать его более осторожным в своих высказываниях, более уважительным по отношению к другим людям. Конечно, многое зависит от воспитания человека и его желания самосовершенствоваться. Известно немало примеров утечки такой «чувствительной» информации, после которой их авторы подвергались общественному осуждению. И даже если они не выказывали смущения и стыда, большинство из них, вероятно, постараются усвоить этот урок и не допускать таких ошибок в будущем. Это приведет к фальши в отношениях (когда человек думает одно, а говорит другое), но только на первом этапе; в дальнейшем такой когнитивный диссонанс будет исправлен естественным образом.

Закон о связи Германии разделяет автоматический доступ к информации, которая хранится оператором связи в течение 6 месяцев (срок, довольно распространенный во многих странах, включая Россию) для публично значимых целей, а также ручной доступ к информации — в тех случаях, когда необходимо идентифицировать местонахождение абонента, т. е. для целей розыска. Статья 112 Закона о связи регулирует автоматический доступ, а ст. 113 регулирует ручной доступ к информации. Эта процедура отличается от российской практики, изученной ЕСПЧ в деле Р. Захарова, когда с помощью оборудования СОРМ, присоединенного напрямую к сети связи, правоохранительные органы в любое время имеют автоматизированный доступ к данным, которые передаются по сети в момент присоединения к линии связи конкретного абонента, интересующего органы. В Германии процедура доступа обусловлена обращением органов к оператору связи с запросом на получение информации от оператора связи и с его участием на основании данных пользователя и номера его телефона или адреса электронной почты. Процедура автоматического доступа эффективна для случаев, когда у органов имеется неполная информация об абоненте и его номерах телефонов и адресах в Интернете и необходимо воспользоваться дополнительной информацией, которая может находиться в распоряжении оператора связи. При ручном доступе обязанность предоставить информацию лежит полностью на операторе связи, поскольку органы ею не обладают.

В Законе не содержится исчерпывающего списка органов, уполномоченных истребовать персональные данные и переписку, однако упоминаются органы, занимающиеся расследованием уголовных преступлений и административных правонарушений, органы, отвечающие за предотвращение угроз общественной безопасности и публичному порядку, защиту Конституции и национальную безопасность (вооруженные силы, разведка и контрразведка).

Конституционный суд Германии также постепенно детализировал свою позицию, адаптируясь к требованиям времени. В 1983 г. Суд определил, что в контексте современной обработки данных защита человека от неограниченного сбора, хранения, использования и раскрытия его персональных данных охватывается конституционными гарантиями защиты прав личности, предусмотренными ст. 1 и 2 Основного закона Германии. Это основное право заключается в возможности человека самому определять раскрытие и использование своей личной информации.

В марте 2010 г. Конституционный суд Германии оценивал конституционность Директивы Европейского Союза 2006/24/ЕС, которая обязывает операторов связи хранить все данные трафика электронных коммуникаций между абонентами оператора в течение шести месяцев и использовать эти данные для раскрытия преступлений. Аналогичная норма Закона о связи была признана судом не соответствующей Основному закону как нарушающая право на защиту тайны переписки. Суд указал, что обязанность хранения информации сама по себе не является неконституционной, однако структура нормы не соответствует принципу соразмерности такого вмешательства. Положение Закона о связи не гарантирует адекватной защиты конфиденциальности и не представляет собой адекватное ограничение для целей дальнейшего использования информации с точки зрения прозрачности и защиты персональных данных.

К аналогичному выводу пришел Суд справедливости Европейского Союза, оценивая вышеуказанную Директиву⁸, посчитав, что обязательному хранению подвергается любая переписка, любые данные вне зависимости от того, относятся ли такие данные к совершению преступления или нет, а также вне зависимости от статуса абонента, т. е. возбуждено ли в отношении такого абонента уголовное преследование. На практике, как указано на примере дела компании Apple, часто возникают ситуации, когда необходимо проверить переписку обвиняемого или преступника до момента, когда возникли основания для возбуждения уголовного дела или до момента совершения самого преступления. Такие же возражения возникли и при рассмотрении конкретной ситуации в деле

⁸ Digital Rights Ireland and Seitlinger and Others (joined cases C-293/12 and C-594/12, EU:C:2014:238), judgment of 8 April 2014.

«Тексейра против Андорры»⁹, где заявитель считал, что его право на личную жизнь нарушено в связи с истребованием такой информации в целях расследования уголовного дела против заявителя в суде. Тогда ЕСПЧ не нашел нарушения, а судья Д. И. Дедов в своем совпадающем особом мнении отметил, что данное решение опровергает позицию Суда справедливости Европейского Союза, который рассматривал не конкретную ситуацию, а абстрактные нормы, оценивая абстрактно принцип соразмерности. Андорра не является членом Европейского Союза, поэтому данное сравнение не могло быть включено в текст постановления, а было использовано для особого мнения. Но суть послания состояла в том, что абстрактный контроль таких норм не является эффективным средством защиты; и следует исходить из конкретной ситуации, т. е. условий, при которых соблюдаются или игнорируются правовые гарантии защиты права на частную жизнь.

Суд ЕС позже воспринял эту критику положительно и в следующем деле подошел к проблеме более осторожно¹⁰. Не признавая автоматически незаконным действующее законодательство, суд отметил, что положения закона должны ограничивать цели получения информации, объем и период хранения действительной необходимостью. Также положения закона должны быть достаточно конкретными и ясными в целях обеспечения минимума гарантий защиты персональных данных от злоупотреблений властными полномочиями.

Можно предположить, что дело Брейера является подтверждением того послания в более развернутом виде, однако постановление ЕСПЧ по делу Тексейра не упоминается в постановлении по делу Брейера предположительно по причине того, что ЕСПЧ предпринял в данном деле именно абстрактный контроль качества закона. Таким образом, ЕСПЧ пошел в данном случае по стопам Конституционного суда Германии и Суда справедливости Европейского Союза, не найдя нарушения ст. 8 Конвенции. КС Германии и Суд ЕС шли к своему результату противоречивым путем, и дело Тексейра могло бы послужить для дела Брейера сигналом не только малоэффективности, но и опасности абстрактного контроля в таких вопросах. Посмотрим далее, как ЕСПЧ удалось прийти к такому результату с помощью абстрактного анализа качества закона. Для этого необходимо более глубоко исследовать позицию Конституционного суда Германии.

Мнение Конституционного суда Германии по делу. Данное мнение является абсолютно обоснованным развитием позиции КС Германии за предыдущие годы. В этом случае наблюдается развитие права в его классическом виде, когда законодатель по инициативе исполнительной власти реагирует на вызовы современности, и только после этого наступает время для конституционного контроля в целях определения, не зашла ли власть за пределы своей компетенции, не нарушены ли основные права и свободы человека.

Конституционный суд Германии решением от 24 января 2012 г., определил, что ст. 111, 112 и 113 Закона о связи в целом соответствуют Основному закону. Что касается положений ст. 112 и 113 об истребовании информации, хранящейся у операторов связи, их положения носят общий характер и реализуются с помощью специального законодательства. В частности, процедура получения информации в ручном режиме не подходит для динамичных интернет-адресов и органы власти могут требовать предоставления информации в ручном режиме только на основании кодов доступа.

На проблемы автоматического доступа суд обратил особое внимание, поскольку такой вид доступа составляет свыше 95% всех запросов. Суд указал, что рассматриваемые нормы закона являются основанием для вмешательства в право граждан на информационное самоопределение (informational self-determination), которое является частью права на свободное развитие личности. Данное право предполагает необходимость правовой защиты от неограниченного сбора, хранения, использования и передачи информации личного характера. Именно гражданину принадлежит изначально право решать, каким образом использовать и раскрывать указанную информацию. Гарантии защиты имеют значение в условиях получения органами власти доступа к такой информации способом, который находится вне контроля или оценки со стороны гражданина. Сфера такого права не ограничивается особо «чувствительной» личной информацией, поскольку любые данные личного характера должны подлежать защите независимо от контекста. В частности, право на информационное самоопределение предполагает, что подлежат защите и те персональные данные, которые раскрываются оператору связи при осуществлении услуг связи (это можно считать возражением идеям крайне консервативного толка).

КС Германии указал, что законодатель должен охватить регулированием каждый способ манипуляции с информацией, включая ее передачу, хранение, использование. Это регулирование должно осуществляться как против индивидуальных интересов, так и в интересах индивида, т. е. имеется в виду не только передача информации от оператора связи уполномоченному органу власти, но и сам порядок истребования этой информации. Каждое такое манипулирование информацией требует независимой и

⁹ Figueiredo Teixeira c. Andorra, no. 72384/14, 8 Novembre 2016.

¹⁰ Tele2 Sverige and Tom Watson and Others (joined cases C-203/15 and C-698/15, EU:C:2016:970), judgment adopted on 21 December 2016).

отдельной законодательной базы, хотя они обе должны представлять собой единое целое, находиться в системной связи друг с другом и даже в одном нормативном акте. Отношения по передаче и истребованию информации корреспондируют друг другу. КС Германии фигурально называет такую систему регулирования «двойная дверь», когда одна «дверь» открыта для передачи информации органам власти, а другая — для создания запроса на получение доступа к информации.

Можно предположить, что таким образом КС Германии подчеркивает равное публичное значение этих двух действий, которые понимаются в системном единстве и дополняют друг друга. Это понимание основано на равной юридической защите публичных и частных интересов и означает ситуацию, при которой законодатель в равной степени отдает должное потребностям обеих заинтересованных сторон (орган власти и гражданин): первая заинтересована в получении информации от оператора связи, а вторая — в существовании особой необходимости в получении такой информации и отсутствии произвола. Эти действия и потребности разделены по времени, интересы не противодействуют друг другу одновременно, но они (особенно частный интерес гражданина) должны быть идентифицированы и удовлетворены.

КС Германии отметил, что вмешательство в право на информационное самоопределение происходит уже на этапе сбора и хранения информации оператором связи. Следующее вмешательство независимым образом от предыдущих возникает на этапе истребования информации уполномоченным органом у оператора связи. Обязанность оператора связи по передаче хранящихся у него персональных данных абонентов представляет собой еще одно вмешательство в фундаментальные права. Отношения по истребованию информации требуют дополнительного и детального регулирования на федеральном или земельном уровне.

Приводя в пример дело Р. Захарова, ЕСПЧ указывает на различия между этими делами и подчеркивает, что обязательство хранить и предоставлять доступ к персональным данным не было решающим фактором для нахождения нарушения ст. 8 Конвенции. Действительно, ЕСПЧ обратил внимание и счел недостаточно эффективной систему контроля судов и прокуратуры за действиями органов власти для получения и дальнейшего использования полученной информации. К сожалению, в деле Брейера ЕСПЧ не идет так далеко и не ищет с пристрастием нарушения Конвенции, как он это сделал в постановлении по делу Р. Захарова.

Конституционный суд Германии, в свою очередь, определил, что обязанность по хранению персональных данных абонентов преследует законную цель, связанную с уголовным преследованием. Несмотря на то что база обеспечивает хранение широкого спек-

тра персональных данных и уголовные преступники могут предпринять меры для того, чтобы избежать контроля над ними путем использования коммуникаций анонимным образом, под вымышленными именами или с помощью сим-карт, приобретенных на подставных лиц, само по себе такое вмешательство в частную жизнь обосновано относительно ограниченной природой хранимой информации. Данный аргумент не представляется убедительным, но является ответом на позицию Суда ЕС, который счел несоразмерным хранение всех персональных данных без какой-либо селекции, например предварительного выделения информации, которая могла бы представлять интерес для уголовного преследования.

Однако КС Германии не нашел нарушения принципа соразмерности в отношении сбора и хранения информации. По его мнению, ограниченное содержание хранимой информации, позволяющей индивидуализировать и разделить весь массив персональных данных на основе индивидуальных сведений о каждом абоненте (имя, дата рождения, регистрационный номер в списке абонентов оператора связи) для дальнейшей передачи означает, что вмешательство каждый раз носит ограниченный и избирательный характер. Более того, сама процедура получения информации уполномоченным органом происходит в автоматическом режиме без посредничества оператора связи, что ограничивает круг лиц, имеющих доступ к такой информации. Передача информации происходит централизованно через Федеральное сетевое агентство (Federal Network Agency), однако данная организация не осуществляет контроль за наличием основания для истребования информации, и уполномоченные органы власти не обязаны обосновывать причины истребования информации. КС Германии придает значение тому, что законные цели (кроме уголовного преследования) сформулированы в слишком общем виде (в деле Р. Захарова это обстоятельство среди прочих привело к нарушению Конвенции), а полномочия органов власти по истребованию и использованию персональных данных, включая полномочия Федерального сетевого агентства, не подвергаются каким-либо особым ограничениям, а, напротив, предоставляют максимальную возможность для полноценного и эффективного выполнения стоящих перед ними задач в пределах их компетенции. При этом КС Германии отмечает, что предоставление информации для выполнения органами власти своих функций не является фактором, ограничивающим степень вмешательства в частную жизнь. Поэтому, несмотря на существенный характер такого вмешательства, оно, по мнению КС Германии, является соразмерным. В целом можно отметить, что вывод о соразмерности сделан Конституционным судом Германии при полном понимании многочисленных негативных факторов, таких как серьезность вмешательства, общий характер пол-

номочий органов власти при осуществлении такого вмешательства, низкий порог для предоставления запроса на получение информации, иногда отсутствие какого-либо обоснования необходимости получения информации и проверки такой необходимости независимым институтом, включая судебную власть; неведение, в котором находятся абоненты по поводу использования их персональных данных, отсутствие детального регулирования относительно дальнейшей судьбы переданной информации. На этом основании можно сделать вывод, что степень требовательности суда по проверке соответствия норм Закона о связи принципу соразмерности в данном случае значительно ниже, чем в деле Р. Захарова.

Позиция ЕСПЧ. В своей аргументации Суд обычно отталкивается от позиции сторон. В обращениях в Суд заявители утверждали, что обязательство хранить их данные в соответствии со ст. 111 Закона о связи нарушило право на неприкосновенность частной жизни, «поскольку согласно ему они были вынуждены раскрывать свои личные данные, которые впоследствии подвергались хранению» (§ 66). По их мнению, обусловленное вмешательство было чрезмерно серьезным, так как не предусматривало каких-либо предварительных требований к хранению и было применимо при этом ко всем пользователям мобильных телефонов, подавляющее большинство которых не были виновными лицами и не представляли какой-либо опасности или риска для общественной или национальной безопасности (§ 67). Заявители не акцентировали специально внимание на нарушении их прав по основаниям, содержащимся в ст. 112 и 113 Закона о связи (см. § 31, 32).

Суд, следуя хорошо установленной практике, прежде всего подчеркнул, что «статья 8 Конвенции... предусматривает право на форму информационного самоопределения, позволяя людям полагаться на свое право на неприкосновенность частной жизни в отношении данных, которые, хотя и нейтральны, однако собираются, обрабатываются и распространяются коллективно и в той форме или таким образом, чтобы их права могли быть задействованы» (§ 75)¹¹. В постановлении подчеркнуто, что ни один из предыдущих случаев, с которыми сталкивался Суд, не касался «хранения такого набора данных, как в настоящем деле» (§ 76).

По мнению Суда, обстоятельства рассматриваемого дела связаны с обычным хранением данных, относящихся к личной жизни человека (ст. 111 Закона о связи) и, следовательно, представляют собой вмешательство по смыслу ст. 8 Конвенции (§ 81). Как видно, в § 83 Суд вновь повторяет свою позицию: «...в контексте, в частности, хранения личной информации важно иметь четкие, подробные правила, регули-

рующие минимальные гарантии, касающиеся, среди прочего, продолжительности хранения, использования, доступа третьих сторон, процедур для сохранения целостности и конфиденциальности данных и процедур их уничтожения»¹². По мнению Суда, ст. 111 позволяет предвидеть вопросы, связанные с объемом данных, продолжительностью хранения и технические стороны вопроса. Суд считает, что для оценки гарантий по проблеме доступа третьих лиц и использования хранимых данных требуется прочтение ст. 111 в сочетании со ст. 112 и 113 (§ 85). Как полагает Суд, национальные власти руководствовались намерениями, преследующими «законные цели общественной безопасности, предотвращение беспорядков и преступлений, защитой прав и свобод других лиц» (§ 86). По сути, Суд соглашается с позицией Конституционного суда Германии, заявив, что эти данные или включают какую-либо очень личную информацию, или позволяют создавать личные профили, либо касаются отдельных событий (§ 92). Суд сослался на позицию Суда ЕС в деле *Ministerio Fiscal* (§ 54), по которому доступ полиции для целей уголовного расследования к информации о подписчике не может быть определен как серьезное вмешательство. Рассмотрев проблему контроля за запросами на информацию, Суд отметил, что возмещение ущерба может быть истребовано в соответствии с общими правилами в ходе судебного разбирательства в отношении действий властей. С учетом изложенного и ввиду предела усмотрения государств в решении данного рода вопросов Суд посчитал, что хранение личных данных заявителя их поставщиками услуг было пропорциональным и необходимым в демократическом обществе (§ 108—109). Таким образом, Суд решил, что хранение в интересах государства данных без разбора и независимо от того, существует ли разумное подозрение в отношении лица, которого касается эта информация, не нарушает Конвенцию.

Изложенная позиция Суда соответствует также избранному подходу в деле “*Big Brother Watch and Others v. The United Kingdom*”, которое все еще ожидает своего решения в Большой палате Суда. В этом деле Суд исходит из того, что при перехвате сообщений (контента) и связанных данных трафика режимы массовых сборов сами по себе не выходят за пределы широкого поля усмотрения, которым обладают власти при выборе средств защиты национальной безопасности. В реальности если нецелевой сбор такой информации, который следует считать гораздо более навязчивым по своей природе, может быть разрешен, тем более допустимо хранение данных подписчика. Между тем до рассмотрения дела *Big Brother Watch* Суд ЕС уже рассмотрел дела *Digital Rights Ireland* и *Tele2 Sverige* и постановил, что предварительное мас-

¹¹ См. также: *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*, постановление от 27 июня 2017 г., § 136—137.

¹² См.: *S. and Marper v. The United Kingdom*, постановление от 4 декабря 2008 г., § 99.

совое удержание поставщиками телекоммуникационных услуг данных о трафике и местоположении нарушают требования ст. 7 (право на уважение частной жизни) и 8 (право на защиту личных данных) Хартии об основных правах ЕС. Такой подход Суда ЕС в большей мере связан с тем, что он рассматривает хранение указанных данных и последующий доступ к ним со стороны правоохранительных органов в качестве серьезного вмешательства в права человека, защищаемые упомянутыми нормами.

Позиция Суда ЕС в упомянутых делах в отличие от дела *Ministerio Fiscal* заключалась в том, что благодаря сохранению данных, взятых в целом, можно сделать очень точные выводы относительно личной жизни людей. К этим данным относятся: повседневные привычки, постоянные или временные места жительства, регулярные перемещения, выполненные действия, социальные отношения этих лиц и социальные условия их проживания. Таким образом, ЕСПЧ в вопросах защиты данных при рассмотрении анализируемого дела опирался на практику Суда ЕС в вопросах защиты данных только в той части, в которой она способствует отсутствию нарушения, хотя и не стремится к использованию более низкого стандарта прав человека, как в деле *Big Brother Watch*, с чем также отчасти связаны разумные ожидания будущего решения Большой палаты.

В деле *Digital Rights Ireland* Суд ЕС отмечал, что законодательство должно установить ясный и точный объем и сферу применения, определив минимальные стандарты защиты персональных данных против злоупотреблений, незаконного доступа к ним. При автоматической обработке личных данных и в случаях, когда существует значительный риск незаконного доступа к ним, необходимость применения таких правил возрастает. Следует дифференцировать режимы удержания в свете цели борьбы с серьезными преступлениями. В то же время сбор персональных данных должен быть ограничен с точки зрения разрешенного срока хранения, географической местности и лиц, которые могут быть причастны к особо тяжким преступлениям. Другой набор требований касался доступа к данным правоохранительных органов, возможностям их использования, а также ограничений с правовой точки зрения на основании материальных и процессуальных условий.

Помимо требований названного постановления Суда ЕС, Суд в данном деле указал на возможность предварительного рассмотрения запроса о доступе к данным в суде или независимом административном органе, при этом Суд предусмотрел выдачу разрешения на использование данных только в случаях строгой необходимости для достижения заданной цели. К представляющему интерес требованию, вытекающему из рассуждений Суда, относится условие проведения различия между неодинаковыми категориями данных на основе их возможной полезно-

сти для преследуемых целей либо самих преследуемых лиц. Законодательство должно увязывать определение срока хранения с объективными критериями, чтобы обеспечить его пределы до той степени, которая крайне необходима.

Особое мнение — основа для дальнейших дискуссий. В рассматриваемом деле интерес представляет особое несовпадающее мнение судьи К. Ранзони, избранного от Лихтенштейна, который оказался единственным из семи судей палаты ЕСПЧ, кто выразил сомнение в правильности создания благодушной и всепрощающей атмосферы по поводу жалобы со стороны КС Германии и ЕСПЧ. Он изложил другую точку зрения как на факты, так и на интерпретацию общих принципов, лежащих в основе содержания тайны переписки и коммуникаций. Судья К. Ранзони проанализировал содержание требований ст. 8 Конвенции в отношении гарантий защиты права в случае хранения персональных данных, а также вопрос о соотношении придания незначительности самому факту хранения с тем, что в результате такого хранения уполномоченные органы получают доступ к огромному массиву данных. КС Германии обращает внимание на индивидуализированный характер выделения необходимой информации из всего массива на основании индивидуальных данных каждого абонента. Предположим, что судья К. Ранзони имеет в виду, что персональные данные, принадлежащие каждому абоненту, отделенные от остального массива, тем не менее достигают значительного объема, особенно в сравнении с действительно необходимой информацией или той, которая может представлять интерес для выполнения многочисленными органами власти разнообразных функций и задач. Судья обращает внимание на диспропорцию, имеющую место при удовлетворении публичных и частных интересов, что снижает эффективность гарантий защиты. В связи с этим он делает вывод, что публичные цели не ограничены борьбой с терроризмом, иными опасными преступлениями или вопросами национальной безопасности. Национальное законодательство обеспечивает хранение персональных данных и для иных, менее значимых, целей, а также обеспечивает доступ к такой информации иным органам власти, среди которых не только суд и прокуратура, но и таможенная и налоговая службы, службы по предотвращению чрезвычайных ситуаций, борьбе с серым рынком труда, финансовому мониторингу и выполнению разведывательных функций.

Судья К. Ранзони не согласился, что степень вмешательства в частную жизнь носит если не тривиальный, то очень ограниченный характер, даже если предположить, что на хранение не попадает чувствительная, интимная информация о личной жизни абонентов. Однако доступ к частной информации конкретного лица существенно упрощен благодаря наличию сведений о его номере мобильного теле-

фона. То есть номер мобильного телефона «привязан» к конкретному человеку и является в современных условиях его индивидуализирующим признаком. Это облегчает быстрый и прямой доступ к самой «чувствительной» и интимной личной информации, содержащейся в телефонном разговоре или в электронной переписке, что создает особую уязвимость для каждого человека.

В своей практике ЕСПЧ обращал внимание на широкие возможности по идентификации личности в сфере коммуникаций, как он это сделал в деле «Бенедик против Словении»¹³. При этом Суд выразил опасения в отношении того, что неограниченный доступ к истребуемой информации позволит получить сведения о деятельности конкретного лица, включая чувствительные детали о его интересах, убеждениях и интимной жизни. В данном деле Суд не обращает внимание на данные обстоятельства и не воспринимает позицию Суда ЕС в делах *Digital Rights Ireland* и *Tele2 Sverige* о хранении всей информации, которая затрагивает интересы всех абонентов сетей мобильной связи независимо от того, имеют они отношение к преступной деятельности или нет.

Однако, по мнению судьи К. Ранзони, данное дело имеет сходство с делами Суда ЕС. Так, ст. 111 Закона о связи предполагает создание единого реестра всех абонентов мобильной связи, причем данные реестра должны соответствовать действительности, т. е. исключить возможность скрыть настоящее имя абонента. Этому обстоятельству не дана должная оценка с точки зрения абстрактной оценки качества закона. Оанее ЕСПЧ обращал на это внимание и отмечал, что анонимность абонентов может иметь вполне объяснимые законные цели избежать преследования за свои убеждения или не привлекать к себе особого внимания и таким образом может способствовать свободному обмену мнениями¹⁴. Эта позиция Суда соответствует мнению Специального докладчика ООН по защите свободы мнения. Таким образом, по мнению судьи, вывод Суда об ограниченном характере вмешательства является преждевременным и необоснованным.

Что касается пропорциональности вмешательства в частную жизнь, судья К. Ранзони высказал сомнения по поводу соблюдения баланса публичных и частных интересов в данном деле в том смысле, что действующее законодательство не содержит гарантий против злоупотреблений властью. Он предложил ограничиться более конкретным подходом (это близко к тому, что Суд сделал в упомянутом выше деле Тексейра). Судья сослался на дело *Ministerio Fiscal*¹⁵, в котором Суд ЕС сформулировал следующий подход: чем менее серьезно вмешательство, тем легче

оно может быть обосновано для целей предотвращения и расследования преступлений. Большинство судей ЕСПЧ применили эту формулу ко всем другим случаям без всяких видимых причин для такой аналогии. Однако в том деле Суд ЕС признал обоснованность вмешательства исходя из конкретных обстоятельств дела (здесь также сказывается влияние дела Тексейра), поскольку была истребована информация по сим-карте, находившейся в украденном телефоне, за период продолжительностью всего 12 дней; запрос касался информации о контактах, сделанных с телефона в тот период, именах и номерах телефонов. Только при таких обстоятельствах Суд ЕС сделал вывод о том, что вмешательство не было серьезным.

Дело Брейера имеет отличительные черты, обусловленные не столько проблемой хранения, сколько проблемой истребования информации. Это дело не затрагивает особенности или детали уголовного преследования, оно не обладает какой-либо спецификой, особыми фактическими обстоятельствами, которые могли бы повлиять на сужение объема запрашиваемой информации, включая период времени с момента совершения преступления. Все прочие публичные цели, основанные на выполнении функций уполномоченными органами власти, имеют общий характер и могут включать все что угодно под предлогом защиты национальной безопасности. Отсутствуют какие-либо границы для получения доступа к персональным данным. Таким образом, предполагаемое вмешательство не основано на критериях, сдерживающих органы власти от произвола, включая, например, критерий острой социальной необходимости (“pressing social need”).

Судья К. Ранзони обращает внимание на огромное число граждан, чьи права затронуты таким вмешательством. Кроме того, ст. 112 Закона о связи позволяет органам власти получать доступ не только к конкретным номерам телефонов, но и к другим «похожим» номерам на основе неполных данных об абонентах, что существенно расширяет сферу поиска. Аналогичная проблема явилась основанием для нахождения нарушения в деле Р. Захарова, поскольку ЕСПЧ выразил сомнение в том, что российские суды проверяют необходимость прослушивания при выдаче разрешения в рамках оперативно-разыскной деятельности, так как почти в 100% случаев суды удовлетворяют запросы на прослушивание телефонных переговоров. Для дела Брейера у ЕСПЧ было припасаено другое мнение, допускавшее получение доступа к персональным данным абонентов, например с похожими именами. Учитывая эти обстоятельства, на основании критериев похожести, аналогии и неполноты информации можно сделать вывод о возможности доступа к огромному массиву данных на многих абонентов одновременно. И права всех этих людей будут подвергаться вмешательству, пока идет допол-

¹³ *Benedik v. Slovenia*, no. 62357/14, 24 April 2018.

¹⁴ *Delfi AS v. Estonia* [GC], no. 64569/09, § 147, 16 June 2015.

¹⁵ *Ministerio Fiscal* (C-207/16, EU:C:2018:788).

нительное расследование и поиск настоящих правонарушителей и их персональных данных.

Центральное место в данном деле занимает проблема оценки гарантий защиты права на защиту персональных данных от злоупотребления властью и произвола. Судья К. Ранзони считает, что гарантии защиты нельзя назвать эффективными, поскольку доступ к персональным данным может быть получен с легкостью, автоматически, как сказано в самом Законе о связи, и не существует каких-либо препятствий или барьеров против произвола, вызываемого такой легкостью и автоматизмом. В результате в 2015 г. органы власти получили доступ почти к 35 млн пакетов данных в автоматическом режиме. Концепция «двойных дверей», придуманная Конституционным судом Германии, не работает в полной мере, поскольку к ним несложно подобрать ключи, чтобы получить доступ к информации, а с обратной стороны «двери» нет никого, кто мог бы проверить наличие пропуска. Таким пропуском могло бы служить обоснование необходимости получения информации. Однако, как верно указал КС Германии, власти не обязаны обосновывать такую необходимость, и этот вопрос вряд ли когда-нибудь возникнет. Судья отмечает, что КС Германии сам выразил сомнение в том, что Федеральное сетевое агентство может служить таким барьером на пути произвольного вмешательства, поскольку ответственность за законность требования о доступе к информации лежит на органе власти, а не на Агентстве, а операторы связи не имеют права требовать такого обоснования у органов власти, которые сами заполняют форму запроса и указывают на его законность. Какой-либо контроль со стороны независимых органов контроля, включая судебный контроль, в таких случаях не предусмотрен.

Судья К. Ранзони использует критерии абстрактной оценки качества закона из постановления ЕСПЧ по делу Р. Захарова, что справедливо и подчеркивает единство стандартов в обоих случаях. В данном деле Суд уклонился от использования этих стандартов. Он не обратил внимания на то, что доступ к информации происходит в режиме конфиденциальности, и граждане, чьи персональные данные были подвергнуты вмешательству, об этом не информируются и не могут оспорить необходимость вмешательства впоследствии, если им об этом станет известно. Возможность оспаривания вмешательства в личную жизнь указана КС Германии, но на деле она возникает только на этапе последующего вмешательства, например при прослушивании телефонных переговоров. Такая возможность, сама по себе ограниченная, существует еще и для ограниченного круга лиц, т. е. тех, кто подвергался уголовному преследованию. Остальные лица, чьи персональные данные были переданы властям, таким средством защиты воспользоваться не смогут.

Заключение. Анализ постановления позволил подробнее рассмотреть проблему защиты персональных данных. В целом надо признать, что доминирует прогосударственный подход, особенно если это касается стран с устойчивой демократией, где общество больше доверяет своим правоохранным органам, обеспечивающим национальную безопасность. Поиск баланса интересов переживает на этом фоне значительную динамику развития, в рамках которой сталкиваются и сближаются позиции крайне либеральная и крайне консервативная в пользу соответственно частных и публичных интересов. Однако на фоне огромного массива данных, который стал доступен для контроля властей над частной жизнью, вопрос доверия к государству остается доминирующим, что препятствует выработке единых критериев и единых стандартов в этой сфере.

Развитие, происходящее в последние годы в области защиты данных, демонстрирует активный рост законодательных актов в этой области, включая как общеевропейские на уровне ЕС, так и национальные, а также стремительное развитие практики — как международной, так и национальной. Отчасти это вызвано объективными потребностями роста наблюдений за подозрительными лицами со стороны правоохранных органов в целях обеспечения безопасности и защиты правопорядка. Обработка данных приобрела широко распространенный характер. Таким образом, появление и использование наиболее совершенных цифровых технологий требуют новых подходов для более эффективных форм защиты данных. Одним из основных недостатков часто называют отсутствие последовательности, особенно в вопросе обработки личных данных, несоблюдение принципов защиты минимальных стандартов. Необходимость единых подходов исходит из самой природы Интернета, для которого границы имеют условный характер.

Следует учесть, что общим знаменателем всех прав на защиту данных является право вмешательства государства в предусмотренных законом случаях. Однако это вмешательство имеет определенные границы, и оно делает право на защиту данных предметом судебных разбирательств. Интерпретация положений законодательства судами и предложенные ими правовые подходы определяют суть самого права, показывая, было ли затронуто или даже нарушено данное право. Поскольку в анализируемом нами деле Европейский суд по правам человека старался (хотя и не проявив последовательности) все же следовать динамике развития законодательства и судебной практики ЕС.

Напомним важные этапы эволюции законодательства. В 1995 г. принята Директива о защите данных и введены далеко идущие обязательства по защите основных прав и свобод человека, в частности в отношении обработки персональных данных

в пределах своей юрисдикции. Принципы, кодифицированные в Директиве о защите данных, были в 2001 г. распространены на институты в соответствии с Регламентом о защите физических лиц в отношении обработки персональных данных органами, ведомствами и агентствами ЕС, в которых также был учрежден Европейский контролер по защите данных (EDPS). После этого в 2016 г. Европарламент и Совет на основе ст. 16 Договора о функционировании Европейского Союза приняли Общий регламент по защите данных (GDPR). Одновременно была принята Директива о защите физических лиц в отношении обработки персональных данных, связанных с уголовными правонарушениями или исполнением уголовных наказаний. GDPR заменил Директиву о защите данных мерами, прямо и единообразно связанными во всех странах ЕС с целью обеспечения более совершенных рамок для защиты данных, отвечающих вызовам глобализации и быстрого технологического развития.

На уровне судебной практики описанное законодательное развитие сопровождалось постоянным вниманием Суда ЕС, который посредством своей практики по защите данных пытался уверенно играть роль суда по правам человека. В значительной степени опираясь на Хартию основных прав, Суд ЕС в пределах своей юриспруденции расширил границы правовых оценок, обеспечив высокий стандарт защиты конфиденциальных данных: 1) по вертикали — в отношении государств — членов ЕС; 2) по горизонтали — в отношении политических ветвей ЕС, а также 3) по диагонали — в отношении частных компаний, наделенных соответствующими полномочиями по обработке персональных данных. Во-первых, по мнению Суда ЕС, ст. 16 Договора о функционировании ЕС и ст. 8 Хартии подразумевали необходимость полной независимости органов по защите данных, принятия ими решений в отношении государств, которые не смогли обеспечить достижение этой цели в своем законодательстве и не отменили нормы, предусматривающие применение мер наблюдения в нарушение права на защиту данных. Во-вторых, Суд ЕС посчитал, что ст. 7 и 8 Хартии предоставили субъектам данных право на защиту от практики систематического государственного надзора и таким образом были рассмотрены как несовместимые с основным законом ЕС и Директивой по хранению данных, которая требовала хранения личных данных для правоприменительных целей. В-третьих, Суд ЕС применил высокий стандарт защиты данных в отношении технологических компаний, в соответствии с

которым поставщики ИТ-услуг, предлагающие их на внутреннем рынке ЕС, соблюдают закон ЕС о защите данных и расширяют эту же защиту, предоставляемую субъектам данных. Именно в этом контексте Суд ЕС признал право быть забытым (*a right to be forgotten*), которое впоследствии было кодифицировано в Общем регламенте по защите данных и взято на вооружение национальными и другими международными судами. В правовой литературе подчеркивается, что в рассмотренных относительно недавно Судом ЕС делах установлен ряд строгих требований, которым должен следовать законодатель при разработке любого положения, чтобы оно не противоречило праву на неприкосновенность частной жизни и защиту личной жизни. В постановлениях Суда ЕС по получившим широкую известность знаковым делам *Google Spain*¹⁶ *Digital Rights Ireland* и *Schrems*¹⁷ Суд настаивал на основном характере и незыблемости названных прав. Таким же образом Европейский суд по правам человека в постановлениях по делам *P. Захарова* и *“Szabo Vissy v. Hungary”* (постановление от 16 января 2016 г.) подтвердил, что с целью соблюдения права на неприкосновенность частной жизни для государственных органов должны быть определены четкие пределы наблюдения за подозрительными лицами¹⁸.

Особо следует еще раз указать на роль национальных и международных судов, за которыми настоящее и будущее в защите персональных данных. Со временем баланс прав на неприкосновенность частной жизни и защиту личных данных, с одной стороны, и противоречивых интересов и прав, с другой стороны, будут в основном определяться судами. Это связано с тем, что методы разработки законодательства носят расплывчатый характер и предел усмотрения при интерпретации норм предполагается широким, опираясь на развивающуюся практику. Таким образом, задача как Суда ЕС, так и ЕСПЧ заключается в своевременном вмешательстве, чтобы обеспечить равномерное и последовательное толкование законодательства с целью поддержания единых стандартов на европейском континенте.

¹⁶ *Google Spain SL and Google Inc. v. Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez*, CJEU case C-131/12 (2014).

¹⁷ *Maximillian Schrems v. Data Protection Commissioner (“Safe Harbor”)*, CJEU case C-362/14 (2015).

¹⁸ См.: *Eliantonio M., Galli F., Schaper M. A Balanced Data Protection in the EU: Conflicts and Possible Solutions // Maastricht Journal of European and Comparative Law. 2016. No. 23 (3). P. 399.*

Библиографический список

Eliantonio M., Galli F., Schaper M. A Balanced Data Protection in the EU: Conflicts and Possible Solutions // *Maastricht Journal of European and Comparative Law*. 2016. No. 23 (3).

Flaherty D. H. *Protecting Privacy in Surveillance Societies. The Federal Republic of Germany, Sweden, France, Canada and the United States*. Chapel Hill, 1989.

Commentary on the Decision of the European Court of Human Rights in “Breyer v. Germany”

D. I. Dedov^a, Kh. I. Hajiye^b

^aEuropean Court of Human Rights, Strasbourg F-67075, France

^bInstitute of Legislation and Comparative Law under the Government of the Russian Federation, Moscow 117218, Russian Federation

E-mail: Dmitry.Dedov@echr.coe.int; khanlar9999@gmail.com

DOI: 10.12737/jflcl.2020.045

The rapid development of digital technologies is accompanied by an increase in the implementation of mass observations which directly concerns the problem of data collection, processing and storage. Those who support an increasing mass observation argue that, while it entails interference with the privacy of individuals, it also serves as an effective means of ensuring the necessary level of security and preventing crime. However, it is clear that the state is obliged to maintain reasonable expectations of privacy, ensuring effective and full protection of fundamental human rights and freedoms and, in particular, the protection of personal data based on the requirements of Article 8 of the European Convention on Human Rights. In the case of Breyer v. Germany, the European Court of Human Rights ruled that the legally required indiscriminate storage of subscriber information by telecommunication service providers does not violate Article 8 of the Convention. The Court found that the interference at hand was rather limited in nature, thereby invoking also the cases considered by both the Court itself and the EU Court that confirm its findings that there was no violation. Meanwhile, as follows from the separate opinion attached to the judgment, guarantees for the protection of personal data in the case at hand cannot be considered effective, since access to personal data can be obtained easily and automatically, and the law does not provide any restrictions against possible abuse. In addition, according to the same opinion, the legislator also failed to provide effective remedies, including judicial control over access to personal data. The Court was selective in justifying its conclusions, not paying attention to all the criteria developed by both the Court itself and the EU Court.

Keywords: digital technologies, protection of personal data, privacy, data storage, interference, balance of interests.

For citation: Dedov D. I., Hajiye Kh. I. Commentary on the Decision of the European Court of Human Rights in “Breyer v. Germany”. *Zhurnal zarubezhnogo zakonodatel'stva i sravnitel'nogo pravovedeniya* = *Journal of Foreign Legislation and Comparative Law*, 2020, no. 5, pp. 112—123. DOI: 10.12737/jflcl.2020.045 (In Russ.)

References

Eliantonio M., Galli F., Schaper M. A Balanced Data Protection in the EU: Conflicts and Possible Solutions. *Maastricht Journal of European and Comparative Law*, 2016, no. 23 (3).

Flaherty D. H. Protecting Privacy in Surveillance Societies. The Federal Republic of Germany, Sweden, France, Canada and the United States. Chapel Hill, 1989.