ГОСУДАРСТВО И ПРАВО В СОВРЕМЕННОМ МИРЕ: ПРОБЛЕМЫ ТЕОРИИ И ИСТОРИИ

DOI: 10.12737/jflcl.2019.6.1

ЗАЩИТА ЧАСТНОЙ ЖИЗНИ В ЦИФРОВУЮ ЭПОХУ*

ГАДЖИЕВ Ханлар Иршадович, заведующий отделом судебной практики и правоприменения Института законодательства и сравнительного правоведения при Правительстве Российской Федерации, доктор юридических наук
Россия, 117218, г. Москва, ул. Большая Черемушнская, 34
E-mail: khanlar9999@gmail.com

Каждая эпоха в развитии человечества характеризуется присущими ей вызовами и одновременно поисками наиболее адекватных ответов на них. Современный период ознаменован стремительным развитием цифровых технологий, принесших неоспоримые преимущества в области информации и коммуникаций, но в то же время сопровождающихся широкими возможностями вмешательства в частную жизнь, которые, в свою очередь, требуют принятия эффективных мер по обеспечению гарантий ее надежной защиты. Интернет-технологии и различные программные платформы не только упростили возможности общения, но и облегчили поиск информации о других людях в режиме онлайн. Многие сокровенные тайны личной жизни человека могут легко стать доступными чужим лицам.

Европейский подход к защите частной жизни, более всего воспринятый российскими законодателем и правоприменителем, рассматривает ее через призму достоинства личности, поддержания разумных ожиданий неприкосновенности личной жизни и наиболее точно отражает реалии цифрового века. Масштаб проблемы требует своевременной реакции законодателя путем постоянного внесения изменений в действующее правовое регулирование и систематического обновления законодательства, способного быстро и эффективно защитить частную жизнь и персональные данные личности. Судьям следует принять более современный подход к тому, что представляет собой разумное ожидание конфиденциальности в контексте цифрового общения и онлайн-сообществ.

Надежный уровень защиты предполагает изучение опыта таких органов международного правосудия, как Европейский суд по правам человека и Суд Европейского Союза, зарубежных конституционных и верховных судов, и соотнесение с ними национальных подходов и развития практики, особенно в сфере обеспечения баланса между защитой частной жизни и необходимостью укрепления собственной безопасности, предупреждения и раскрытия преступлений.

Ключевые слова: права человека, частная жизнь, технология, неприкосновенность, защита, персональные данные, конфиденциальность.

Для цитирования: Гаджиев Х. И. Защита частной жизни в цифровую эпоху // Журнал зарубежного законодательства и сравнительного правоведения. 2019. № 6. С. 5—20. DOI: 10.12737/jflcl.2019.6.1

PRIVACY PROTECTION IN THE DIGITAL AGE

Kh. I. HAJIYEV, Institute of Legislation and Comparative Law under the Government of the Russian Federation, Moscow 117218, Russian Federation
E-mail: khanlar9999@gmail.com

Each era in the development of mankind is characterized by the challenges inherent in the corresponding stage and at the same time by the search for the most appropriate responses to them. The current period is marked by the rapid development of digital technologies that have brought undeniable advantages in the field of information and communications and have been accompanied at the same time by numerous opportunities for interference with privacy, which in turn require the adoption of efficient measures to ensure reliable protection. Internet technologies and various software platforms not only simplified the possibilities of communication but also made the online search for information about other people easier. Many intimate secrets of personal life can become easily accessible.

The European approach to the protection of privacy (most widely adopted by Russian legislators and law enforcement agencies) examines it through the lens of the individual's dignity, maintains reasonable expectations of privacy and most accurately reflects the

* Статья написана при поддержке РФФИ в рамках научно-исследовательского проекта № 18-29-16051 «Основные тенденции в правовом регулировании цифровых технологий. Сравнительно-правовое исследование».

realities of the digital age. The scale of the problem requires the timely reaction of legislators by constant introduction of changes to the existing legal regulation and systematical update of legislation that can quickly and effectively protect the privacy and personal data of an individual. Judges should adopt a modern approach to what constitutes a reasonable expectation of confidentiality in the context of digital communication and online communities.

A reliable level of protection implies exploring the experience of international justice bodies such as the European Court of Human Rights and the Court of the European Union, national constitutional and supreme courts, correlating own approaches with theirs, and developing practices — especially in the sphere of ensuring a balance between privacy protection and the need to strengthen national security and the prevention and detection of crime.

Keywords: human rights, privacy, technology, integrity, personal data, confidentiality, protection.

For citation: Hajiyeв Kh. I. Privacy Protection in the Digital Age. *Zhurnal zarubezhnogo zakonodatel'stva i sravnitel'nogo pravovedeniya* = *Journal of Foreign Legislation and Comparative Law*, 2019, no. 6, pp. 5—20. (In Russ.) DOI: 10.12737/jflcl.2019.6.1

Частная жизнь и неприкосновенность данных: от доктрины к практике. Право на частную жизнь — достаточно широкое понятие и не просто охватывает желание человека сохранить тайность информации относительно его или ее личной жизни, но касается непосредственно стремления защитить неприкосновенность частной сферы от незаконного вмешательства, любых посягательств, способных ограничить или воспрепятствовать реализации простых и порой привлекательных сторон человеческой жизни, отражающих не просто наличие, но и состояние свободы личности. Одной из таких особенностей частной жизни является разработанное и широко применяемое «право быть в одиночестве».

Вместе с тем защита неприкосновенности частной жизни в последние десятилетия осложнена стремительным развитием технологий с широко применяемыми мерами наблюдения, съемками, записями, сбором, хранением и обработкой данных об отдельных людях. Парадокс прогресса в том, что создание и развитие Интернета и других цифровых технологий, расширивших границы наших познаний, служивших эволюции научной мысли, принесших обычный комфорт в жизнь каждого, несут в себе одновременно угрозу ограничения нашей же свободы в случаях отсутствия надежных правовых пределов и условий взаимодействия человека и технологий в целях защиты частной жизни. Использование данных ставит законодательство в области неприкосновенности частной жизни и защиты персональных данных перед сложными испытаниями и требует постоянных усилий с целью создания эффективной системы защиты, способной ответить на возрастающие вызовы в контексте обеспечения прав человека.

Общий регламент о защите данных (General Data Protection Regulation) от 27 апреля 2016 г. № 2016/679 в странах Европейского Союза вступил в силу 25 мая 2018 г. и рассматривался в качестве инструмента для решения обозначенных проблем. Однако указанное регулирование, по мнению исследователей, не дает адекватных ответов на расту-

щую тревогу среди европейских граждан, поскольку оно не предназначено для сегодняшней цифровой реальности¹.

Основой частной жизни служит автономия, способность самоопределения, позволяющая осознанно подходить к решению вопросов, как и каким образом наши данные могут быть использованы. При проверке конфиденциальности на предмет социальных ожиданий названная автономия может сужаться, что означает отсутствие полной идентичности двух важных элементов: конфиденциальности и защиты данных.

Важнейшим и, пожалуй, испытанным временем критерием служит разумность ожиданий защиты неприкосновенности частной жизни. Вместе с тем безграничная природа технологий предполагает как адекватность законодательных мер, так и необходимый уровень судебного правотворчества выражаемых в эволюционной интерпретации правовых норм, способных более мобильно и динамично реагировать на технологические новшества, чем это способен сделать законодатель. Справедливо отмечается, что «цифровизация» оказывает заметное воздействие на сферу правового регулирования, являясь важным (хотя и не единственным) фактором, обуславливающим ее динамику. В нее вовлекаются новые общественные отношения, которые прежде либо не существовали, либо не требовали правового регулирования или объективно не могли быть урегулированы правом². Анализ эволюции международного права и правосудия с параллельно развивающимся национальным правом и судебной практикой демонстрирует постоянный сдвиг в правовом реагировании, отражающий движение права в поисках своевременных ответов на влияние «цифровизации» с целью защиты неприкосновенности част-

¹ См.: De Hingh A. E. Some Reflections on Dignity as an Alternative legal Concept in Data Protection Regulation // *German Law Journal*. 2018. Vol. 19. No. 5. P. 1274.

² См.: Хабриева Т. Я., Черногор Н. Н. Право в условиях цифровой реальности // *Журнал российского права*. 2018. № 1. С. 94.

ной жизни и личных данных. Полнота анализа требует определенного освещения истории проблемы.

Считается, что отношения между неприкосновенностью частной жизни и правами личности можно назвать проблемным браком. Автор этих слов — Стиг Стрёмхольм, человек, который в 1967 г. в числе первых обозначил различие между двумя типами прав в работе «Право на неприкосновенность частной жизни и права личности: сравнительный обзор»³. Его идея заключалась в том, что право на неприкосновенность частной жизни должно рассматриваться в первую очередь как негативное право, которое защищает право человека на одиночество, в то время как права личности включают интересы человека представлять себя в публичном контексте и развивать свою индивидуальность. Одновременно он выдвигал гипотезу, что названное право первоначально возникло как американская концепция, выдвинутая Томасом Кули⁴ и ставшая известной после статьи «Право на неприкосновенность частной жизни»⁵. Вместе с тем развивались подходы к рассматриваемым правам и на европейском континенте, имеющие долгую и богатую историю.

Исследователи отмечали различия между американским и европейским подходами. Так, в основе американского отношения находится рациональное отношение к уважению свободы личности. Европейский подход отличается тем, что главное внимание сосредоточивается вокруг достоинства человека. Указанные различия объясняются значительным влиянием на объем соответствующих прав рациональности отношений. Так, если американское право о конфиденциальности чрезвычайно разграничено и считается, на европейский взгляд, минималистским, то европейская система защиты неприкосновенности частной жизни более широкая и, с американской точки зрения, довольно всеобъемлющая⁶. Важно подчеркнуть также, что в европейской правовой традиции сердцевина обеспечения рассматриваемой неприкосновенности зиждется на конституционных гарантиях. J. Q. Whitman ссылается на концепцию развития и реализации личности в качестве основного принципа немецкого подхода к неприкосновенности частной жизни, защита которой в немецкой правовой традиции рассматривается как аспект защиты личности, особенно достоинства человека. Такой подход, характерный для немецкой концепции, можно объяснить тем, что ее корни восходят к философии Кан-

та, Гумбольдта и Гегеля. Не случайно в продолжение традиций защиту личных данных сегодня также рассматривают с точки зрения защиты достоинства личности, что характерно для современного конституционного порядка Германии. Названную концепцию необходимо рассматривать в качестве одного из перспективных направлений исследования, особенно в связи с обработкой данных. Предполагается, что человеческое достоинство в контексте коммодификации⁷ и коммодизации⁸ персональных данных в Интернете следует рассматривать несколько в ином аспекте. По мнению Anne de Hingh, при будущем регулировании конфиденциальности и защиты данных внимание должно сместиться в сторону ограничивающих аспектов человеческого достоинства⁹.

Вместе с тем представляются интересными мысли видного французского политика Андре Сантини, предложившего сетевому сообществу «Декларацию прав цифрового человека», ставшую важной частью более обширного документа «Белая книга». Автор в указанном проекте исходит из того, что выполнение правом своего предназначения гарантируется обеспечением свободы слова, плюрализма мнений, свободы предпринимательства и конкуренции, защиты собственности. По его мнению, защита прав и свобод человека в цифровом мире — это то, с чего законодатель должен начинать и без чего дальнейшее законодотворчество лишается всякой опоры и основания.

Уникальность российской Конституции в том, что она, гарантируя в ясной форме право на неприкосновенность частной жизни (ст. 23), специально предусматривает возможность сбора, хранения, использования и распространения информации о частной жизни лица исключительно на основании его согласия (ст. 24). Названное регулирование, находясь в общеевропейском русле, позволяет реализовывать национальные доктрины с учетом выработанных на международном уровне концепций защиты частной жизни, соотносить собственные позиции с достижениями других правовых систем. Обоснованно отмечается, что проблема обеспечения прав человека в цифровом мире выходит на первый план¹⁰. Защита прав заключается в том числе в изучении и своевременном заимствовании многих элементов применяемых доктрин, законодательных регулирований и судебных интерпретаций, особенно практики конституционных судов, поскольку с деятельностью этих судов связывается во

³ Strömholm S. Right of Privacy and Rights of the Personality: A Comparative Survey. Stockholm, 1967.

⁴ См.: Cooley T. M. A Treatise on the Law of Torts. Chicago, Callaghan, 1888.

⁵ См.: Warren S. D., Brandeis L. D. The Right to Privacy // Harvard Law Review. 1890. Vol. 4. No. 5.

⁶ См.: Whitman J. Q. The Two Western Cultures of Privacy: Dignity Versus Liberty // Yale Law Journal. 2004. Vol. 113. No. 6.

⁷ Характеристика особенностей современного производства информационного продукта, который приобретает черты рыночного товара.

⁸ Такой период развития технологий (не только IT), когда создаваемые с помощью них товары/услуги становятся предметом массового спроса.

⁹ См.: De Hingh A. E. Op. cit. P. 1269.

¹⁰ См.: Талалпина Э. В. Право и цифровизация: новые вызовы и перспективы // Журнал российского права. 2018. № 2. С. 8.

многих странах надежда быстрого реагирования на новые вызовы ввиду технологического и технического развития. По мнению В. Д. Зорькина, какой бы ни была цифровая реальность по степени ее развитости, она в конечном счете должна подпадать под действие Конституции как нормативного акта, имеющего высшую юридическую силу в российской правовой системе, в том числе по отношению к законоположениям, регулирующим указанную сферу новых отношений¹¹. Важна выработка современных подходов, концепций, отвечающих новой реальности, когда цифровые технологии проникают во все сферы жизни. В этих условиях краеугольным камнем правовых исследований должна быть защита права на частную жизнь и защита данных, а также отношение к защите прав как к системе, необходимой в демократическом правовом порядке.

Конституционный Суд РФ, исходя из требований ст. 23 (ч. 2), предусматривающей право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, подчеркнул, что в силу ст. 15 (ч. 1 и 2) Конституции она имеет высшую юридическую силу, прямое действие и применяется на территории РФ. Законы и иные правовые акты, принимаемые в Российской Федерации, не должны противоречить Конституции РФ. Органы государственной власти, органы местного самоуправления, должностные лица, граждане и их объединения обязаны соблюдать Конституцию РФ и законы. Суд также признал, что отсутствие в федеральном законодательстве прямого указания на обязанность именно правообладателя интернет-сервиса, посредством которого осуществляется отправка и получение электронных сообщений, обеспечивать тайну связи, не может рассматриваться как свидетельство отсутствия у него такой обязанности¹².

В Конституции Соединенных Штатов прямо не упоминается право на конфиденциальность или защиту данных. Развитие этих доктрин происходило благодаря судебному правотворчеству, в котором основная роль принадлежала Верховному суду США. Однако для этого требовалось время. Так, еще в 1928 г. Суд рассмотрел дело *Olmstead v. United States*, касающееся несанкционированного прослушивания телефонных разговоров¹³. Рассматривающий дело судья Тафт первоначально считал, что Четвертая поправка к Конституции может быть расширена, чтобы распространить ее действие на телефонные разговоры. В то же время вместо того, чтобы проследить значение и роль

технологий, которую она играет в обществе, он обратился к закону о собственности, посчитав недобросовестным отнесение «проводов к части дома или офиса, протянутых вдоль шоссе». Суд усилил подход к Четвертой поправке в деле *Goldman v. United States*¹⁴, но вновь не нашел обоснованных и разумных различий между упомянутыми делами. Как отмечалось в литературе, оба дела — подтверждение отсутствия должной оценки новых технологий и того, как они функционируют¹⁵. Подход был изменен Верховным судом в 1967 г. в деле *Katz v. United States*¹⁶, постановившим, что использование правительством электронного устройства для записи разговоров внутри телефонной будки без ордера нарушило Четвертую поправку. Провозгласив, что Четвертая поправка «защищает людей, а не места», суд сделал серьезный сдвиг в своей практике, подчеркнув: «человек стремится сохранить свою конфиденциальность в конституционном порядке в зоне, доступной для общественности». В совпадающем мнении судья Харлан стремился установить общий стандарт неприкосновенности частной жизни согласно Четвертой поправке, выводя из предыдущих решений двойное требование. «Во-первых, человек продемонстрировал фактическое (субъективное) ожидание неприкосновенности частной жизни, и, во-вторых, это ожидание, которое общество готово признать “разумным”»¹⁷. Впоследствии использованная формула в виде «разумных ожиданий неприкосновенности частной жизни» стала в большинстве случаев лакмусовой бумажкой Четвертой поправки, особенно в делах, связанных с электронным наблюдением. Названная «разумными ожиданиями» формула перекочевала и в юриспруденцию Европейского суда по правам человека, который применяет ее в различных трансформациях. Для справедливости оценки заметим, что тогда же эта концепция подверглась критике как ослабляющая расширяющееся применение обысков и изъятий со стороны полиции, и что «эти ожидания нетрудно уменьшить, систематически объявляя по телевидению что... мы все сразу оказались под всеобъемлющим электронным наблюдением»¹⁸. Очевидно, что подход Верховного суда в деле *Katz* является приемлемым, когда проблема касается обыска или доступа к медицинским данным, но он не предоставляет надлежащих рамок оценки по Четвертой поправке данных, которыми владеют третьи лица, необходимых для реакции на те процессы, которые происходят в эпоху цифровых технологий. Оценивая в целом по-

¹¹ См.: Зорькин В. Д. Право в цифровом мире. Размышление на полях Петербургского международного юридического форума // Российская газета. 2018. 29 мая.

¹² Постановление КС РФ от 26 октября 2017 г. № 25-П по делу о проверке конституционности п. 5 ст. 2 Федерального закона «Об информации, информационных технологиях и о защите информации».

¹³ *Olmstead v. United States*, 277 U. S. 438 (1928).

¹⁴ 316 U. S. 129, 135 (1942).

¹⁵ См.: Price M. W. Rethinking Privacy: Fourth Amendment “Papers” and the Third-Party Doctrine // Journal of National Security Law and Policy. 2016. Vol. 8. P. 260.

¹⁶ 389 U. S. 347 (1967).

¹⁷ Id. at 361; Harlan J., Concurring.

¹⁸ *Amsterdam A. G. Perspectives on the Fourth Amendment* // Minnesota Law Review. 1974. Vol. 58. P. 349, 384.

следствия дела Katz, нельзя пройти мимо негативных последствий, особенно для цифровой конфиденциальности. В этом свою роль сыграла и доктрина третьей стороны¹⁹, эффект которой сегодня почти нулевой, хотя и он способствовал эволюции позиции Верховного суда в поисках адекватной реакции на широкое использование цифровых технологий.

Дальнейшие доктринальные изменения сопровождались эволюцией подходов Верховного суда, исходя из понимания того, что формулируемые позиции не просто отличаются современностью, но и должны учитывать значительные изменения в характере и объеме нарушений. Основные угрозы для неприкосновенности частной жизни возникают не при сборе личных данных, а при их последующем использовании. Несмотря на то что чаще всего рассматриваемые дела интересны с точки зрения законности сбора данных, важно обращать внимание, каким образом при распоряжении ими нарушено право на частную жизнь. Оцифровка информации, использование Интернета, внедрение, систем искусственного интеллекта для обработки и анализа огромных объемов данных увеличили масштабы вторичного использования. Таким образом, основное внимание в первую очередь следует уделять не обработке данных с минимальной долей затрат и с несравненно более высокими скоростями, а методу анализа. К изложенному необходимо добавить активную роль Конгресса США, принявшего ряд законов, защищающих граждан от несоразмерного вторжения как со стороны власти, так и частных лиц. Развивая доктрину конфиденциальности кибервека, усиливается внимание к киберактивности частного сектора в лице влиятельных корпораций и компаний.

Защита частной жизни и данных личного характера ясно представлена в Европе как на конституционном уровне, так и в Хартии Европейского Союза об основных правах (далее — Хартия) и в Европейской конвенции о защите прав человека и основных свобод (далее — Конвенция). Так, ст. 8 Конвенции и ст. 7 Хартии предусматривается уважение частной жизни. В отличие от Конвенции в Хартии (ст. 8) особо регулируются вопросы защиты данных, в ч. 2 данной статьи подчеркивается, что «обработка подобных данных должна производиться без манипуляций, в четко определенных целях, с согласия заинтересованного лица, либо при наличии других правомерных оснований, предусмотренных законом. Каждый имеет право на получение доступа к собранным в отношении него данным, и право на устранение в них ошибок». Интересно, что Конвенция Совета Европы о защите

физических лиц при автоматизированной обработке персональных данных 1981 г. провозглашает, подробно регламентирует защиту личных данных и предусматривает ее как обязательный элемент в случае присоединения к Конвенции государств — членов Совета Европы, который находится в юрисдикции Европейского суда по правам человека. Несмотря на разницу в регулировании между Конвенцией и Хартией, на практике в обоих актах обоснованно считается, что неприкосновенность частной жизни — основа защиты персональных данных. Как Суд ЕС, так и ЕСПЧ исходят из того, что понятие частной жизни не может интерпретироваться узко, поэтому, по их мнению, широко толкуемое понятие частной жизни включает и защиту данных. Статья 2 Конвенции о защите физических лиц при автоматизированной обработке персональных данных определяет «персональные данные» в качестве любой информации об определенном или поддающемся определению физическом лице. Согласно Общему регламенту по защите данных «персональные данные» означают любую информацию, относящуюся к идентифицированному или идентифицируемому физическому лицу («субъект данных»).

Практика Европейского суда по правам человека. Европейский суд по правам человека путем интерпретации ст. 8 Конвенции стремился не просто расширить пределы действия данной нормы или дать наиболее точное и ясное определение частной жизни, но и ответить путем эволютивного и динамичного толкования на возникающие со временем вопросы, включая эффективную защиту персональных данных. Так, в деле *Leander v. Sweden*, рассмотренном 26 марта 1987 г., Суд подчеркнул, что цель системы личного контроля в Швеции следует считать законной с точки зрения целей ст. 8 Конвенции, направленной на защиту национальной безопасности. Основной вопрос исследования заключается в установлении, было ли вмешательство предусмотрено законом и необходимо в демократическом обществе. Требование «предусмотрено законом» означает, что вмешательство должно иметь какую-либо основу в местном законодательстве. Однако этого недостаточно. Закон должен быть доступным, и лицо должно предвидеть его последствия.

В то же время требование предвидения в контексте тайного контроля персонала в областях, влияющих на национальную безопасность, не может быть аналогичным применительно к другим сферам. Это не означает, что человек должен иметь возможность предвидеть, какие проверки будут проводиться в его отношении специальной службой по защите национальной безопасности. В системе, применяемой к людям, закон должен быть достаточно ясным, чтобы дать им адекватное понимание в отношении обстоятельств и условий, при которых власти могут прибегнуть к такой тайной и потенциально опасной мере вмеша-

¹⁹ Согласно этой доктрине конституционная защита не относится к информации, переданной третьим сторонам, — будь то интернет-провайдеры, банки или телефонные компании, — поскольку мы «принимаем риск» передачи информации этими третьими сторонами государству.

тельства в частную жизнь (§ 49—51). В постановлении *Niemietz v. Germany* (от 16 декабря 1992 г.) Суд указал, что не считает возможным и необходимым пытаться дать исчерпывающее определение понятия «частная жизнь». Было бы слишком ограничительным сводить данное понятие к внутреннему кругу, в котором лицо может проживать собственную личную жизнь по своему усмотрению, полностью исключив из нее внешний мир. Уважение частной жизни должно включать определенную степень права устанавливать и развивать отношения с другими людьми (§ 29). В деле же *Amann v. Switzerland* (от 15 февраля 2000 г.) Суд отметил, что хранение данных, относящихся к частной жизни человека, подпадает под действие ст. 8 (п. 1) Конвенции. Он указал, что термин «частная жизнь» нельзя интерпретировать ограничительно и нет оснований исключать из этого понятия деятельность профессионального или делового характера. Такое расширительное толкование соответствует Европейской конвенции о защите физических лиц при автоматизированной обработке персональных данных, цель которой — защита прав и основных свобод, в частности права на неприкосновенность частной жизни гражданина в отношении автоматизированной обработки касающихся его данных личного характера (§ 65). В деле *Rotaru v. Romania* (от 4 мая 2000 г.) Суд еще раз напомнил, что хранение информации, касающейся частной жизни лица, в секретном реестре и раскрытие такой информации подпадают под действие ст. 8 (п. 1). Одновременно Суд, повторив некоторые из упомянутых положений, подчеркнул, что публичная информация может вторгаться в сферу частной жизни, когда она систематически собирается и хранится в файлах со стороны органов власти, особенно в тех случаях, когда такая информация касается отдаленного прошлого человека (§ 43). Добавим, что в указанном деле информация о частной жизни заявителя, в частности, касалась учебы, политической деятельности, судимости, причем некоторые из этих данных были собраны более 50 лет назад. В постановлении *M. M. v. The United Kingdom* (от 13 ноября 2012 г.) Суд определил, что рассматриваемые данные представляют собой как «личные данные», так и «конфиденциальные личные данные» в значении Закона о защите данных 1998 г. Они образуют «личные данные» и определены как особая категория данных в Конвенции Совета Европы о защите данных. Более того, эти данные отражают факты о судимости. В этом отношении Суд считает, что, хотя указанные данные являются публичной информацией, их систематическое хранение свидетельствует об их доступности для раскрытия спустя много времени, когда многие люди уже забыли об этом. Таким образом, когда осуждение или предостережение уходит в прошлое, оно становится частью личной жизни человека, которую необходимо уважать (§ 188).

Европейское законодательство недвусмысленно различает неприкосновенность частной жизни и за-

щите данных как по форме, так и по содержанию, хотя они часто пересекаются. Однако важно подчеркнуть, что защита персональных данных применяется при каждой их обработке, а влияние Суда на данный процесс происходит в случаях, когда он решит: рассматриваемая обработка представляет собой вмешательство в право человека на неприкосновенность частной жизни в соответствии со ст. 8 Конвенции. Суд только вырабатывает и развивает комплекс критериев для определения того, можно ли конкретную обработку личных данных включить в право на неприкосновенность частной жизни, используя, как правило, критерии, заключающиеся в характере данных и степени их обработки. Для Суда важно выяснить, насколько близка связь между данными и правом на неприкосновенность частной жизни. Отсутствие элемента «частности» данных подталкивает Суд проверить интенсивность обработки и регулярность хранения таких данных. В упомянутых делах *Amann v. Switzerland* и *Rotaru v. Romania* Суд согласовал обработку данных с конфиденциальностью субъектов данных, поскольку степень обработки была такова, что создавала проблемы с точки зрения неприкосновенности частной жизни, хотя это не происходило во всех делах²⁰.

Анализируя работу Суда в отношении интерпретации ст. 8 Конвенции, легко обнаружить, что он истолковал ее не просто как право личности, обеспечивающее гражданам свободу, но и образующее позитивное обязательство для государств. Такая практика как следствие расширяла применение права на неприкосновенность частной жизни, одновременно раздвигая пределы ее действия. Следуя применяемой доктрине, Суд, как мы указали, согласился с рядом понятий, важных для защиты данных в пределах права на неприкосновенность частной жизни. В их числе сбор таких данных, как запись телефонных переговоров, фотографии, материалы дела, записи в истории болезни, а также огромное количество данных, находящихся в руках государственных органов, к которым лицо имеет доступ. Суд в рассмотренных им делах установил определенные ограничения на использование и передачу данных личного характера третьим лицам. Он продемонстрировал на основе рассмотренных дел, что персональные данные могут собираться для определенных и законных целей, посчитав в качестве позитивного обязательства наличие соответствующего законодательства о защите данных. В постановлении *S. and Marper v. the United Kingdom* (от 4 декабря 2008 г., § 103) Суд подчеркнул, что защита персональных данных — фундаментально важный вопрос уважения права человека на частную жизнь.

²⁰ См.: *Gellert R., Gutwirth S. The Legal Construction of Privacy and Data Protection // Computer Law and Security Review. 2013. Vol. 29. P. 528.*

Национальное право должно предоставить соответствующие гарантии для предотвращения любой возможности использования личных данных способом, противоречащим требованиям Конвенции. Потребность в таких гарантиях возрастает, когда речь идет о защите личных данных, подвергающихся автоматической обработке, и не в последнюю очередь, когда они используются в полицейских целях. Национальное законодательство должно обеспечивать, чтобы такие данные были релевантными и нечрезмерными по отношению к целям, для которых они хранятся. Оно должно гарантировать, что эти данные хранятся в том виде, который позволит идентифицировать субъектов данных и не более, что требуется для целей их хранения. Следует предложить адекватные гарантии защиты данных от злоупотребления и неправильного обращения.

В соответствии с постановлением Суда *Roche v. the United Kingdom* (от 19 октября 2005 г.) заявитель был уволен из армии в конце 1960-х гг. В 1980-х гг. у него развилось высокое кровяное давление, а позже он уже страдал гипертонией и бронхиальной астмой. Заявитель был зарегистрирован в качестве инвалида и утверждал, что его проблемы со здоровьем являются результатом участия в испытаниях горчичного и нервно-паралитического газов, проведенных под командованием британских вооруженных сил в 1960-х гг. По мнению заявителя, он не имел доступа ко всей соответствующей и подходящей информации, которая позволила бы ему оценить любой риск, которому он подвергался во время своего участия в этих тестах. Суд решил, что нарушено право по ст. 8 Конвенции, заключающееся в невыполнении Соединенным Королевством своего позитивного обязательства по предоставлению эффективной и доступной процедуры, позволяющей иметь доступ ко всей соответствующей информации, чтобы оценить любой риск, которому заявитель подвергался во время испытаний. В деле *Körke v. Germany* (от 5 октября 2010 г.) Суд подчеркнул, что имеются разные возможности по обеспечению уважения частной жизни и характер обязательства государства будет зависеть от конкретного аспекта частной жизни в рассматриваемом деле. Выбор средств для обеспечения соблюдения требований ст. 8 Конвенции в сфере защиты против действий лиц находится в пределах усмотрения государства. В определенных обстоятельствах, однако, позитивное обязательство государства по ст. 8 Конвенции соблюдается надлежащим образом, если государство гарантирует уважение частной жизни в отношениях отдельных лиц между собой положениями законодательства, обеспечивающими основу для примирения различных интересов, которые соревнуются в обеспечении защиты в соответствующем контексте.

Следующая проблема касается поддержания баланса между правом на неприкосновенность частной жизни и проведением систематического мониторин-

га рабочего места для обеспечения безопасности с целью предотвращения или выявления случаев промышленного шпионажа, кражи коммерческой тайны, другой конфиденциальной информации, нарушений авторских прав и патентов, неразрешенного доступа к компьютерным системам, защиты компьютерной сети от перегрузки, а также предупреждения неприемлемого поведения сотрудников. Очевидно, что каждый работодатель заинтересован в обеспечении своих законных прав и интересов в целях защиты своего имущества и предупреждения вреда, который могут причинить действия сотрудников. В то же время процесс мониторинга поднимает серьезные вопросы, связанные с правами и свободами работников, поскольку он может привести к нарушению неприкосновенности частной жизни. Кроме того, такое вмешательство может сопровождаться существенным нарушением права на свободу общения.

В литературе отмечалась разница между подходами в правовом порядке США, который условно назван минимальным ожиданием неприкосновенности частной жизни, и европейским, который выражен частично в упомянутом деле *Niemietz v. Germany*: «...именно в течение своей трудовой жизни большинство людей имеют значительную возможность развивать отношения с внешним миром». Минимальному ожиданию соответствует «содержательный подход», когда суды «решают вопрос о законности интересов работодателя... путем анализа мониторинга и того, насколько содержание сообщения разумно связано с предлагаемыми целями». В «контекстуальном» подходе суды определяют обоснованность ожиданий работников «путем анализа процедур уведомления работодателя»²¹. Между тем в деле *Smyth v. Pillsbury* судья отметил, что истец не имел разумных ожиданий неприкосновенности частной жизни, несмотря на заверения его работодателя относительно конфиденциальности сообщений²². С учетом характера рабочего места и преследуемой цели утверждается, что нанятые для работы в компании сотрудники не имеют «разумных ожиданий конфиденциальности», поскольку отслеживаемые сообщения добровольно передаются по сети работодателя с использованием оборудования, предназначенного для выполнения бизнес-задач²³.

Возвращаясь к европейскому подходу, остановимся на деле *Barbulescu v. Romania* (от 5 сентября 2017 г.), рассмотренном ЕСПЧ. Оно касается реше-

²¹ *Kesan J. P.* Cyber-working or Cyber-shirking?: a First Principles Examination of Electronic Privacy in the Workplace // *Florida Law Review*. 2002. Vol. 54. P. 289.

²² См.: *Michael A. Smyth v. The Pillsbury Company*, 914 F.Supp. 97. E. D. Pa. 1996.

²³ См.: *Fazekas Ch. P.* 1984 Is Still Fiction: Electronic Monitoring in the Workplace and U. S. Privacy Law // *Duke Law and Technology Review*. 2004. No. 15.

ния частной компании уволить работника после проверки его электронных сообщений частного характера с рабочего компьютера, предварительно получив доступ к их содержанию. Заявитель указывал, что решение работодателя было основано на нарушении его частной жизни и национальные суды не защитили его право на уважение частной жизни и корреспонденции.

Суд пришел к выводу о нарушении ст. 8 Конвенции, посчитав, что власти не защитили должным образом права заявителя. Национальные суды не смогли поддержать справедливый баланс между интересами, находящимися под угрозой, не определив, получал ли заявитель предварительное уведомление от работодателя о возможности мониторинга его сообщений. Не учитывался также ими тот факт, что он не был проинформирован о характере и масштабах мониторинга или о степени вторжения в его личную жизнь и корреспонденцию. По мнению Суда, национальные суды не обратили внимание, во-первых, на конкретные причины, оправдывающие осуществление мониторинга; во-вторых, на то, мог ли работодатель использовать меру, повлекшую меньшее по характеру вмешательство; в-третьих, на то, возможно ли получить доступ к сообщениям без ведома заявителя.

В постановлении *Libert v. France* (от 22 февраля 2018 г.) заявитель — работник французской национальной железнодорожной компании был уволен после изъятия его рабочего компьютера, в котором были обнаружены файлы порнографического содержания и поддельные сертификаты, составленные для третьих лиц. Заявитель подчеркивал, что работодатель открыл его личные файлы, хранящиеся на жестком диске его рабочего компьютера. Суд не нашел нарушения ст. 8 Конвенции, указав, что в данном деле французские власти не преступили имеющийся у них предел усмотрения. Суд отметил, что просмотр файлов работодателем преследовал законную цель защиты прав работодателя, которые могут на законных основаниях добиваться, чтобы их сотрудники использовали компьютеры, предоставленные в их распоряжение, в соответствии с договорными обязательствами и применяемыми правилами. Как сказано в постановлении, французское право содержит механизм защиты конфиденциальности, который хотя и позволяет открывать профессиональные файлы, однако предусматривает ограничение, касающееся файлов, идентифицированных как личные. Такие файлы можно открывать только в присутствии работника. Национальные суды Франции решили, что указанный механизм не помешал бы работодателю открыть и эти файлы, поскольку они не были должным образом определены как частные. Наконец, Суд посчитал также, что местные суды

заявитель, и привели достаточно оснований, подтверждающих их выводы.

Хотелось бы особо упомянуть дело *Halford v. the United Kingdom* (от 25 июня 1997 г.), которое важно с точки зрения расширения защиты неприкосновенности частной жизни в переписке с использованием электронных сообщений. Суд подчеркнул, что перехват телефонных звонков служащих на работе является нарушением и отклонил доводы правительства об отсутствии у заявителя разумных ожиданий конфиденциальности этих звонков, так как они были сделаны с использованием телефонов, предоставленных работодателем.

В европейском подходе к рассматриваемой проблеме проглядывается очевидное опасение уменьшения роли конституционных прав, служащих основой конституционных ожиданий в защите от рассмотрения их в качестве простых элементов правовых отношений. Именно требования права человека влияют на кажущуюся бесспорность требований работодателей во всех случаях. Такой подход подтверждается и практикой конституционных судов. Общеизвестно, что в трактовке Конституционного суда Германии понятие достоинства представляется в качестве абсолютной и непреложной ценности. Такое понимание человеческого достоинства является одним из главных элементов конституционной идентичности. Подобное отношение характерно и для правовых систем других государств. Верховный суд Австрии в рассмотренном в 2002 г. деле установил, что мониторинг работодателем использования телефона сотрудника затрагивает достоинство сотрудников. Национальный суд Франции в деле *Onof v. Nikon* указал, что работодатель не может прочитывать личные сообщения, отправленные или полученные сотрудниками, не нарушая как право на неприкосновенность частной жизни, так и основополагающую свободу конфиденциальности переписки, даже если работодатель запретил использование в личных целях рабочего компьютера²⁴.

Для полноты анализа отдельных позиций ЕСПЧ назовем два постановления Палаты Суда, которые впоследствии были приняты на рассмотрение Большой палатой Суда: *Centrum för Rättvisa v. Sweden* (от 13 сентября 2018 г.) и *Big Brother Watch and Others v. the United Kingdom* (от 13 сентября 2018 г.). Хотя новые решения только ожидаются, но на данном этапе нельзя не указать на встреченное с определенной долей критики имеющее сдерживающий эффект признание Суда, что массовое наблюдение не нарушает Конвенцию, а служит цели использования режима массового перехвата для выявления неизвестных ранее

²⁴ См.: *Lasprogata G., King N., Pillay S.* Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy Through a Comparative Study of Data Privacy Legislation in the E. U., U. S. and Canada // *Stanford Technology Law Review*. 2004. No. 4.

угроз национальной безопасности, подпадая в рамки широкого предела усмотрения, которыми государства пользуются в выборе средства: «как наилучшим образом достичь законной цели защиты национальной безопасности». Справедливо оговориться, что Суд ранее лишь в деле *The Weber and Saravia v. Germany* (от 29 июня 2006 г., § 106) указал на последовательное признание им наличия у государства широкого предела усмотрения в выборе средств для достижения законной цели по защите национальной безопасности. Тем не менее Суд учитывал и риски, сопровождающие тайное наблюдение, которые способны подорвать или даже разрушить сами основы демократического порядка. Данное решение выносилось в пору значительного развития технических возможностей для перехвата, хранения и обработки больших данных (*big data*). В вышеуказанных делах Суд, излагая свою позицию в отношении допустимости сбора данных, прямо указал на предел усмотрения; это фактически не что иное, как признание консенсуса. Эти дела демонстрируют, как активно государства могут использовать массовый перехват сообщений, личных данных и метаданных, указывая не просто на угрозу вторжения в частную жизнь огромного количества людей, но и уязвимость самой системы защиты данных.

Практика Суда Европейского Союза. Рассмотрим некоторые, на наш взгляд, важные решения Европейского Суда Справедливости (Суд ЕС), который принял решающие меры по обеспечению защиты основных прав на защиту частной жизни и защиту личных данных согласно Хартии основных прав Европейского Союза. В этом ряду представляются интересными постановления по делу *Österreichischer Rundfunk and Others* (от 20 мая 2003 г.) и по делу *Lindqvist* (от 6 ноября 2003 г.), по вопросу, касающемуся сферы применения Директивы о защите данных 95/46/ЕС, замененной принятым в апреле 2016 г. Общим регламентом по защите данных. В обоих делах Суд ЕС подтвердил применимость Директивы: он постановил, что Директива должна применяться в качестве общего правила и что отказ от ее применения должен представлять собой исключение, которое следует рассматривать в узком смысле. В деле *Lindqvist* Суд ЕС установил, что основные принципы Директивы имеют непосредственное отношение к использованию персональных данных на веб-сайтах. Обращение по ссылке на интернет-странице к различным лицам и идентификация их по имени или с помощью других средств, например номера телефона или информации об условиях работы и хобби, представляет собой «обработку персональных данных полностью или частично автоматически» по смыслу ст. 3 (1) Директивы. Важный вопрос, на который Суд ЕС должен был дать ответ, касался того, означает ли факт загрузки личных данных на интернет-сайте их доступности для тех, кто подключается к Интернету, включая граждан третьей страны. Следует учесть, что по смыслу Директивы 95/46 дол-

жен был осуществляться мониторинг передачи персональных данных в третьи страны и запрет на ее осуществление, если не обеспечивается адекватный уровень защиты. Суд решил, что обработка данных не является их передачей в третьи страны по смыслу ст. 25 Директивы. Иное толкование может привести к ситуации, когда государства должны будут предотвращать размещение любых личных данных на интернет-сайтах, когда лишь одна из стран, для которой доступна веб-страница, будет рассматриваться как не обеспечивающая соответствующий уровень защиты. Между тем важной чертой постановления *Österreichischer Rundfunk*, как первого по названной Директиве, является последовательная позиция, что нарушение основных свобод, и в частности неприкосновенности частной жизни, должно толковаться в свете фундаментальных прав и свобод, которые составляют неотъемлемую часть общих принципов права, соблюдение которых важно для Суда ЕС.

Право на доступ к документам и право на защиту личных данных основаны на договоре ЕС (см. ст. 255 и 286 Договора). Необходимость принятия ст. 286 была связана с желанием избежать правового вакуума, гарантируя защиту данных со стороны институтов ЕС. Эти права доступа к документам и защиты данных были впоследствии регламентированы в Хартии ЕС об основных правах. В деле *Bavarian Lager Company Ltd v. Commission* (от 8 ноября 2007 г.) речь шла о раскрытии имен официальных лиц (при отсутствии запроса о личных данных), которые содержались в протоколе встречи, и участники обоснованно могли ожидать раскрытия данных, поскольку они участвовали в заседании Европейской комиссии. Суд посчитал, что доступ к документам, содержащим личные данные, подпадает под соответствующие постановления, принятые Сообществом. В то же время ст. 4 (1) (в) постановления № 1049/2001 о публичном доступе к документам предусматривает, что институты ЕС должны отказывать в этом в случаях, когда раскрытие подрывает защиту конфиденциальности и целостности личности. В данном постановлении интересно то, как Суд ЕС понимает связь между конфиденциальностью и защитой данных. Он отметил, что понятие «частная жизнь» в широком смысле может включать в себя и защиту личных данных. Однако не все личные данные обязательно подпадают под понятие частной жизни, и тем более не все личные данные следует рассматривать как способные по своей природе подорвать частную жизнь (§ 114—115). Простое присутствие имени человека в списке участников собрания, действующих от имени организации, которую он представляет, не ставит, по мнению Суда ЕС, под угрозу защиту неприкосновенности частной жизни. В любом случае задача Суда — достигнуть лучшего баланса между двумя рассматриваемыми правилами.

Следующими важными постановлениями Суда ЕС по вопросам защиты права на частную жизнь и лич-

ных данных являются *Google Spain SL v. González* (от 13 мая 2014 г.) и *Schrems v. Data Protection Commissioner (Ireland)* (от 6 октября 2015 г.). Оба постановления основаны на положениях Директивы о защите данных 1995 г. и ст. 8 Хартии ЕС об основных правах. В первом деле жалоба была подана в Национальное агентство по защите данных против *Google Spain SL, Coogole, Inc.* и испанской ежедневной газеты “*La Vanguardia*”. Согласно жалобе *Google serch* привел имя заявителя в связи с опубликованными в 1998 г. в газете “*La Vanguardia*” объявлениями об аукционе его дома в связи с взысканием долгов по социальному обеспечению. По мнению заявителя, после того как разбирательство было завершено, упомянутая ссылка в газете потеряла актуальность. Он указал на обязанность газеты удалить соответствующие страницы с его личными данными, а *Google* просил распорядиться стереть или скрыть результаты поиска, ведущие на веб-страницы, содержащие эти ссылки. Выводы Суда были основаны на том, что деятельность такой поисковой системы, как *Google* следует квалифицировать как обработку персональных данных по смыслу Директивы о защите данных 1995 г., и что оператор поисковой системы считается «контролером» таких процедур. Суд также подчеркнул, что обработка данных рассматривается как осуществляемая на территории государства — члена ЕС, когда оператор поисковой системы создает в данном государстве филиал или дочернюю компанию для того, чтобы продвигать продажу рекламного пространства. Наконец, Суд особо остановился на «праве быть забытым», отметив, что при определенных условиях люди имеют право попросить поисковые системы удалить ссылки, содержащие личную информацию, когда последняя потеряла свою актуальность. И это даже в случаях признания самой публикации вполне законной. Как указал Суд в постановлении, «право на забвение», между тем, должно оцениваться не только в отношении экономической заинтересованности оператора поисковой системы, но также и относительно общественного интереса к наличию доступа к той же информации, когда человек играет публичную роль. Рассматриваемое дело по существу дало стимулирующий эффект для принятия Общего регламента (ЕС) 2016/679 о защите данных и отмене Директивы 95/46/ЕС. В то же время главная особенность дела *Google Spain* заключается в попытке Суда ЕС разрешить возможный конфликт с важнейшей свободой — свободой выражения в цифровом мире.

В связи с вышеупомянутым делом обратим внимание на другое постановление Суда ЕС — по делу *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni* (от 9 марта 2017 г.), где Суд указал на отсутствие «права на забвение» в отношении персональных данных в реестре компаний. Существуют различия между обоими делами, которые необходимо проанализировать.

Во-первых, основные права, поставленные под угрозу, в этих двух постановлениях различны. В *Google Spain* права на неприкосновенность частной жизни и защиту данных вступают в противоречие с необходимостью обеспечить свободу выражения мнений и информации (для предоставления публичного доступа к информации) и свободы ведения бизнеса в связи с деятельностью онлайн-платформы. В настоящем же деле интерес, который вступает в конфликт с правом на частную жизнь, заключается в обеспечении прозрачности деловых отношений с целью содействовать развитию внутреннего рынка, как это предусмотрено Первой Директивой на уровне ЕС от 9 марта 1968 г. и положениями национального права²⁵.

Немногим ранее анализируемого выше дела Суд ЕС принял постановление *Digital Rights Ireland Ltd.* (от 8 апреля 2014 г.), в котором высказал предположение о широкой интерпретации права на частную жизнь. Как отмечалось и в предыдущем деле, Правила хранения данных от 3 мая 2006 г. были введены для гармонизации национальных законодательств, регулирующих массовое хранение метаданных из цифрового трафика с целью предотвращения серьезных преступлений. В нем же подчеркивалось, что такие данные могут храниться не менее шести месяцев и не более двух лет. В рассматриваемом деле Суд ЕС сначала отметил, что вмешательство этих положений в права, установленные ст. 7 и 8 Хартии основных прав, было «особо серьезным», поскольку оно «может вызвать у заинтересованных лиц чувство, что их частная жизнь является предметом постоянного наблюдения» (§ 37). Названные Правила были отменены ввиду нарушения ими фундаментальных прав. Суд оценил, насколько вмешательство было оправданным в свете ст. 52 Хартии, которая допускает ограничения свобод при условии соблюдения самой сути этих свобод, если ограничения служат общим интересам и пропорциональны преследуемой цели. По мнению судей Суда ЕС, вмешательство не причинило вред самой сути права, ограничившись использованием данных и не рассмотрев содержание сообщения. При этом сбор данных был направлен на предотвращение преступлений и борьбу с ними, что оправдано соображениями общественной безопасности. В то же время возникли проблемы по вопросу соразмерности. Во-первых, директивные правила, по-видимому, носят общий характер и содержат пробелы, когда речь идет о людях, на которых влияет сбор данных, охватывающий «все население Европы» (§ 56) и «охватывает обобщенно всех людей и все средства электронной связи, а также все данные о дорожном движении без каких-либо раз-

²⁵ См.: *Pollicino O., De Gregorio G. Privacy or Transparency? A New Balancing of Interests for the “Right to be Forgotten” of Personal Data Published in Public Registers // The Italian Law Journal. 2017. Vol. 3. No. 2. P. 659.*

личий, ограничений или исключений, сделанных в свете цели борьбы с серьезными преступлениями» (§ 57). Во-вторых, правило «не устанавливает какого-либо объективного критерия, с помощью которого можно определить пределы доступа компетентных национальных органов к данным и их последующего использования в целях предотвращения, выявления или уголовного преследования за преступления, которые, с учетом степени и серьезности вмешательства в основные права, закрепленные в ст. 7 и 8 Хартии, могут считаться достаточно серьезными, чтобы оправдать его» (§ 60). Эффект постановления в первую очередь касался законодательства ЕС и, таким образом, оно не лишало законной силы национальные правила. Однако оно давало гражданам ЕС возможность добиваться отмены национальных правил хранения данных судами ввиду нарушения права на защиту личных данных²⁶. Интересно, что после решения Суда ЕС во многих правовых системах соответствующие правила были признаны неконституционными, подчеркивая тем самым возрастающую роль права на защиту личных данных²⁷.

Упомянутое постановление Суда ЕС в деле *Schrems v. Data Protection Commissioner (Ireland)* — результат небезосновательных опасений по обе стороны Атлантики, что трансграничную передачу личных данных между ЕС и США необходимо немедленно прекратить. Согласно постановлению австрийский активист по защите права на неприкосновенность частной жизни М. Шремс оспорил действительность так называемых принципов *Safe Harbor* («Безопасная Гавань») или, точнее, решение Комиссии от 26 июля 2000 г., одобрявшее названные принципы как гарантирующие адекватный уровень защиты персональных данных. Ирландское агентство по защите данных отклонило иск заявителя, признав достаточными гарантии, предусмотренные соглашением между правительством США и Европейской комиссией. Суд ЕС постановил, что существование решения Комиссии, устанавливающего, что третья страна обеспечивает надлежащий уровень защиты передаваемых данных, не может устранить или сократить полномочия, предоставленные национальному надзорному органу в соответствии с Директивой о защите данных 1995 г. или Хартией об основных правах. Он подчеркнул также, что только Суд

ЕС обладает полномочиями для принятия решения о том, что такой акт ЕС, как решение Комиссии, является недействительным. Как следует из постановления, законодательство ЕС, разрешающее публичным властям на общей основе иметь доступ к содержанию электронных сообщений, ставит под угрозу суть основного права на уважение частной жизни. То же самое относится и к законодательству, которое не предоставляет физическим лицам возможности использовать правовые средства защиты для доступа к личным данным. По мнению Суда ЕС, решение Комиссии должно быть признано утратившим силу, поскольку она не имеет полномочий по ограничению компетенций национальных надзорных органов.

Подчеркнем, что после указанного постановления Европейский Союз и Соединенные Штаты разработали новую схему — *Privacy Shield*, обязывающую компании США к строгому отношению к защите личных данных, требующую от властей США более надежного мониторинга и обеспечения выполнения обязательств в тесном сотрудничестве с европейскими органами по защите данных. Крупные многонациональные технологические компании, расположенные в США, такие как Google, Facebook, Apple и Microsoft, более не имеют права автоматически передавать данные пользователей. При этом они должны принять типовые положения для каждого случая передачи данных из ЕС в США, соблюдая правила ЕС. Соответственно, после постановления Суда ЕС многие компании начали принимать типовые договорные положения для продолжения передачи данных согласно решениям Европейской комиссии по договорным положениям. Принятие таких положений может быть временным решением, но в долгосрочной перспективе представляется не таким эффективным методом в связи с неспособностью предотвратить общие меры наблюдения со стороны государственных органов США²⁸.

В продолжение предыдущей позиции Суда ЕС заметим, что в 2017 г. Суд ЕС по просьбе Европарламента рассмотрел так называемое дело *PNR* на предмет получения мнения о соответствии соглашения между ЕС и Канадой о передаче и обработке данных пассажиров требованиям ст. 7 и 8 Хартии об основных правах с точки зрения защиты персональных данных (мнение 1/15 Суда ЕС от 26 июля 2017 г.). В Соглашении предусматривалась передача авиаперевозчиками, функционирующими между ЕС и Канадой, определенных личных данных пассажиров в правительственные органы Канады с целью борьбы с серьезными преступлениями и терроризмом. В своем мнении Суд ЕС заключил, что предлагаемое Со-

²⁶ См.: *Vanoni L. P. Balancing Privacy and National Security in the Global Digital Era: A Comparative Perspective of EU and US Constitutional Systems // The Fragmented Landscape of Fundamental Rights Protection in Europe: the Role of Judicial and Non-judicial Actors / ed. by L. Violini, A. Baraggia. Northampton, 2018. P. 120.*

²⁷ См.: *Vainio N., Miettinen S. Telecommunications Data Retention after Digital Rights Ireland: Legislative and Judicial Reactions in the Member States // International Journal of Law and Information Technology. 2015. Vol. 23. Iss. 3. P. 290.*

²⁸ См.: *Bu-Pasha Sh. Cross-border issues under EU data protection law with regards to personal data protection // Information and Communications Technology Law. 2017. Vol. 26. P. 218.*

глашение о передаче персональных данных пассажиров по ряду перечисленных в мнении обстоятельств несовместимо с правом на защиту частной жизни и защиту личных данных.

В одном из недавних решений Суд ЕС, рассмотрев дело *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH* (от 5 июня 2018 г.), подчеркнул, что администратор страницы Facebook должен рассматриваться в качестве совместного контролера вместе с Facebook и, таким образом, также отвечать за обработку персональных данных посетителей фан-страницы. Аргументация Суда ЕС заключается в том, что администратор участвует в определении целей и средств обработки данных. Это имеет место и в случаях, когда администратор не осуществляет сбор и обработку персональных данных. В качестве совместного контролера администратор будет нести ответственность за неправильное информирование посетителей о действиях по обработке личных данных посетителей фан-страницы. Администратор должен взять на себя и другие обязанности в качестве контролера с Facebook, хотя их ответственность необязательно будет равной. Facebook считается контролером платформы как таковой, поскольку он собирает и обрабатывает персональные данные от пользователей фан-страниц с целью улучшения системы рекламы, включая создание статистики. Администратор страницы определяет параметры на основе собственных целей продвижения и получают соответствующие демографические данные, предоставленные Facebook. Постановление Суда ЕС подтверждает мнение о том, что в законе о защите данных не должно быть никаких пробелов относительно ответственности за неправильное информирование посетителей, и основные права каждого человека должны эффективно обеспечиваться.

В то же время следует указать, что несмотря на очевидные достижения Суда ЕС в усилении эффективности защиты права на частную жизнь и права на защиту личных данных в правовой литературе высказывались и замечания. Так, критически оценивая практику Суда ЕС, В. М. Пфистерер указывает на необходимость продолжения разработки комплексной, понятной и последовательной концепции выше-названных прав. При таком подходе Суд ЕС значительно повысит степень определенности, надежности и предсказуемости своей будущей практики и в конечном счете укрепит верховенство права в государствах — членах ЕС²⁹.

Практика национальных судов. Сложно утверждать, что суды в целом отличаются особо активным

участием в толковании и применении законов о защите частной жизни и персональных данных. Современные технологии предоставляют широкие возможности для вторжения в частную жизнь. Решение международных и национальных судов — отражение лишь небольшого количества случаев, несоразмерных масштабу явления, когда человеку удается добиться восстановления нарушенного права. В то же время существуют очень важные решения, в которых толкование законодательства имеет основополагающее значение для правоприменения. Отметим одновременно, что сами технологии, распространяясь на все сферы общественной жизни, не могли не затронуть судебную систему. Непосредственный доступ к цифровой информации, беспрепятственное использование источников могут оказать влияние на такие фундаментальные ценности, как независимость и беспристрастность судей, сохранение баланса между защитой права на частную жизнь и прозрачностью правосудия, требуя выявления и разрешения проблем с целью минимизации противоречий в данной сфере. Вместе с тем особая активность в поддержании баланса между защитой права на частную жизнь и защитой данных принадлежит конституционным и верховным судам.

В отсутствие всеобъемлющего закона о праве на частную жизнь практика судов *Великобритании* развивалась таким образом, чтобы защитить баланс между правами на уважение частной и семейной жизни и свободу выражения, закрепленными в ст. 8 и 10 Европейской конвенции о защите прав человека и основных свобод и введенными во внутреннее законодательство в соответствии с Актом о правах человека 1998 г. В 2018 г. был принят Акт о защите данных, регламентирующий вопросы осуществления контроля над использованием личной информации организациями, предприятиями или правительством.

По мнению исследователей, имеются две основные проблемы, связанные с государственным надзором за содержанием и метаданными личных сообщений. Во-первых, законы Великобритании и частичный надзор за деятельностью органов безопасности неизбежно отстают от программ перехвата данных службами безопасности. Таким образом, правовая база всегда будет отставать от технологических разработок и требовать регулярного обзора и проверки, если это будет соответствовать преследуемой цели. Во-вторых, другая главная проблема, о которой свидетельствует анализ таких судебных дел, как *Secretary of State for Home Department v. Davis, Watson and Others* (30 января 2018 г.) и *R (on application of Liberty) v. Home Secretary and Foreign Secretary* (20 апреля 2018 г.), заключается в том, что недавние законодательные реформы не смогли должным образом соблюсти нормы Европейской конвенции по правам человека и Хартии об основных правах. Было установлено, что национальные законы лишены транспарентности и непропорционально вмешиваются в право на хранение

²⁹ См.: *Pfisterer V. M. The Right to Privacy — A Fundamental Right in Search of Its Identity: Uncovering the CJ EU's Flawed Concept of the Right to Privacy // German Law Journal. 2019. Vol. 20. Iss. 5. P. 733.*

личных данных. В одном из указанных дел законодательство предоставило полномочия по перехвату данных органам, абсолютно не связанным с защитой национальной безопасности или предупреждением и раскрытием преступлений, в нарушение Хартии об основных правах³⁰.

В *Бельгии*, несмотря на ряд важных решений Конституционного суда, дела по защите права на частную жизнь в основном рассматриваются Кассационным судом Бельгии, который постоянно ориентируется на практику ЕСПЧ. Среди интересных решений можно отдельно назвать те, которые послужили совершенствованию доктрины использования доказательств, полученных незаконным путем, имеющих влияние на защиту права на частную жизнь. Данная доктрина восходит к постановлению по делу *Antigone* (14 октября 2003 г.), в котором судья разрешил использование незаконно добытых доказательств. По смыслу судебного решения до тех пор, пока незаконные действия не влияют на достоверность доказательств или не нарушают права на справедливое судебное разбирательство, использование незаконно полученных доказательств в судах является правилом. До 2003 г. нормы законодательства о доказательствах были строгими и местные суды систематически отклоняли доказательства, представленные работодателями, в случае их противоречия законодательству о защите права на частную жизнь. С делом *Antigone* все больше доказательств, полученных в результате действий работодателей и сотрудников полиции, нарушающих конфиденциальность, стали использоваться в суде. Рассматриваемая доктрина уменьшила степень защиты права на частную жизнь и личных данных. Нарушение права на частную жизнь не оказывает никакого влияния, если только не сопровождается нарушением права на справедливое судебное разбирательство.

В постановлении от 5 июня 2012 г. Кассационный суд Бельгии (№ 11.2100. № 5, 5 июня 2012 г.) рассмотрел дело относительно использования скрытой камеры наблюдения со стороны частных лиц, установивших камеры на балконе для слежки за автомобилями, которые несколько раз подвергались вандализму. Камера засняла мужчину, прокалывающего шины. Отснятый материал был раскрыт для инициирования расследования. Приемлемость доказательств была оспорена в соответствии со ст. 6 Конвенции (уважение права на защиту), одновременно с этим указанный мужчина утверждал о нарушении его права на частную жизнь и защиту персональных данных. Кассационный суд применил «*Antigone* тест», установив, что нарушение указанного права пропорционально очень низко по сравнению с ма-

териальным ущербом, причиненным заявителям, не обнаружив нарушения ст. 8 Конвенции и Закона о защите данных 1992 г. и признав доказательства приемлемыми. Суд также разъяснил свое решение тем, что «видеокамера была расположена таким образом, чтобы вмешательство в право на неприкосновенность частной жизни прохожих было минимальным». Одновременно Кассационный Суд отметил, что Закон о защите данных 1992 г. не предусматривает санкции об исключении доказательств в случае выявленного нарушения. Наконец, по мнению Суда, объективная информация, полученная из материалов, которые помогли полиции установить личность вандала, была исключительно дополнительной и ограничивалась сугубо персональными данными. Таким образом, указанное постановление не содержит каких-либо ссылок на европейское право или практику. Кассационный суд не отрицает нарушения права на частную жизнь лица и не видит причин для отказа в использовании доказательства после баланса всех соответствующих интересов³¹.

Вопросы, рассматриваемые как Судом ЕС, так и ЕСПЧ в связи с «правом на забвение» (см. описанное дело *Google Spain SL v. Gonzalez* или постановление ЕСПЧ по делу *Węgrzybowski and Smolczewski v. Poland* от 16 июля 2013 г.), были предметом ряда судебных решений в *Италии*, которые, однако, отличаются иным подходом по сравнению с тем, который был принят названными судами. В постановлении от 5 апреля 2012 г. Верховный кассационный суд Италии подчеркнул, что при защите своих прав следует обращать внимание на жалобы не на поисковую систему, а непосредственно на владельца так называемого исходного веб-сайта. Последний при желании сохранить информацию в сети будет обязан обновить ее для того, чтобы она стала точной и полной. Рассмотренное дело возникло в связи с заявлением, зарегистрированным первоначально в органе защиты данных, а затем соответственно в Суде по гражданским делам г. Милана. Заявитель, пытаясь найти статью, опубликованную много лет назад и перемещенную в область исходного веб-сайта, обнаружил отсутствие проиндексированности поисковыми системами, или альтернативного обновления с добавлением новостей о событиях, произошедших после выхода указанной статьи. Заявитель указывал, что статья правильно сообщала о его аресте и могла бы вызвать публичный интерес, но не упоминала о последующих событиях — а именно об оправдании заявителя. Следовательно, с технической точки зрения этот случай не относился к «праву быть забытым», а касался желания субъекта данных, чтобы неполные и устаревшие новости были бы недоступны

³⁰ См.: The Right to Respect for Private Life: Digital Challenges, a Comparative-Law Perspective — The United Kingdom // EPRS: European Parliamentary Research Service. October 2018. P. 29—30.

³¹ См.: *De Hert P.* Belgium, Courts, Privacy and Data Protection: An inventory of Belgian case law from the pre-GDPR regime (1995—2015) // Brussels Privacy HUB: Working Paper. 2019. Vol. 5. No. 14.

в Интернете. Заявитель утверждал, что, не упоминая об оправдании, статья «породила неумолимый скандал вокруг него, ставшего жертвой распространяемого в СМИ позора». Реальная проблема для Суда заключалась в установлении того, должна ли информация — при наличии индивидуального права отдельного человека на информацию, доступную онлайн — постоянно обновляться так, чтобы личная идентичность субъекта данных достоверно отображалась по мере ее динамического развития, т. е. и в отношении недавних событий. Верховный суд в противовес решениям органа защиты данных и суда первой инстанции признал, что обстоятельства дела не могут быть истолкованы как требующие удаления из Интернета обновленных новостей. Правильный баланс между рассматриваемыми интересами, включая заинтересованность общества в учете прошлых новостей, требовал от ответственного за архив новостей лица соответствующего веб-сайта, публикующего новости, «системы, подходящей для оповещения о возникновении последующих событий и развития истории и того, что они из себя представляют, к чему должен быть предоставлен быстрый и легкий доступ, чтобы обеспечить постоянное внимание». Суд также подробно описал наличие обязательства добавлять и обновлять новости, которые более не являются точными, стали уже «историей» и включены в архивы, но в то же время потенциально наносят ущерб и могут нарушить «социальную защиту» личной идентичности субъекта данных — и это, по мнению Суда, опять же в случае существования общественной потребности в систематическом прослеживании событий прошлого, объясняемой необходимостью защиты своего права быть забытым со стороны субъекта данных. Суд отметил, что «это необходимо для защиты текущей социальной идентичности человека, которого волнуют новости, чтобы позволить себе последнюю контекстуализацию и обновление прошлых новостей, которые касаются его или ее» (постановление № 5525 Верховного суда (Гражданская секция III)).

Вывод Верховного суда заслуживает уважения, поскольку веб-сайт или онлайн-архив должен выделять ресурсы для разработки и управления системой, способной регулярно обновлять весь онлайн-контент. Если такое внедрение невозможно, соответствующий оператор будет нести ответственность за любой причиненный ущерб и за незаконную обработку персональных данных. Таким образом, рассмотренное постановление отличается от упомянутых подходов двух международных судов и представляет интерес для развития судебной практики.

Конституционный суд Германии, не оценивая Директиву о хранении данных (Directive 2006/24/EC) в целом, обнаружил тем не менее, что обязанность хранить данные без исключения (независимо от того, поддается ли лицо, чьи данные должны храниться, в преступлении) и отсутствие судебного контроля за

доступом к ним и их использованием является нарушением принципа пропорциональности и противоречит ст. 10 (1) Основного закона страны, защищающего тайну переписки. По мнению Конституционного суда Германии, хранение данных не является неконституционным, но оно нарушает право на неприкосновенность частной жизни и поэтому должно подлежать «строгой проверке соразмерности» (постановление от 2 марта 2010 г., 1 B v. R. 256/08).

В другом деле Конституционный суд Германии признал Закон о федеральном управлении криминальной полиции частично неконституционным, поскольку некоторые его положения, касающиеся полномочий по расследованию дел по борьбе с международным терроризмом, не были пропорциональными. Конституционный суд раскритиковал правовые требования для проведения скрытых мер наблюдения как слишком широкие и неопределенные, решив, что нормы закона, разрешающие передачу данных сторонним органам власти и властям третьих стран, не содержат достаточных правовых ограничений. Среди положений Закона, которые особо отмечены в постановлении, — положения о видео- и акустическом наблюдении за частными домами, признанные частично неконституционными. Суд отметил, что наблюдение было бы уместным, если бы оно сосредоточивалось исключительно на цели, а не на третьих лицах. Более того, любые собранные данные должны быть проверены независимым органом, затем использованы криминальной полицией, чтобы убедиться, содержат ли они конфиденциальную информацию особой важности. По мнению Суда, положения, которые открывают доступ к компьютерам, мобильным телефонам и другим системам информационных технологий, не обеспечивают достаточную защиту для «основной сферы» (т. е. наиболее неприкосновенной внутренней области) частной жизни. Относительно положения, позволяющего осуществлять наблюдение за частными домами, необходимо иметь независимый орган для оценки выполненных работ. В постановлении также подчеркивается, что нормы, предусматривающие надзор за текущими телекоммуникациями и сбор данных о телекоммуникационном трафике, были слишком широкими и не отличались конкретностью. Отсутствовали адекватная защита лиц, соответствующая принципу профессиональной конфиденциальности, инструкция проведения регулярных обязательных проверок, требования к исчерпывающей документации или обязанности по представлению отчетности перед парламентом и общественностью.

Конституционный суд Германии, наконец, подверг критике норму, допускающую исключение из обязанности удалять собранные данные, если они важны для обеспечения правопорядка, предотвращения преступлений или в качестве меры предосторожности для будущего преследования за совершение пре-

ступления, имеющего серьезное значение (постановление от 20 апреля 2016 г., 1BVR 966/09, § 200, 223—225, 131—144, 274).

Конституционный совет *Франции* постановлением от 12 июня 2018 г. одобрил новый Закон о защите данных, принятый в целях имплементации Общего регламента по защите персональных данных ЕС. Сенаторы французского парламента оспаривали конституционность многих положений Закона, которые в итоге были признаны соответствующими Основному закону, за исключением ст. 13, предусматривающей, что личные данные, касающиеся уголовных осуждений и правонарушений или связанных с ними мер безопасности, могут обрабатываться только «под контролем официальных властей» или определенными категориями лиц, перечисленными в Законе. Конституционный совет подчеркнул, что законодатель просто воспроизвел формулировку ст. 10 Общего регламента по защите данных, не указав категории лиц, уполномоченных обрабатывать такие данные под контролем официального органа, или цели такой обработки. Отсутствие конкретности в норме Закона послужило основанием признания слов «под контролем официальных властей» неконституционными. В результате данные слова не появились в одобренном тексте Закона³².

Заключение. Защита права на частную жизнь, безусловно, одна из самых необходимых ценностей,

своего рода система для демократического правопорядка. В определенных обстоятельствах она должна уступать место конкурирующим и очень важным интересам защиты национальной безопасности, предупреждения и раскрытия преступлений, несущих угрозу для демократического правления в целом. Вместе с тем необходимо, чтобы полномочия, предоставленные органам безопасности и полиции, главным образом осуществлялись пропорционально преследуемой цели и находились под контролем с точки зрения защиты права на частную жизнь. Главное в оценке законности использования мер против нарушений указанного права заключается в существовании ясного правового регулирования и требований о предварительном судебном контроле. Представляется особо актуальным в век бурного технологического развития систематически соотносить нормы национального законодательства и практику его применения с правовым регулированием и судебной практикой на международном и национальном уровне других стран. С целью своевременной и адекватной реакции на возникающие в правовом регулировании проблемы особо актуальными становятся развитие правотворческих функций судов, усиление эффективности их деятельности по выявлению пробелов и временному урегулированию, обращая одновременно внимание законодателя на обнаруженные судами факты отставания законодательства, вновь возникших правоотношений.

³² *Thompson M.* French constitutional court leaves GDPR bill largely intact // *Global Data Review*. 2018. 18 June.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

- Amsterdam A. G. Perspectives on the Fourth Amendment // *Minnesota Law Review*. 1974. Vol. 58.
- Bu-Pasha Sh. Cross-border issues under EU data protection law with regards to personal data protection // *Information and Communications Technology Law*. 2017. Vol. 26.
- Cooley T. M. A Treatise on the Law of Torts. Chicago, Callaghan, 1888.
- De Hert P. Belgium, Courts, Privacy and Data Protection: An inventory of Belgian case law from the pre-GDPR regime (1995—2015) // *Brussels Privacy HUB. Working Paper*. Vol. 5, 14, January 2019.
- De Hingh A. E. Some Reflections on Dignity as an Alternative legal Concept in Data Protection Regulation // *German Law Journal*. 2018. Vol. 19. No. 5.
- Fazekas Ch. P. 1984 Is Still Fiction: Electronic Monitoring in the Workplace and U. S. Privacy Law // *Duke Law and Technology Review*. 2004. No. 15.
- Gellert R., Gutwirth S. The Legal Construction of Privacy and Data Protection // *Computer Law and Security Review*. 2013. Vol. 29.
- Kesan J. P. Cyber-working or Cyber-shirking?: a First Principles Examination of Electronic Privacy in the Workplace // *Florida Law Review*. 2002. Vol. 54.
- Lasprogata G., King N., Pillay S. Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy Through a Comparative Study of Data Privacy Legislation in the E. U., U. S. and Canada // *Stanford Technology Law Review*. 2004. No. 4.
- Michael A. Smyth v. The Pillsbury Company, 914 F.Supp. 97. E. D. Pa. 1996.
- Pfisterer V. M. The Right to Privacy — A Fundamental Right in Search of Its Identity: Uncovering the CJ EU's Flawed Concept of the Right to Privacy // *German Law Journal*. 2019. Vol. 20. Iss. 5.
- Pollicino O., De Gregorio G. Privacy or Transparency? A New Balancing of Interests for the "Right to be Forgotten" of Personal Data Published in Public Registers // *The Italian Law Journal*. 2017. Vol. 3. No. 2.
- Price M. W. Rethinking Privacy: Fourth Amendment "Papers" and the Third-Party Doctrine // *Journal of National Security Law and Policy*. 2016. Vol. 8.
- Strömholm S. Right of Privacy and Rights of the Personality: A Comparative Survey. Stockholm, 1967.
- The Right to Respect for Private Life: Digital Challenges, a Comparative-Law Perspective. The United Kingdom // *EPRS: European Parliamentary Research Service*. October 2018.

- Thompson M. French constitutional court leaves GDPR bill largely intact // *Global Data Review*. 2018. 18 June.
- Vainio N., Miettinen S. Telecommunications Data Retention after Digital Rights Ireland: Legislative and Judicial Reactions in the Member States // *International Journal of Law and Information Technology*. 2015. Vol. 23. Iss. 3.
- Vanoni L. P. Balancing Privacy and National Security in the Global Digital Era: A Comparative Perspective of EU and US Constitutional Systems // *The Fragmented Landscape of Fundamental Rights Protection in Europe: the Role of Judicial and Non-judicial Actors* / ed. by L. Violini, A. Baraggia. Northampton, 2018.
- Warren S. D., Brandeis L. D. The Right to Privacy // *Harvard Law Review*. 1890. Vol. 4. No. 5.
- Whitman J. Q. The Two Western Cultures of Privacy: Dignity Versus Liberty // *Yale Law Journal*. 2004. Vol. 113. No. 6.
- Зорькин В. Д. Право в цифровом мире. Размышление на полях Петербургского международного юридического форума // *Российская газета*. 2018. 29 мая.
- Талапина Э. В. Право и цифровизация: новые вызовы и перспективы // *Журнал российского права*. 2018. № 2.
- Хабриева Т. Я., Черногор Н. Н. Право в условиях цифровой реальности // *Журнал российского права*. 2018. № 1.

REFERENCES

- Amsterdam A. G. Perspectives on the Fourth Amendment. *Minnesota Law Review*, 1974, vol. 58, 349 p.
- Bu-Pasha Sh. Cross-border issues under EU data protection law with regards to personal data protection. *Information and Communications Technology Law*, 2017, vol. 26, pp. 213—228.
- Cooley T. M. A Treatise on the Law of Torts. Chicago, Callaghan, 1888. 839 p.
- De Hert P. Belgium, Courts, Privacy and Data Protection: An inventory of Belgian case law from the pre-GDPR regime (1995—2015). *Brussels Privacy HUB: Working Paper*, 2019, vol. 5, no. 14, 34 p.
- De Hingh A. E. Some Reflections on Dignity as an Alternative legal Concept in Data Protection Regulation. *German Law Journal*, 2018, vol. 19, no. 5, pp. 1269—1290.
- Fazekas Ch. P. 1984 Is Still Fiction: Electronic Monitoring in the Workplace and U. S. Privacy Law. *Duke Law and Technology Review*, 2004, no. 15, pp. 1—16.
- Gellert R., Gutwirth S. The Legal Construction of Privacy and Data Protection. *Computer Law and Security Review*, 2013, vol. 29, pp. 1—16.
- Kesan J. P. Cyber-working or Cyber-shirking?: a First Principles Examination of Electronic Privacy in the Workplace. *Florida Law Review*, 2002, vol. 54, pp. 1—27.
- Khabrieva T. Y., Chernogor N. N. The Law in the Conditions of Digital Reality. *Zhurnal rossijskogo prava = Journal of Russian Law*, 2018, no. 1, pp. 85—102. (In Russ.)
- Lasprogata G., King N., Pillay S. Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy Through a Comparative Study of Data Privacy Legislation in the E. U., U. S. and Canada. *Stanford Technology Law Review*, 2004, no. 4, pp. 1—46.
- Michael A. Smyth v. The Pillsbury Company, 914 F.Supp. 97. E. D. Pa. 1996. Available at: <https://law.justia.com/cases/federal/district-courts/FSupp/914/97/2131293/>.
- Pfisterer V. M. The Right to Privacy — A Fundamental Right in Search of Its Identity: Uncovering the CJ EU's Flawed Concept of the Right to Privacy. *German Law Journal*, 2019, vol. 20, iss. 5, pp. 722—733.
- Pollicino O., De Gregorio G. Privacy or Transparency? A New Balancing of Interests for the “Right to be Forgotten” of Personal Data Published in Public Registers. *The Italian Law Journal*, 2017, vol. 3, no. 2, pp. 1—22.
- Price M. W. Rethinking Privacy: Fourth Amendment “Papers” and the Third — Party Doctrine. *Journal of National Security Law and Policy*, 2016, vol. 8.
- Strömholm S. Right of Privacy and Rights of the Personality: A Comparative Survey. Stockholm, 1967, pp. 247—299.
- Talapina E. V. Law and Digitalization: New Challenges and Prospects. *Zhurnal rossijskogo prava = Journal of Russian Law*, 2018, no. 2, pp. 5—17. (In Russ.)
- The Right to Respect for Private Life: Digital Challenges, a Comparative-Law Perspective — The United Kingdom. *EPRS: European Parliamentary Research Service*, 2018, October, pp. 1—35.
- Thompson M. French constitutional court leaves GDPR bill largely intact. *Global Data Review*, 2018, 18 June. Available at: <https://globaldatareview.com/>.
- Vainio N., Miettinen S. Telecommunications Data Retention after Digital Rights Ireland: Legislative and Judicial Reactions in the Member States. *International Journal of Law and Information Technology*, 2015, vol. 23, iss. 3, pp. 290—309.
- Vanoni L. P. Balancing Privacy and National Security in the Global Digital Era: A Comparative Perspective of EU and US Constitutional Systems. *The Fragmented Landscape of Fundamental Rights Protection in Europe: the Role of Judicial and Non-judicial Actors*. Ed. by L. Violini, A. Baraggia. Northampton, 2018. 256 p.
- Warren S. D., Brandeis L. D. The Right to Privacy. *Harvard Law Review*, 1890, vol. 4, no. 5, pp. 193—220.
- Whitman J. Q. The Two Western Cultures of Privacy: Dignity Versus Liberty. *Yale Law Journal*, 2004, vol. 113, no. 6, pp. 1—73.
- Zorkin V. D. Law in the digital world. Marginal thinking St. Petersburg International Law Forum. *Rossiyskaya gazeta*, 2018, May 29. (In Russ.)