
ЗАКОН
ИЗиСП
ИНСТИТУТ ЗАКОНОДАТЕЛЬСТВА И СРАВНИТЕЛЬНОГО ПРАВОВЕДЕНИЯ ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Институт законодательства и сравнительного правоведения
при Правительстве Российской Федерации

ЗАЩИТА ДАННЫХ
научно-практический комментарий к судебной практике

Ответственные редакторы
доктор юридических наук, профессор
В.В. Лазарев,
доктор юридических наук
Х.И. Гаджиев

Москва
ООО «ЮРИДИЧЕСКАЯ ФИРМА
КОНТРАКТ»
2020

УДК 342.7
ББК 67.400.32
340

Одобрено секцией публичного права ученого совета Института законодательства и сравнительного правоведения при Правительстве Российской Федерации

Рецензенты:

А.И. Щукин – старший научный сотрудник отдела международного частного права ИЗиСП, кандидат юридических наук;

С.В. Липень – профессор кафедры теории и истории государства и права МГЮА, доктор юридических наук, профессор.

340 **Защита данных: научно-практический комментарий к судебной практике** / В.В. Лазарев, Х.И. Гаджиев, Э.В. Алимов и др.; отв. ред. В.В. Лазарев, Х.И. Гаджиев; Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации. — М.: ООО «ЮРИДИЧЕСКАЯ ФИРМА КОНТРАКТ», 2020. — 176 с.

ISBN 978-5-6043246-6-0

Ценность информации растет в геометрической прогрессии, и хозяйствующие субъекты используют новые формы ее извлечения и обработки. При этом юридические методы охраны личных данных в разных правоотношениях подлежат постоянному пересмотру, а предстоящие годы видятся временем поиска компромисса между охраной частной жизни и обеспечением безопасности государства.

Настоящий научно-практический комментарий подготовлен с целью выявления тенденций развития судебной практики в сфере обработки информации, содержащей личные данные.

Рассматриваются вопросы: насколько согласие на обработку персональных данных должно быть информированным в части возможностей их обработки и сроков хранения; какие границы усмотрения должны соблюдать правоприменители при определении баланса частных и публичных интересов в случае доступа к персональным данным без соответствующего разрешения; каким образом должно быть выражено волеизъявление субъекта персональных данных о согласии на обработку персональных данных; как личная информация и персональные данные, содержащиеся в электронных документах, квалифицируются судами в качестве доказательств; какие рекомендации для законодателя вытекают из практики Конституционного Суда Российской Федерации прямо или косвенно, равно как и из практики других судов; каков зарубежный опыт рассмотрения судами дел о защите личных данных; какие тенденции порядка обработки персональных данных формируются в практике Европейского Суда по правам человека.

Для правоведов – ученых и практиков, представителей деловых кругов и интернет-сообщества, преподавателей, студентов и аспирантов юридических вузов и факультетов, а также для широкого круга читателей, заинтересованных в правомерном использовании своих личных данных.

УДК 342.7
ББК 67.400.32

© Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации, 2019

ISBN 978-5-6043246-6-0

The Institute of Legislation and Comparative Law
under the Government of the Russian Federation

DATA PROTECTION
Scientific and Practical Commentary on Judicial Practice

Executive editors
Doctor of Law, Professor
V.V. Lazarev,
Doctor of Law
Kh.I. Gajiev

Moscow
LAW FIRM CONTRAKT
2020

Approved by the Section of Public Law of the Scientific Council of the Institute of Legislation and Comparative Law under the Government of the Russian Federation

Reviewers:

A.I. Shchukin – Senior Researcher, Department of Private International Law, ILCL, Candidate of Law;

S.V. Lipen – Professor, Department of Theory and History of State and Law, Moscow State Law Academy, Doctor of Law, Professor.

Data protection: scientific and practical commentary on judicial practice / V.V. Lazarev, H.I. Gadzhiev, E.V. Alimov etc; ex. ed. V.V. Lazarev, Kh.I. Gajiev; The Institute of Legislation and Comparative Law under the Government of the Russian Federation. — M.: LAW FIRM CONTRACT, 2020. — 176 p.

ISBN 978-5-6043246-6-0

The value of information is growing exponentially and business entities are using new forms of its extraction and processing. The classical methods of personal data protection in various legal relations are the subject of constant review, which is why the nearest future probably will be the time of searching a compromise between protecting private life and ensuring the security of state.

This scientific and practical commentary is aimed on identifying trends in the processing of information containing personal data.

The following issues are considered: how much informed should be a consent to the processing of personal data regarding the possibilities of their processing and storage periods; what margins of discretion should law enforcement entities have to insure the balance between private and public interests in case of accessing to personal data without permission; how the expression of will of the subject of personal data to agree on processing of personal data should be expressed; how personal information and personal data contained in electronic documents is qualified by the courts as evidence; what recommendations for the legislator concerning personal data directly or indirectly follows from the practice of the Constitutional Court of the Russian Federation and from the practice of the other courts; what foreign experience of judicial practice on cases of protection of personal exists; what trends might be found in the practice of the European Court of Human Rights concerning processing of personal data.

For lawyers – scientists and practitioners, representatives of the business community and the Internet community, teachers, students and graduate students of law schools and faculties, as well as for a wide range of readers interested in the legitimate use of their personal data.

ISBN 978-5-6043246-6-0

© The Institute of Legislation and Comparative Law under the Government of the Russian Federation, 2019

АВТОРЫ И СОСТАВИТЕЛИ

Лазарев В.В. — главный научный сотрудник центра фундаментальных правовых исследований ИЗиСП, доктор юридических наук, профессор, заслуженный деятель науки РФ (введение);

Гаджиев Х.И. — заведующий отделом судебной практики и правоприменения ИЗиСП, доктор юридических наук (гл. 10, заключение);

Алимов Э.В. — старший научный сотрудник отдела конституционного права ИЗиСП, кандидат юридических наук (гл. 2);

Алимова Д.Р. — младший научный сотрудник отдела теории права и междисциплинарных исследований законодательства ИЗиСП (гл. 1);

Грачева С.А. — старший научный сотрудник отдела судебной практики и правоприменения ИЗиСП, кандидат юридических наук (гл. 6);

Долова М.О. — старший научный сотрудник отдела гражданского законодательства и процесса ИЗиСП, кандидат юридических наук (гл. 3);

Ибрагимова Ю.Э. — младший научный сотрудник отдела судебной практики и правоприменения ИЗиСП (гл. 5);

Сидоренко А.И. — ведущий научный сотрудник отдела судебной практики и правоприменения ИЗиСП, кандидат юридических наук (гл. 8);

Черемисинова М.Е. — заведующий центром научных изданий ИЗиСП (гл. 4);

Черенкова В.С. — младший научный сотрудник отдела обеспечения деятельности секретариата делегации Российской Федерации в Европейской комиссии за демократию через право (Венецианской комиссии) ИЗиСП (гл. 9);

Щербак С.С. — научный сотрудник отдела гражданского законодательства иностранных государств ИЗиСП (гл. 7).

AUTHORS

Lazarev V.V. — Chief Researcher of the Center for Fundamental Legal Researches of the ILCL, Doctor of Law, Professor, Honored Scientist of the Russian Federation (introduction);

Gadzhiev H.I. — Head of the Department of Judicial Practice and Law Enforcement of the ILCL, Doctor of Law (ch. 10, conclusion);

Alimov E.V. — Senior Researcher of the Department of Constitutional Law of the ILCL, Candidate of Legal Sciences (ch. 2);

Alimova D.R. — Junior Researcher of the Department of Theory of Law and Interdisciplinary Studies of Legislation of the ILCL (ch. 1);

Gracheva S.A. — Senior Researcher of the Department of Judicial Practice and Law Enforcement of the ILCL, Candidate of Legal Sciences (ch. 6);

Dolova M.O. — Senior Researcher of the Department of Civil Legislation and Process of the ILCL, Candidate of Legal Sciences (ch. 3);

Ibragimova Y.E. — Junior Researcher of the Department of Judicial Practice and Law Enforcement of the ILCL (ch. 5);

Sidorenko A.I. — Leading Researcher of the Department of Judicial Practice and Law Enforcement of the ILCL, Candidate of Legal Sciences (ch. 8);

Cheremisinova M.E. — Head of the Center for Scientific Publications of the ILCL (ch. 4);

Cherenkova V.S. — Junior Researcher of the Department for Support of the Secretariat of the Delegation of the Russian Federation in the European Commission for Democracy through Law (Venice Commission) of the ILCL (ch. 9);

Shcherbak S.S. — Scientific Researcher of the Department of Civil Legislation of Foreign States of the ILCL (ch. 7).

ОГЛАВЛЕНИЕ

CONTENT

ВВЕДЕНИЕ

Как предсказывается многими учеными, озабоченными глобальными проблемами современности, повсеместное внедрение цифровых технологий подразумевает преобладающее значение информации в общественных отношениях. Ценность информации растет в геометрической прогрессии, в связи с чем хозяйствующие субъекты изобретают все новые формы ее извлечения и обработки. В таких условиях классические методы охраны личных данных в самых разных правоотношениях подлежат постоянному пересмотру с учетом меняющихся реалий. Судебная практика является одним из инструментов выявления отклонения развития правоотношений от целей законодательного регулирования, провозглашенных в Конституции Российской Федерации. Допустимы утверждения, что с онтологической точки зрения формируется новая реальность — киберреальность, в рамках которой существует потребность в соответствующем правовом регулировании. В настоящее время цифровые права уже признаны объектами гражданских прав. При этом многими отмечается, что такие цифровые права по существу представляют собой средства фиксации гражданских прав. В связи с этим значение порядка обработки персональных данных в сети Интернет возрастает колоссально, поскольку достоверность средства фиксации обеспечивается именно привязкой к автору и адресату юридически значимого сообщения. Только благодаря надлежащему порядку обработки персональных данных в сети Интернет можно упорядочить правоотношения, возникающие, существующие и прекращающиеся в названной киберреальности.

Другой важный аспект, на котором следует заострить внимание, — это обеспечение публичного порядка, что является одной из первоочередных задач государства. Современные технологии предоставляют беспрецедентные возможности для заинтересованных государственных структур по сбору и обработке персональных данных граждан, что в перспективе имеет как огромный потенциал для повышения эффективности государственного управления, так и не меньший потенциал злоупотреблений в процессе использования таких данных не по назначению. Предстоящие годы, а может и десятилетия, видятся временем поиска компромисса между охраной частной жизни и обеспечением безопасности государства. Уже сейчас ответом на обозначенный вызов среди представителей гражданского общества является внедрение технологий шифрования, благодаря которым личная переписка, иные сведения будут храниться в системах распределенных реестров, доступ к ним будет только у специаль-

но уполномоченного лица. Названные технологии, характеризуемые в качестве панацеи в области противостояния государственному контролю, поднимают множество вопросов, ответы на которые также должны следовать из имеющегося, пускай пока незначительного, опыта судебного рассмотрения подобных дел. Формируемые сегодня судами подходы могут стать базой для приведения к единообразию судебной практики и апробирования планируемых способов законодательного регулирования.

Отдельно следует упомянуть право на свободу слова. Европейский суд по правам человека неоднократно обозначал ориентиры, в рамках которых средства массовой информации могут собирать и распространять открытые для всеобщего доступа данные: сбор и систематизация информации должны поднимать общественно значимые проблемы, а не удовлетворять любопытство. Однако с внедрением технологий обработки больших данных вполне возможно, что данный подход устареет, поскольку многие открытые данные смогут предоставляться в один клик.

Настоящий научно-практический комментарий подготовлен с целью отслеживания тенденций в сфере обработки информации, содержащей личные данные как по гражданским, так и по уголовным делам. Важными являются вопросы: насколько согласие на обработку персональных данных должно быть информированным в части возможностей их обработки и сроков хранения; какие границы усмотрения должны соблюдать правоприменители, в части определения баланса частных и публичных интересов в случае доступа к персональным данным без соответствующего разрешения; каким образом должно быть выражено волеизъявление субъекта персональных данных о согласии на обработку персональных данных, в том числе с учетом возможностей выражения его в электронной форме; как личная информация и персональные данные, содержащиеся в электронных документах, квалифицируются судами в качестве доказательств; какие рекомендации для законодателя вытекают из практики Конституционного Суда Российской Федерации прямо или косвенно, равно как и из практики других судов, которые может воспринять законодатель; каков зарубежный опыт рассмотрения судами дел о защите личных данных, в особенности, на территории Европейского Союза; какие тенденции порядка обработки персональных данных вытекают из практики Европейского суда по правам человека, в особенности по делам о слежке в порядке уголовного преследования за лицами, подозреваемыми или обвиняемыми в совершении преступления.

Ответы на перечисленные, а также на многие другие вопросы постарались дать авторы настоящего комментария, при этом делая акцент на потребности юридической практики.

Глава 1
СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ: ВОПРОСЫ СУДЕБНОЙ ПРАКТИКИ

Современное российское законодательство о защите персональных данных предусматривает, что для их обработки оператору необходимо получить соответствующее согласие от субъекта персональных данных. Одной из основных целей регулирования порядка дачи субъектом согласия на обработку персональных данных является устранение информационной асимметрии в отношениях между оператором и субъектом персональных данных и обеспечение автономии воли последнего[1]. Согласие субъекта персональных данных на их обработку является единственным законным основанием для любого вида обработки персональных данных. Все случаи обработки персональных данных при отсутствии согласия субъекта на их обработку можно отнести к специальным: речь идет либо о специальных целях обработки, либо о специальном субъекте на стороне оператора, либо об обоих указанных случаях в совокупности.

§ 1. Общие требования к согласию на обработку персональных данных

В статье 9 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее — Федеральный закон «О персональных данных», Закон № 152-ФЗ) к согласию на обработку персональных данных предъявляется ряд общих требований. Указанный закон содержит несколько условий принятия решения о предоставлении согласия на обработку персональных данных: такое решение принимается свободно, своей волей и в своем интересе. Кроме того, согласие должно отвечать следующим требованиям:

– быть точным, определенным и неабстрактным. Факт дачи согласия должен быть следствием действий субъекта персональных данных, а не вытекать из характера отношений между оператором их обработки и субъектом персональных данных. Молчание или

[1] См.: Савельев А.И. Научно-практический постатейный комментарий к Федеральному закону «О персональных данных». М., 2017. С. 71.

бездействие субъекта персональных данных, даже если такое поведение в соответствии с политикой конфиденциальности оператора будет признаваться согласием, не будет удовлетворять указанному требованию. Также и в случае использования интернет-ресурсов с применением настроек конфиденциальности по умолчанию при отсутствии их изменения пользователем согласие на обработку персональных данных не будет считаться данным в надлежащей форме;

– быть информированным, то есть осведомленным о последствиях дачи такого согласия. Это требование означает, что перед дачей согласия субъекту предоставляется вся необходимая и достоверная информация о целях обработки, обрабатываемых данных, операторе и иных лицах, которые будут осуществлять обработку его персональных данных, сроки обработки, иная значимая информация, касающаяся обработки персональных данных. При этом из материалов сложившейся судебной практики следует, что желательно также и разъяснить субъекту персональных данных значение используемых терминов для полного соответствия согласия требованиям закона, поскольку без такого разъяснения информированность данного согласия может быть оспорена. Так, в постановлении Арбитражного суда Северо-Западного округа от 18 июля 2016 г. по делу № А44-9647/2015 указано: «Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным и предполагает, как минимум, письменное разъяснение субъекту персональных данных значения понятия «обработка персональных данных»;

– быть сознательным. Такое условие к даче согласия предполагает осмысленное принятие решения. Вынужденный характер дачи согласия ставит под сомнение его соответствие требованиям закона.

Статья 9 Закона № 152-ФЗ также содержит требования к форме согласия на обработку персональных данных: оно может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено Федеральным законом. При этом помимо собственноручной подписи субъекта персональных данных на бумажном носителе признается и согласие в форме электронного документа, подписанного в соответствии с Федеральным законом электронной подписью. Таким образом, закон предусматривает широкую вариативность в вопросе оформления такого согласия.

В настоящее время согласие на обработку персональных данных может быть дано в различных формах.

§ 2. Согласие на обработку персональных данных в виде письменного документа с собственноручной подписью субъекта персональных данных

Получение согласия на обработку персональных данных в письменной форме является обязательным в следующих случаях, прямо предусмотренных Законом № 152-ФЗ:

– если в целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных (ст. 8);

– если речь идет об обработке специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни (ст. 10);

– если речь идет о сведениях, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных (ст. 11);

– если в процессе обработки предполагается трансграничная передача персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных. При этом, если речь идет о защите жизни, здоровья, иных жизненно важных интересов субъекта персональных данных или других лиц, а получение согласия в письменной форме субъекта персональных данных невозможно, то такая передача может быть осуществлена (ст. 12);

– если решение, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных (ст. 16).

В остальных случаях соблюдение письменной формы не является обязательным.

В Законе № 152-ФЗ предусмотрен также конкретный перечень сведений, которые должны содержаться в согласии в письменной форме:

1) фамилия, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

2) фамилия, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

3) наименование или фамилия, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;

4) цель обработки персональных данных;

5) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

6) наименование или фамилия, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;

7) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

8) срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;

9) подпись субъекта персональных данных.

Следует отметить, что письменная форма такого согласия всегда предполагает составление отдельного документа, а не включение положения о согласии на обработку персональных данных в качестве пункта в какой-либо договор. Так, в решении по делу № А65-33540/2017 суд указывает, что включение пункта о согласии субъекта на обработку персональных данных в договор не отвечает требованиям конкретности, информированности и сознательности. Подписывая заранее разработанный текст договора, оформленный мелким шрифтом и содержащий специфические, используемые в целях Закона № 152-ФЗ и не используемые в обиходе понятия и термины, такие как «обработка персональных данных», «трансграничная передача», субъект вряд ли был достаточно информирован об истинном смысле этих понятий и терминов, а также о возможных последствиях своего согласия на обработку своих персональных данных. Суд делает вывод, что данное в договоре страхования согласие на обработку персональных данных нельзя признать в качестве надлежащего согласия в целях Закона № 152-ФЗ, поскольку такое согласие не отвечает требованиям о письменном согласии, изложенным в п. 4 ст. 9 Закона № 152-ФЗ.

Требование Закона № 152-ФЗ в части того, что согласие на обработку персональных данных должно быть конкретным, информированным и сознательным, предполагает как минимум письменное разъяснение субъекту персональных данных значения понятия «обработка персональных данных», которое включает в себя любое действие (операцию) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных. Однако ни договор страхования, ни любой другой документ не содержат никаких сведений о разъяснении страхователю как субъекту персональных данных указанного понятия. Кроме того, из смысла ст. 9 Закона № 152-ФЗ следует, что субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку не просто путем подписания договора с условием о согласии, а согласие должно быть выражено свободно, своей волей и в своем интересе отдельно.

Как указано выше, среди требований законодательства к согласию на обработку персональных данных есть положение об обязательном указании срока, в течение которого действует согласие субъекта персональных данных. При этом следует отметить, что в согласии на обработку персональных данных может быть установлен и неопределенный срок его действия до отзыва со стороны субъекта персональных данных в письменной форме, и такое установление считается соответствующим требованиям закона. Так, в решении Суда апелляционной инстанции по делу № А42-342/2017 указано, что законодательная норма не предусматривает указания в согласии конкретного срока, в течение которого оно действует, предельный срок действия такого согласия также не установлен законодателем. В рассматриваемом случае срок действия согласия определен началом его действия (со дня подписания) и заканчивается моментом востребования — письменным отзывом в произвольной форме. Таким образом, срок действия согласия субъекта персональных данных на их обработку в любом случае ограничен действием самого субъекта персональных данных по представлению письменного отзыва ранее данного им согласия, в связи с чем указанный срок можно квалифицировать как срок, определяющий момент востребования. Указанное не противоречит общим правилам определения сроков, установленных по аналогии закона гражданским законодательством (ст. 190 ГК РФ).

Более того, суд указывает, что указание точного срока действия согласия субъекта персональных данных на их обработку в привязке к конкретному временному периоду или календарной дате в данном случае невозможно, поскольку предприятие как оператор персональных данных не в состоянии заранее с достоверностью определить временной промежуток, до какой календарной даты конкретный пользователь услуг плавательного бассейна будет фактически посещать бассейн и в какую дату пользователь таких услуг может прекратить таковое посещение по собственной инициативе. Между тем действием самого субъекта персональных данных по представлению письменного отзыва ранее данного им согласия его права не нарушаются. В решении по делу № А42-342/2017 суд заключает, что в части получения согласия на обработку персональных данных в отношении срока такого согласия нарушений предприятием не допущено. В рамках указанного дела также был рассмотрен вопрос об обработке биометрических персональных данных (фотографии) без письменного согласия субъекта персональных данных. В данном случае пропуск с фотографией, характеризующей физиологические и биологические особенности человека (относящейся к биометрическим персональным данным), позволяет установить, принадлежит ли данному лицу предъявляемый пропуск, на основе которых можно установить его личность путем сравнения фото с лицом предъявителя пропуска и указываемых владельцем пропуска фамилии, имени и отчества. Суд указывает, что эти данные используются оператором для установления личности субъекта персональных данных в случае сомнения в том, что пропуск предъявляется его действительным владельцем, а потому он используется оператором для установления личности субъекта персональных данных, и данная обработка должна осуществляться в строгом соответствии со ст. 11 Закона № 152-ФЗ. Суд пришел к выводу о том, что фотографические изображения, содержащиеся на документе «пропуск», являются биометрическими персональными данными, поскольку характеризуют физиологические и биологические особенности человека. Обработка указанных данных должна осуществляться с соблюдением требований п. 1 ст. 11 Закона № 152-ФЗ, а именно при наличии согласия субъекта персональных данных. Суд апелляционной инстанции установил, что в соответствии с положением о порядке посещения плавательного бассейна для различных категорий населения в рамках государственной программы Мурманской области «Развитие физической культуры и спорта» на 2014–2020 годы, утвержденным председателем Комитета по физической культуре и спорту Мурманской области 26 апреля 2016 г., посе-

тителями предоставлялись предприятию фотографии, которые размещались заявителем на документе «пропуск» для последующего использования в целях установления их личности. Указанные действия предприятия (сбор, оформление (размещение), использование фотографий) подпадают под понятие обработки персональных данных с позиции ч. 3 ст. 3 Закона № 152-ФЗ. Между тем согласия указанных лиц на обработку их биометрических персональных данных (фотографий) в нарушении требования ч. 1 ст. 11 Закона № 152-ФЗ предприятием не получено. При таком положении суд признал, что в данном случае использование фотографий для пропуска является обработкой биометрических персональных данных в смысле Закона № 152-ФЗ и поэтому предприятием были допущены нарушения[1].

§ 3. Согласие на обработку персональных данных в конклюдентной форме

Такая форма дачи согласия предполагает, что оно вытекает из действий субъекта. Например, факт заполнения и предоставления резюме был признан судом в качестве согласия субъекта персональных данных, отвечающих требованиям закона[2].

Таганский районный суд в решении от 1 апреля 2015 г. по делу № 2-1464/2015 признал правомерным привлечение к дисциплинарной ответственности сотрудника, в трудовые обязанности которого входила работа с персональными данными, за распространение анкет соискателей без их согласия путем направления с корпоративной почты на адреса третьих лиц, не являющихся работниками организации. Данный факт был обнаружен службой безопасности компании. Выяснилось, что резюме кандидатов были направлены в качестве примера без согласия соискателей и иных законных оснований, что стало нарушением не только локальных нормативных актов организации, но и Федерального закона «О персональных данных»[3].

§ 4. Согласие на обработку персональных данных в форме электронного документа, подписанного простой электронной подписью

В соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» (далее — Федеральный закон

---

1 Там же.

2 См.: Апелляционное определение Московского городского суда от 28 сентября 2016 г. по делу № 33-38280/2016.

3 См.: решение Таганского районного суда от 1 апреля 2015 г. по делу № 2-1464/2015.

«Об электронной подписи»простая электронная подпись — это электронная подпись, которая создается посредством использования кодов, паролей или иных средств и подтверждает факт формирования электронной подписи определенным лицом. Суды признают документ, в котором было выражено согласие в подобной форме, в качестве подписанного простой электронной подписью. Следует отметить, что для обеспечения документа, подписанного простой электронной подписью, юридической силой необходимо идентифицировать лицо, которое использует простую электронную подпись. По общему правилу идентификация лица происходит, когда субъект лично посещает организацию, выдающую ключи электронной подписи. Подписант предъявляет документ, удостоверяющий личность, и получает ключ электронной подписи.

При этом ключ простой электронной подписи может генерироваться и онлайн с использованием различных кодов подтверждения по электронной почте, SMS-кодов и др. Такая форма не предполагает очной идентификации лица с предоставлением документа, удостоверяющего личность. Однако механизм с генерированием ключей простых электронных подписей онлайн широко применяется в сфере онлайн-банкинга для физических лиц, где идентификация подписанта осуществляется в момент выдачи дебетовой или кредитной карты, к которой услуга онлайн-банкинга привязана. Также получение согласия на обработку персональных данных в форме электронного документа, подписанного простой электронной подписью, распространено в области государственных услуг для физических лиц и в сфере коммунального хозяйства.

Так, в определении Приморского краевого суда от 7 апреля 2015 г. по делу № 33-2865 указано: «Согласно оферте СМС-код используется в качестве электронной подписи клиента для формирования им каждого электронного документа. В случае идентичности СМС-кода, направленного банком, и СМС-кода, введенного в форме электронного документа для подтверждения передачи клиентом соответствующего распоряжении/заявления через интернет-банк, такая электронная подпись считается подлинной и предоставленной клиентом»[1].

Также в качестве подписанного простой электронной подписью признается согласие, подписанное с помощью кода подтверждения, высланного по электронной почте.

При этом важно соблюсти положения ст. 6 Федерального закона «Об электронной подписи», в частности, чтобы стороны (оператор и субъект) достигли соглашения о том, что направление сообщения

[1] Определение Приморского краевого суда от 7 апреля 2015 г. по делу № 33-2865.

с определенного электронного адреса будет считаться подписанием документа простой электронной подписью. Юридическая сила сообщений электронной почты подтверждается и судебной практикой. Так, в постановлении Президиума ВАС РФ от 12 ноября 2013 г. № 18002/12 указано, что «получение или отправка сообщения с использованием адреса электронной почты, известного как почта самого лица или служебная почта его компетентного сотрудника, свидетельствует о совершении этих действий самим лицом, пока им не доказано обратное».

§ 5. Согласие на обработку персональных данных без использования электронной подписи

Электронная форма дачи согласия на обработку персональных данных может быть также выражена путем проставления так называемой галочки под условиями обработки персональных данных, например в соответствующем поле на экране при оформлении заказа или регистрации на веб-сайте.

При определенных обстоятельствах такого рода согласие также может рассматриваться в качестве электронного документа, подписанного простой электронной подписью.

При регистрации на интернет-сайтах пользователь принимает условия пользования указанным интернет-сайтом (пользовательское соглашение) и тем самым берет на себя обязательства, установленные указанным соглашением, а также всеми дополнительными правилами (правила верификации), являющимися неотъемлемой частью пользовательского соглашения.

Пользователь конкретного ресурса в момент регистрации самостоятельно принимает решение о предоставлении собственных персональных данных и дает согласие на их обработку, отвечающее требованиям закона, — конкретное, информированное и сознательное. В случае если пользователь не согласен с какими-либо положениями пользовательского соглашения конкретного интернет-ресурса, он может отказаться от его использования.

В пользовательских соглашениях нередко указано, что пользователь понимает и согласен с тем, что правообладатель может использовать информацию, предоставленную пользователем, в том числе и персональные данные. Например, при регистрации в качестве участника конкурса субъект персональных данных принимает условия правил проведения конкурса, размещенных на сайте, и тем самым берет на себя обязательства, установленные указанными правилами. При этом факт участия в конкурсе означает конкретное, информи-

рованное и сознательное согласие участника на обработку организатором конкурса предоставленных участником персональных данных, в том числе фамилии, имени, отчества, номера телефона, а также почтового адреса.

§ 6. Отзыв согласия на обработку персональных данных

Часть 2 ст. 9 Закона № 152-ФЗ предусматривает возможность субъекта отозвать ранее данное согласие на обработку персональных данных. Правовым последствием отзыва является утрата права оператора на обработку персональных данных этого субъекта, за исключением случаев, когда оператор имеет иные предусмотренные Законом № 152-ФЗ основания для обработки таких данных (п. 2–11 ч. 1 ст. 6, ч. 2 ст. 10, ч. 2 ст. 11).

Следует отметить, что бремя доказывания наличия таких оснований возлагается на самого оператора. Так, например, А.И. Савельев указывает, что в случае заключения кредитного договора у банковской организации возникает сразу несколько оснований обработки персональных данных: 1) согласие субъекта персональных данных; 2) цели исполнения договора, стороной которого является субъект персональных данных (п. 5 ч. 1 ст. 6 Закона № 152-ФЗ); 3) выполнение возложенных законодательством на оператора обязанностей (например, сохранять идентифицирующие клиента документы в течение не менее пяти лет[1]); хранение первичных учетных документов, регистров бухгалтерского учета и бухгалтерской отчетности в течение сроков, устанавливаемых в соответствии с правилами организации государственного архивного дела, но не менее пяти лет (ч. 1 ст. 17 Федерального закона от 21 ноября 1996 г. № 129-ФЗ «О бухгалтерском учете», причем все хозяйственные операции, проводимые организацией, должны оформляться оправдательными документами)[2]. Из указанного выше следует, что даже после надлежащего исполнения кредитного договора его сторонами у банковской организации возникают обязательства перед государством, связанные с персональными данными заемщика, и поэтому даже в случае отзыва согласия на обработку персональных данных обязанности по немедленному прекращению обработки и уничтожению персональных данных не возникает.

---

1 См.: ч. 4 ст. 7 Федерального закона от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

2 См.: Савельев А.И. Указ. соч. С. 76.

Обработка персональных данных без согласия субъекта персональных данных допускается в случае, если она осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, законодательством Российской Федерации о пенсиях по государственному пенсионному обеспечению, о трудовых пенсиях. Поэтому отзыв работником своего согласия на обработку персональных данных в таких случаях также не может являться основанием для прекращения обработки его персональных данных работодателем.

Согласно ч. 5 ст. 21 Закона № 152-ФЗ в случае отзыва субъектом персональных данных согласия на обработку его персональных данных оператор обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий 30 дней с даты поступления отзыва, если иное не предусмотрено законодательством о персональных данных. Следует подчеркнуть, что нормами Закона № 152-ФЗ не предусмотрена обязанность оператора уведомлять субъекта персональных данных о факте прекращения обработки персональных данных в связи с удовлетворением отзыва согласия субъекта на обработку его персональных данных.

Нередко возникают ситуации, когда субъект персональных данных вынужден дать согласие на их обработку, поскольку оператор обусловил предоставление товара или оказание услуги дачей согласия на обработку персональных данных любыми способами, явно несоразмерными целям дачи согласия со стороны субъекта персональных данных. Такое согласие предусматривает обработку персональных данных с указанием целей, способов, сроков и иных параметров обработки, которые явно избыточны по отношению к тем целям, ради которых субъект персональных данных обратился к оператору. При этом в случае отказа от подписания такой формы согласия обычно оператор отказывается в свою очередь заключить договор. Такая ситуация фактически лишает субъекта персональных данных возможности выбора и противоречит действующему законодательству не только о защите персональных данных, но и о защите прав потребителей. Так, в соответствии с ч. 2 ст. 16 Закона РФ от 7 февраля 1992 г. № 2300-1 «О защите прав потребителей» (далее — Закон «О защите прав потребителей») запрещается обусловливать приобретение одних

товаров (работ, услуг) обязательным приобретением других товаров (работ, услуг). Следует подчеркнуть, что это положение ст. 16 данного закона, посвященной недействительности условий договора, ущемляющих права потребителя. Очевидно, что в тех ситуациях, когда субъект персональных данных, выступая в качестве потребителя, вынужден дать под угрозой незаключения договора согласие с условиями обработки персональных данных, заранее сформулированными предпринимателем и содержащими явно избыточные положения и требования, можно говорить об ущемлении прав потребителя субъекта персональных данных и о нарушении не только законодательства о персональных данных, но и законодательства о защите прав потребителей. Данный вывод подтверждается и судебной практикой. Так, в постановлении Арбитражного суда Северо-Западного округа от 18 июля 2016 г. по делу № А44-9647/2015[1] указано, что отсутствие у потребителя права выбора возможности согласия или отказа в согласии на обработку персональных данных ущемляет права потребителей. Поскольку потребитель является экономически более слабой стороной, предоставление ему полной и достоверной информации, необходимой для принятия самостоятельного решения, является важным условием, обеспечивающим соблюдение его прав.

Федеральный арбитражный суд Московского округа в постановлении от 19 августа 2011 г. по делу № А40-129864/10-21-809 указывает, что нарушением законодательства о персональных данных является отсутствие указания в заявлении о согласии на обработку персональных данных перечня действий с персональными данными, а также указание неверного срока хранения персональных данных.

§ 7. Дача согласия на обработку персональных данных представителем субъекта персональных данных

Закон № 152-ФЗ также предусматривает возможность дачи согласия в случае недееспособности субъекта персональных данных законным представителем субъекта. Представительство в данном случае может быть законным (например, если речь идет о несовершеннолетнем ребенке, то его законными представителями являются его родители; законным представителем лица, лишенного дееспособности, выступает его опекун и др.). Документами, подтверждающими законность представительства, могут являться свидетельство о рождении, акт о назначении опекуном, а в случае добровольного пред-

[1] СПС «КонсультантПлюс».

ставительства — надлежащим образом оформленная доверенность. Важно иметь в виду, что в действующем законодательстве нет требований об обязательном нотариальном заверении доверенности на право совершения действий с персональными данными представляемого лица.

Порядок получения согласия субъекта персональных данных на их обработку в целях предоставления государственных и муниципальных услуг в форме электронного документа устанавливается Правительством РФ. Так, постановлением Правительства РФ от 25 января 2013 г. № 33 утверждены Правила использования простой электронной подписи при оказании государственных и муниципальных услуг[1]. Данные правила устанавливают порядок использования простой электронной подписи любыми лицами при обращении за получением государственных и муниципальных услуг в электронной форме, оказываемых федеральными органами исполнительной власти, государственными корпорациями, которые в соответствии с федеральным законом наделены полномочиями по предоставлению государственных услуг в установленной сфере деятельности, органами государственных внебюджетных фондов, органами исполнительной власти субъектов Российской Федерации, органами местного самоуправления, а также за получением услуг, перечень которых устанавливается Правительством РФ и которые предоставляются государственными и муниципальными учреждениями и другими организациями, которым дается государственное или муниципальное задание на предоставление таких услуг.

В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни. К форме и содержанию такого согласия применяются общие правила, установленные для согласия субъекта персональных данных.

Часть 8 ст. 9 Федерального закона «О защите персональных данных» содержит положение, согласно которому оператор может получить персональные данные не от самого субъекта, а от третьего лица. Однако при этом оператор обязан убедиться, что персональные данные были получены и предоставлены оператору таким третьим лицом на законном основании (п. 2–11 ч. 1 ст. 6, ч. 2 ст. 10, и ч. 2 ст. 11).

---

[1] Постановление Правительства РФ от 25 января 2013 г. № 33 (в ред. от 20 ноября 2018 г.) «Об использовании простой электронной подписи при оказании государственных и муниципальных услуг» // СЗ РФ. 2013. № 5. Ст. 377.

Глава 2
ПРАВОВЫЕ ПОЗИЦИИ КОНСТИТУЦИОННОГО СУДА РОССИЙСКОЙ ФЕДЕРАЦИИ О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

В соответствии с п. «в», «и» ч. 1 ст. 71 Конституции РФ регулирование и защита прав и свобод человека и гражданина, информация и связь отнесены к ведению Российской Федерации. Субъекты Российской Федерации не могут принимать нормативные правовые акты в указанной сфере. Поэтому, как справедливо указывает Конституционный Суд РФ (далее — КС РФ) в своей правовой позиции, обязанность обеспечить — с учетом современного уровня развития средств и способов обращения такого специфического нематериального объекта, как информация — баланс прав и законных интересов, а также определенность правового положения участников правоотношений, объектом которых она выступает, и правоотношений, связанных с ее поиском, получением, передачей, производством и распространением, возлагается на федерального законодателя (постановление от 26 октября 2017 г. № 25-П).

Несмотря на сформированную практику по вопросам защиты персональных данных, КС РФ не принял ни одного постановления, предметом которого были бы нормы Закона № 152-ФЗ. При этом КС РФ принял множество определений и постановлений, касающихся иных федеральных законов, затрагивающих отдельные аспекты защиты персональных данных.

§ 1. Защита персональных данных граждан при обращении в медицинские учреждения

Интерес представляют несколько наиболее актуальных вопросов: обработка сведений о пациенте и возможность их передачи другим лицам без его согласия; допустимость аудио- и видеозаписи в кабинетах учреждений здравоохранения.

В пункте 4 ч. 2 Закона № 152-ФЗ закреплено, что обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и ме-

дико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну. КС РФ отметил, что данная норма позволяет хранить информацию о состоянии здоровья граждан исключительно в целях реализации их права на охрану здоровья и медицинскую помощь, при этом конфиденциальность персональных данных обеспечивается врачебной тайной, а потому не может рассматриваться как нарушение конституционных прав заявителями в указанном им аспекте (определение от 16 июля 2013 г. № 1176-О)[1]

КС РФ также отмечал, что положения Закона об охране здоровья граждан, допускающие использование локальных информационных систем, направлены на обеспечение прав граждан на получение медицинской помощи необходимого объема и надлежащего качества на основе установленных стандартов ее оказания и сами по себе не могут рассматриваться как нарушающие конституционные права граждан в указанном заявителем аспекте (определение от 24 сентября 2013 г. № 1333-О). При этом в любом случае пациент или работник медицинского учреждения должен предоставить письменное согласие на обработку персональных данных подобным способом. В частности, предоставление данных сведений без согласия гражданина допускается указанным федеральным законом для осуществления контроля качества и безопасности медицинской деятельности, в том числе в целях внутреннего контроля.

Несмотря на небольшое количество решений КС РФ по отмеченным вопросам, можно отметить, что в Законе № 152-ФЗ сформулированы общие положения, гарантирующие соблюдение врачебной и

---

[1] Согласно ч. 4 ст. 13 Федерального закона от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» (далее — Закон об охране здоровья граждан) предоставление сведений, составляющих врачебную тайну, без согласия гражданина или его законного представителя допускается в 11 случаях (в целях проведения медицинского обследования и лечения гражданина, который в результате своего состояния не способен выразить свою волю; при угрозе распространения инфекционных заболеваний, массовых отравлений и поражений; по запросу органов дознания и следствия, суда в связи с проведением расследования или судебным разбирательством, по запросу органов прокуратуры в связи с осуществлением ими прокурорского надзора, по запросу органа уголовно-исполнительной системы в связи с исполнением уголовного наказания и осуществлением контроля за поведением условно осужденного, осужденного, в отношении которого отбывание наказания отсрочено, и лица, освобожденного условно-досрочно, и др.).

иной охраняемой законом тайны и защиту персональной информации учреждениями, осуществляющими сбор и хранение такой информации, а в Законе об охране здоровья граждан закреплены основания предоставления сведений, составляющих врачебную тайну, без согласия гражданина или его законного представителя, которые в полной мере отвечают целям защиты прав и законных интересов граждан, соблюдения баланса частных и публичных интересов (постановления от 20 декабря 2011 г. № 29-П, от 22 июня 2017 г. № 16-П, от 17 апреля 2019 г. № 18-П и др.).

§ 2. Оперативно-розыскная деятельность

В данном случае наибольший интерес представляет практика КС РФ по вопросу допустимости сбора информации о гражданах без их согласия в рамках оперативно-разыскных действий с помощью технических средств. Так, в своей жалобе в КС РФ гражданин, привлеченный к уголовной ответственности за совершение преступления, предусмотренного ч. 4 ст. 290 УК РФ, оспаривал конституционность ч. 2–5 ст. 8 Федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» (далее — Федеральный закон № 144-ФЗ), позволивших проводить наблюдение с использованием технических средств, в результате которого получены аудио- и видеозаписи переговоров (разговоров) граждан в служебных помещениях, без судебного решения. По мнению заявителя, оспариваемые нормы в системной связи с положениями ст. 9, 11 Федерального закона № 144-ФЗ, а также ст. 13, 29, 186 УПК РФ допускают произвольное вторжение в частную жизнь и сбор информации без согласия и уведомления лица, что нарушило гарантированное ст. 23 Конституции РФ право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений.

КС РФ отметил, что поскольку осуществление оперативно-разыскных мероприятий, в том числе наблюдения, возможно лишь в целях выполнения задач, предусмотренных ст. 2 Федерального закона № 144-ФЗ, и при наличии оснований, указанных в ст. 7, то данный федеральный закон не допускает сбора, хранения, использования и распространения информации о частной жизни проверяемого лица, если это не связано с выявлением, предупреждением, пресечением и раскрытием преступлений, а также с выявлением и установлением лиц, их подготавливающих, совершающих или совершивших, и другими законными задачами и основаниями оперативно-разыскной деятельности (определение от 14 июля 1998 г. № 86-О).

КС РФ в своих решениях неоднократно указывал на то, что применение технических средств фиксации наблюдаемых событий само по себе не предопределяет необходимость вынесения о том специального судебного решения, которое признается обязательным условием для проведения отдельных оперативно-разыскных мероприятий, ограничивающих конституционные права человека и гражданина (определения от 16 ноября 2006 г. № 454-О, от 20 марта 2007 г. № 178-О-О, от 21 октября 2008 г. № 862-О-О, от 13 октября 2009 г. № 1148-О-О и др.), а потому положения Федерального закона № 144-ФЗ, допускающие проведение наблюдения с использованием средств аудио- и видеозаписи, как сами по себе, так и в системной связи с указанными в жалобе законоположениями не могут рассматриваться как ограничивающие права заявителя. К тому же согласно ст. 5 Федерального закона № 144-ФЗ органы, осуществляющие оперативно-разыскную деятельность, при проведении оперативно-разыскных мероприятий обязаны обеспечивать соблюдение прав человека и гражданина на неприкосновенность частной жизни, личную и семейную тайну, неприкосновенность жилища и тайну корреспонденции и им запрещено разглашать сведения, которые затрагивают неприкосновенность частной жизни, личную и семейную тайну, честь и доброе имя граждан и которые стали им известны в процессе проведения оперативно-разыскных мероприятий, без согласия граждан, за исключением случаев, предусмотренных федеральными законами.

§ 3. Личные данные участников административного разбирательства

Согласно позиции КС РФ право на неприкосновенность частной жизни, личную и семейную тайну означает предоставленную человеку и гарантированную государством возможность контролировать информацию о самом себе, препятствовать разглашению сведений личного, интимного характера; в понятие «частная жизнь» включается та область жизнедеятельности человека, которая относится к отдельному лицу, касается только его и не подлежит контролю со стороны общества и государства, если не носит противоправного характера (определения от 24 декабря 2013 г. № 2128-О, от 9 июня 2005 г. № 248-О, от 26 января 2010 г. № 158-О-О и др.).

В постановлении от 18 февраля 2000 г. № 3-П КС РФ отметил, что права, закрепленные в ст. 23, 24,и 29 Конституции РФ, обосновывают и обеспечивают в том числе возможность для гражданина требовать предоставления ему собираемых органами государственной

власти и их должностными лицами сведений, непосредственно затрагивающих его права и свободы, и тем более касающихся его частной жизни, чести и достоинства. Основания для ограничения указанных прав могут устанавливаться законом только в качестве исключения из общего дозволения (ч. 2 ст. 24 Конституции РФ) и должны быть связаны именно с содержанием информации, поскольку иначе они не были бы адекватны конституционно признаваемым целям. Из ряда решений КС РФ можно установить, в каких случаях обработка персональных данных признается соответствующей охраняемым Конституцией РФ гарантиям.

В отношении вопроса об отнесении информации о личных данных заявителя и свидетеля в рамках административного процесса к категории тайны частной жизни КС РФ указал, что «личные данные (имя, адрес места жительства, почтовый адрес, контактный телефон) лица, заявляющего о правонарушении, указываемые им в официально подаваемом заявлении, а равно личные данные свидетеля, которые фиксируются в процессуальных документах, в том числе с их слов (например, в протоколе об административном правонарушении), не относятся к сведениям о частной жизни таких лиц и не признаются законодательством об административных правонарушениях закрытыми сведениями, поскольку такие данные необходимы для производства по делу об административном правонарушении» (определения от 16 июля 2013 г. № 1217-О, от 23 апреля 2015 г. № 1075-О).

Данные выводы КС РФ были сформулированы применительно к действующему правовому регулированию производства по делам об административных правонарушениях и не носят универсального характера (определение от 22 декабря 2015 г. № 2906-О). В частности, КС РФ в названных решениях указал, что законодатель вправе определить случаи, когда личным данным лица, заявляющего об административном правонарушении, указываемым им в официально подаваемом заявлении, придавался бы закрытый характер.

В отмеченных определениях КС РФ также подчеркнул, что несмотря на отсутствие соответствующих положений в действующем правовом регулировании не может рассматриваться как нарушение конституционных прав и свобод, в том числе права на государственную защиту, отмеченная выше ситуация, поскольку лицо, заявляющее об административном правонарушении, и свидетель в рамках существующего правового регулирования не лишены возможности обратиться в правоохранительные органы в связи со всеми случаями противоправного, по их мнению, вмешательства в их частную жизнь и посягательства на их безопасность.

§ 4. Удаление персональных данных гражданина по его требованию

Статья 7 Закона № 152-ФЗ в качестве общего правила закрепляет конфиденциальность персональных данных, которая предполагает, что операторы и иные лица, получившие доступ к персональным данным, то есть к любой информации, относящейся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных), обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом (определение от 22 декабря 2015 г. № 2906-О).

В ряде случаев гражданин не может требовать исключения персональных данных о нем, поскольку они приобретают общедоступный и открытый характер. Этим руководствовался КС РФ, отклоняя жалобу индивидуального предпринимателя, который направлял в соответствующие государственные органы заявления об исключении своих персональных данных (имени, фамилии, отчества, даты рождения) из открытых и общедоступных сведений, содержащихся в выписке из Единого государственного реестра индивидуальных предпринимателей и на официальном сайте Федеральной налоговой службы (определение от 17 июля 2012 г. № 1346-О).

Остается актуальной проблема хранения данных о судимостях, фактах привлечения к уголовной и административной ответственности в связи с реализацией гражданами избирательных прав, а также в области доступа к некоторым видам деятельности (правоохранительная, педагогическая, охотничья и т.д.). Это вызвало многочисленные обращения граждан по поводу удаления данных о себе из баз данных соответствующих правоохранительных органов.

В данном случае примечательны определения КС РФ от 27 февраля 2018 г. № 558-О, от 24 апреля 2018 г. № 1099-О в связи с жалобами граждан, которые оспаривают конституционность ряда положений ст. 17 Федерального закона от 7 февраля 2011 г. № 3-ФЗ «О полиции» и ч. 3, 4 ст. 10 Закона № 152-ФЗ, определяющих особенности обработки специальных категорий персональных данных, в частности о судимости. Заявители полагают, что хранение данных о погашенной судимости нарушает их конституционные права, а оспариваемые законоположения допускают не ограниченные по срокам хранение и обработку полицией данных о лице, осужденном за совершение преступления, вне зависимости от погашения либо снятия судимости, а также без учета декриминализации совершенного деяния и не предусматривают механизма уничтожения этих данных по

достижении целей обработки, тем самым не позволяя указанному лицу по прошествии определенного времени с момента погашения (снятия) судимости ограничить и контролировать разглашение этих данных в целях реализации и защиты своих прав и свобод, поскольку доступ иных лиц к указанным данным затрудняет реализацию ими прав и свобод.

КС РФ в таких делах отклоняет жалобы заявителей, обосновывая это особым правовым положением полиции и предназначением данного органа государственной власти, которое состоит в защите жизни, здоровья, прав и свобод граждан Российской Федерации, иностранных граждан, лиц без гражданства, противодействии преступности, охране общественного порядка, собственности и обеспечении общественной безопасности. КС РФ также отметил то, что формирование и ведение банков данных о гражданах осуществляются в соответствии с требованиями, установленными российским законодательством, а содержащиеся в них персональные данные обрабатываются в соответствии с установленными законодательством Российской Федерации требованиями в области персональных данных и подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в достижении этих целей, то есть во всяком случае не могут храниться бессрочно.

В определении от 25 февраля 2016 г. № 335-О КС РФ указал, что Федеральный закон от 7 февраля 2011 г. № 3-ФЗ «О полиции» наделяет полицию правом обрабатывать информацию обо всех лицах, подвергающихся или подвергавшихся уголовному преследованию для исполнения возложенных на нее обязанностей. Соответственно она не предназначена для бессрочного хранения.

При этом полиция может ссылаться на то, что, например, информация о различных правонарушениях необходима для анализа статистики правонарушений за определенный период времени, на той или иной территории и т.д. В любом случае ни в законодательстве, ни в практике КС РФ не установлено критериев, четко регулирующих данные вопросы. В частности, отсутствует правовой механизм, обеспечивающий обязанность полиции уничтожать информацию об уголовном преследовании граждан, что говорит о широкой дискреции полиции в решении рассматриваемого вопроса. Кроме того, законодательно не установлена ответственность за собственно бессрочное хранение указанной информации полицией без соответствующих обоснований, что было проигнорировано КС РФ в отмеченных решениях.

В определении от 16 июля 2013 г. № 1176-О КС РФ указал, что Закон № 152-ФЗ позволяет хранить информацию о состоянии здо-

ровья граждан исключительно в целях реализации их права на охрану здоровья и медицинскую помощь, при этом конфиденциальность персональных данных обеспечивается врачебной тайной. Таким образом, КС РФ придерживается позиции, в силу которой при наличии предусмотренной законом обязанности обеспечения конфиденциальности персональных данных обработка и хранение таких данных допустимы. При этом следует заметить, что ст. 13 Закона об охране здоровья граждан предусматривает запрет разглашения любых сведений, полученных в связи с обращением гражданина в медицинское учреждение. При этом указанная статья содержит конкретный перечень оснований, при наступлении которых допускается использование сведений, составляющих врачебную тайну. Важно также учесть, что положения ст. 13 Закона об охране здоровья граждан корреспондируют п. 1, 6 ч. 1 ст. 6 Закона № 152-ФЗ.

Следовательно, можно заключить, что требование об удалении персональных данных исходя из практики КС РФ по таким делам, должно быть основано на следующем:

1) нарушение прав заявителя обработкой и хранением персональных данных;

2) фактическая возможность удаления персональных данных из общего доступа;

3) отсутствие у оператора оснований для хранения и обработки персональных данных, предусмотренных ст. 13 Закона № 152-ФЗ;

4) отсутствие специального режима охраны персональных данных, предусмотренных федеральным законом.

§ 5. Защита персональных данных при рассмотрении обращений граждан

Определенные проблемы возникают в правоприменительной практике в отношении защиты персональных данных при рассмотрении обращений граждан. Спорной является ситуация относительно возможности граждан лично знакомиться с материалами дела и оценивать тем самым законность решения по итогам направленного ими обращения в орган власти или иную организацию, выполняющую функции публичного управления. Согласно позиции КС РФ все зависит от сложившихся обстоятельств: уполномоченный орган или должностное лицо в соответствующих случаях по своему административному усмотрению отказывает или предоставляет возможность доступа к указанным документам и материалам на том основании, что содержащаяся в них информация, затрагивающая права, свободы и законные интересы других лиц, хотя и не защища-

ется в качестве государственной или иной охраняемой федеральным законом тайны, однако отнесена к сведениям, распространение которых в Российской Федерации в установленном федеральным законом порядке ограничено или запрещено (определение от 7 февраля 2013 г. № 134-О). Соответственно ограничение на раскрытие и распространение информации, относящейся к персональным данным, направлено на обеспечение разумного баланса конституционно защищаемых ценностей (определение от 28 июня 2018 г. № 1664-О).

Напротив, в силу ст. 6 Федерального закона от 2 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» не допускается разглашение сведений, содержащихся в обращении, а также сведений, касающихся частной жизни гражданина, без его согласия.

В определении от 22 декабря 2015 г. № 2906-О КС РФ рассмотрел следующую ситуацию в отношении некоммерческой организации Управлением Минюста России проводилась внеплановая проверка, основанием для которой послужило требование прокуратуры Челябинской области. Между тем само требование прокуратуры было направлено в связи с обращением гражданина в прокуратуру Челябинской области. Представители некоммерческой организации просили Минюст России предоставить исходное обращение, явившееся поводом для проверки, но им было отказано со ссылкой на то, что обращение содержит персональные данные, которые не могут быть разглашены без согласия гражданина. КС РФ указал, что лицо, в отношении которого осуществляется внеплановая проверка, вправе требовать для ознакомления все материалы, послужившие основанием для ее проведения, и рассчитывать на их получение при соблюдении ограничений, предусмотренных федеральным законодательством. Вместе с тем лица, которые направляют в органы публичной власти обращения, содержащие информацию, которая может послужить основанием для проведения внеплановых проверок, вправе рассчитывать на то, что сообщенные ими сведения, относящиеся к их частной жизни, а равно их персональные данные не будут автоматически (без необходимости) предоставлены лицам, в отношении которых проводятся указанные проверки. Однако это не исключает возможности ознакомления проверяемых лиц с данными, содержащимися в соответствующих обращениях. Но при этом должно быть гарантировано, что лицо, направляющее обращение, не будет идентифицировано, если оно не давало согласия на распространение его персональных данных, и к его персональным данным не будет получен доступ.

§ 6. Ограничение права на получение (истребование) информации нормами Закона № 152-ФЗ

Неоднократными были обращения в КС РФ граждан, усматривавших ограничение их процессуальных и профессиональных прав на истребование информации нормами Закона № 152-ФЗ. Оспаривание норм федерального законодательства в данном случае сводится преимущественно к вопросам конституционности ограничения правомочий адвоката и, соответственно, прав гражданина получать доказательства, содержащие персональные данные, для участия в судебном процессе (определение от 29 января 2009 г. № 3-О-О). Данным определением был подтвержден особый правовой режим информации, содержащей персональные данные. Было отмечено, что Конституция РФ «допускает возможность установления в отношении той или иной информации специального правового режима, в том числе режима ограничения свободного доступа к ней со стороны граждан. Исключение информации, относящейся к персональным данным, которая была запрошена заявителем, из режима свободного доступа полностью соответствует предписаниям ч. 2 ст. 24 Конституции Российской Федерации. В противном случае под угрозой оказалось бы гарантированное ч. 1 ст. 23 и ч. 1 ст. 24 Конституции Российской Федерации право на неприкосновенность частной жизни». Основываясь на данной правовой позиции, КС РФ признал, что действие Федерального закона от 22 декабря 2008 г. № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации» не распространяется на отношения, связанные с обеспечением доступа к информации о деятельности судов, содержащей персональные данные (определение от 16 декабря 2010 г. № 1626-О-О). Однако эта норма не предусматривает полного запрета доступа к любой информации, содержащей персональные данные. Некоторые субъекты имеют право на доступ к ней, и они должны быть непосредственно поименованы в законе, однако законодатель формально не отнес к их числу адвокатов (определение от 17 июня 2008 г. № 434-О-О).

В части 2 ст. 24 Конституции РФ не установлены порядок и условия реализации гарантируемого ею права — это компетенция федерального законодателя, который, исходя из необходимости защиты частных и публичных интересов, вправе установить разные уровни гарантий и степень возможных ограничений права на получение информации при условии соразмерности таких ограничений конституционно признаваемым целям их введения (ч. 3 ст. 55 Конституции РФ). При этом, как указал КС РФ в постановлении от 18 фев-

раля 2000 г. № 3-П, ограничение права, вытекающего из ч. 2 ст. 24 Конституции РФ, допустимо лишь в соответствии с федеральным законом, устанавливающим специальный правовой статус не подлежащей распространению информации, обусловленный ее содержанием, в том числе наличием в ней данных, составляющих государственную тайну, конфиденциальных сведений, связанных с частной жизнью, со служебной, коммерческой, профессиональной, изобретательской деятельностью. Федеральный законодатель не называет адвокатов в числе лиц, запросы которых о предоставлении информации, составляющей коммерческую тайну, являются обязательными для обладателей данной информации, а также для органов публичной власти, которым она стала известна в силу выполнения ими своих функций.

В определении от 29 сентября 2011 г. № 1063-О-О, предметом оценки которого был запрет на самостоятельное истребование адвокатом сведений, содержащих персональные данные, для предоставления их суду в качестве доказательств по делу, КС РФ отметил, что нормы Закона № 152-ФЗ устанавливают специальные категории персональных данных, условия обработки которых предусматривают также специальный правовой режим доступа к ним, обеспечивающий конфиденциальность сведений о частной жизни лица (определение от 29 сентября 2011 г. № 1063-О-О). Такой режим, по мнению КС РФ, не исключает возможность доступа к персональным данным посредством судебных запросов, поскольку заявитель не лишен возможности при рассмотрении судом конкретного дела с участием его доверителя обратиться к суду с ходатайством об истребовании доказательств, в том числе сведений, содержащих конфиденциальную информацию.

Интерес представляет жалоба в КС РФ Т.М. Вербицкой, в которой она оспаривает конституционность п. 5 ч. 1 ст. 6 Закона № 152-ФЗ, в соответствии с которым обработка персональных данных допускается в случае, если она необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем (определение от 17 июля 2018 г. № 1810-О). По мнению заявительницы, указанное законоположение не соответствовало ст. 17 (ч. 3), 24, 46 (ч. 1) Конституции РФ в той мере, в какой оно допускает использование ресурсоснабжающей организацией персональных данных (личного номера телефона) без согласия субъекта персональных данных, на-

рушает баланс прав и законных интересов сторон договора о предоставлении коммунальных услуг, отдавая приоритет интересам юридического лица. КС РФ отметил, что п. 5 ч. 1 ст. 6 Закона № 152-ФЗ «допуская обработку персональных данных, если она необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, направлен на реализацию принципа надлежащего исполнения обязательств в соответствии с условиями обязательства и требованиями закона (ст. 309 ГК РФ), обеспечивает защиту прав участников договорных отношений, в том числе по предоставлению коммунальных услуг, справедливый баланс их законных интересов и не может расцениваться как нарушающий конституционные права и свободы заявительницы в указанном в жалобе аспекте».

Интерес представляет позиция КС РФ по вопросу возможности выдачи копии документов, составляющих врачебную тайну, гражданину об его умершем близком (родственнике, супруге и т.д.). Так, в определении от 9 июня 2015 г. № 1275-О КС отметил, что медицинская информация, непосредственно касающаяся не самого гражданина, а его умерших близких (родственника, супруга и т.д.) как связанная с памятью о дорогих ему людях, может представлять для него не меньшую важность, чем сведения о нем самом, а потому отказ в ее получении, особенно в тех случаях, когда наличие такой информации помогло бы внести ясность в обстоятельства их смерти, существенно затрагивает его права — как имущественные, так и личные неимущественные. В то же время подобная информация является конфиденциальной и составляет медицинскую тайну не только при жизни лица, но и после его смерти. Исходя из ряда конституционных положений (ч. 1 ст. 24, ч. 1 ст. 41 Конституции РФ) в их неразрывной взаимосвязи и учитывая, что гарантии защиты чести и достоинства умершего и доброй памяти о нем не могут быть исключены из сферы общего (публичного) интереса в государстве, где человек, его права и свободы являются высшей ценностью (постановление от 14 июля 2011 г. № 16-П), КС РФ полагает, что введение законодателем ограничений на предоставление медицинских сведений в отношении умершего гражданина третьим лицам само по себе отвечает этим конституционным положениям[1].

В определении от 9 июня 2015 г. № 1275-О КС РФ отметил, что в случае, когда сведения о причине смерти и диагнозе заболевания пациента доступны заинтересованному лицу в силу закона, сохранение в тайне от него информации о предпринятых мерах медицинско-

[1] Подробнее см. § 10 настоящего комментария.

го вмешательства, в частности о диагностике, лечении, назначенных медицинских препаратах, не может во всех случаях быть оправдано необходимостью защиты врачебной тайны, особенно с учетом мотивов и целей обращения за такими сведениями. В подобных ситуациях суд при осуществлении подготовки гражданского дела к разбирательству, правоохранительные органы при решении вопроса о возбуждении уголовного дела, а прокурор при проведении проверки в порядке надзора за соблюдением прав и свобод человека и гражданина могут на основе принципов соразмерности и справедливости принять решение о необходимости ознакомить заинтересованное лицо со сведениями, относящимися к истории болезни умершего пациента, в той мере, в какой это необходимо для эффективной защиты прав заявителя и прав умершего лица. При этом федеральный законодатель не лишен возможности в порядке совершенствования нормативно-правового регулирования в данной сфере предусмотреть конкретные правовые механизмы доступа к сведениям, составляющим врачебную тайну умершего лица, с учетом конституционных требований и сформулированных на их основании правовых позиций КС РФ с соблюдением разумного баланса прав и интересов всех субъектов соответствующих правоотношений. Таким образом, КС РФ по существу отметил наличие пробела в рассматриваемой норме, который хоть и не нарушает охраняемых Конституцией РФ прав и свобод граждан, тем не менее может быть устранен законодателем для целей реализации обозначенного в приведенном определении механизма доступа к сведениям о персональных данных истории болезни умерших лиц.

Кроме того, КС РФ со ссылкой на ряд решений Европейского Суда по правам человека (постановления от 25 февраля 1997 г. по делу «Z. против Финляндии», от 27 августа 1997 г. по делу «M.S. против Швеции» и др.) отметил, что международное право и конституционные нормы не устанавливают конкретных процедур, в рамках которых заинтересованное лицо может ознакомиться с информацией, содержащей медицинскую тайну иного лица. Соответственно федеральный законодатель обладает определенной свободой усмотрения при создании правовых механизмов, которые при соблюдении надлежащего баланса защищаемых Конституцией РФ ценностей позволяли бы заинтересованному лицу осуществлять эффективную защиту (в том числе судебную) как принадлежащих ему имущественных прав и нематериальных благ, так и права на человеческое достоинство умершего лица. Мотивируя свое решение, КС РФ указал на то, что в материалах, представленных в КС РФ заявителем, отсутствуют сведения о том, что он выражал намерение ознакомить-

ся со сведениями, содержащимися в материалах проверки следственными органами его сообщения о преступлении, либо оспаривал вынесенное следователем по итогам проверки процессуальное решение, либо обращался в прокуратуру с соответствующим заявлением. В этих материалах также не содержатся сведения, которые позволяли бы сделать вывод о том, что заявитель воспользовался гражданско-правовыми средствами защиты своих прав.

Таким образом, можно сделать ряд выводов:

1. Учет правовых позиций КС РФ способствует развитию правоприменительной практики, позволяет определять направления совершенствования законодательства в сфере персональных данных, что должно быть направлено на защиту конституционных ценностей (прав и свобод человека и гражданина, обеспечение баланса частных и публичных интересов и т.д.). Так, актуальной проблемой остается преодоление несоответствия понятийного аппарата Закона № 152-ФЗ и норм, регулирующих обработку персональных данных. Возможным способом преодоления данной проблемы является конкретизация положений Закона № 152-ФЗ (в частности, понятия «персональные данные», так как к ним формально-юридически может быть отнесена практически любая информация о человеке), чему может способствовать КС РФ путем указания в своих решениях федеральному законодателю на необходимость совершенствования законодательства Российской Федерации по тому или иному вопросу (на примере постановлений от 20 октября 2016 г. № 20-П, от 10 июля 2018 г. № 30-П, от 4 февраля 2019 г. № 8-П и др.).

2. Правовые позиции КС РФ в области персональных данных отражают определенные тенденции взаимодействия общего правового режима персональных данных и специальных правовых режимов обработки отдельных видов информации. Так, в своих решениях КС РФ указывает, что большей юридической силой обладает специальное регулирование отношений в сфере персональных данных, можно наблюдать признание приоритета отраслевых законов над общими нормами Закона № 152-ФЗ.

3. В правовых позициях КС РФ прослеживается стремление разрешить конкретную спорную ситуацию с точки зрения соблюдения баланса интересов субъекта персональных данных и интересов иных лиц, сведения о которых содержатся в истребуемых им документах.

4. Большинство спорных ситуаций, ставших основанием для обращения в КС РФ, вытекали из конфликта частных и публичных интересов. Анализ практики конституционного судопроизводства в сфере персональных данных показал, что по своему характеру данные ситуации имеют в целом административно-правовую природу и воз-

никают по поводу обработки персональных данных в различных сферах государственного управления в процессе предоставления (или организации предоставления) услуг органами публичной власти или непосредственно связанными с ними организациями. При этом, несмотря на декларируемую конституционную ценность — обеспечение баланса частных и публичных интересов, КС РФ в последнее время отдает приоритет защите публичных интересов в области сбора, хранения и предоставления персональных данных граждан без их согласия уполномоченным органам и лицам, а также удаления персональных данных граждан по их требованию, предоставленных ими ранее в медицинские учреждения либо связанных с судимостью.

Глава 3
ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ПРАВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ДОСТИЖЕНИИ ОСНОВНЫХ ЗАДАЧ ПРАВОСУДИЯ

В условиях широкого распространения цифровых технологий и роста объема и значения информационных ресурсов для развития национальной экономики действующее российское законодательство нуждается в модернизации, в том числе в изменении правового режима персональных данных, а также сведений, составляющих тайну личной жизни, семейную тайну, тайну частной жизни. Главная задача такой модернизации состоит не только в создании правовых условий для эффективного развития производства и сферы услуг, но и в обеспечении правовых гарантий защиты прав граждан и организаций.

Судебная практика так или иначе обнаруживает ряд принципиальных недостатков действующего правового регулирования.

Так, отсутствие в Законе № 152-ФЗ конкретизированного понятия персональных данных приводит к различному толкованию его содержания и разночтениям при отнесении тех или иных данных к категории персональных, как было отмечено в гл. 2 настоящего комментария.

Законом № 152-ФЗ регулируется только обработка персональных данных как таковых, однако такие действия не осуществляются сами по себе и не образуют самостоятельный объект правового регулирования[1]. Обработка персональных данных не связывается Законом № 152-ФЗ с гарантиями защиты прав субъекта-гражданина, специальные способы защиты которых законом не определены. Статья 17 закона лишь указывает, что субъект персональных данных может обратиться в суд с требованием о возмещении убытков и (или) компенсации морального вреда, но этого недостаточно для эффективности компенсаторно-восстановительной функции гражданского права в указанной сфере[2].

Цифровизация обработки судебных актов и иной информации, необходимой для выполнения задач правосудия, предполагает ис-

---

[1] См.: Синицын С.А. Субъективные публичные права: к разработке вопроса о понятии и системе // Адвокат. 2016. № 7.

[2] Там же.

пользование персональных данных лиц, участвующих в деле, объем которого законом также не определен.

Эти и другие проблемы законодательного регулирования не способствуют формированию единых подходов в правоприменительной практике, а, напротив, создают предпосылки для возникновения ряда коллизий, примером которых может служить практика судов по вопросу доступа к персональным данным в связи с участием лица в судебном разбирательстве.

По общему правилу обработка персональных данных осуществляется с согласия субъекта персональных данных. Вместе с тем Законом № 152-ФЗ предусматривается закрытый перечень случаев, при которых такое согласие не требуется. Так, персональные данные обрабатываются «в связи с участием лица в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах» (п. 3 ст. 6). При этом речь идет об обработке персональных данных частными лицами, которые вынуждены указывать в процессуальных документах персональные данные других лиц без их согласия, а не самим судом.

Согласно ранее действовавшей редакции указанной нормы обработка персональных данных допускалась, если была «необходима для осуществления правосудия», однако, как указано в пояснительной записке к законопроекту, которым эта формулировка была изменена, понятие «осуществление правосудия» в самом Законе № 152-ФЗ не раскрывается, поэтому было уточнено, что обработка персональных данных допускается без согласия субъекта персональных данных в том случае, если лицо является участником конституционного, уголовного, административного и гражданского судопроизводства, судопроизводства в арбитражных судах[1]. Вместе с тем понятия судопроизводства в Законе № 152-ФЗ также не содержится, в связи с чем необходимость внесения указанных изменений, полагаем, обусловлена возникающими в судебной практике трудностями применения недостаточно конкретизированной нормы, однако следует признать, что в результате внесенных изменений ситуация кардинально не изменилась.

По-прежнему в процессе правоприменения суды сталкиваются с коллизией между нормами Закона № 152-ФЗ и нормами процессуального законодательства, что обусловлено спецификой правового режима персональных данных, а также поиском баланса интересов

---

[1] См.Е Федеральный закон от 29 июля 2017 г. № 223-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» // СЗ РФ. 2017. № 31 (ч. I). Ст. 4772.

субъекта персональных данных в части защиты сведений о себе и интересов третьих лиц в части получения данных сведений в целях реализации их процессуальных прав.

Общее правило распределения бремени доказывания гласит, что каждая сторона должна доказать те обстоятельства, на которые она ссылается как на основание своих требований и возражений. Вместе с тем довольно часто для подтверждения своих требований или возражений лицу, участвующему в деле, требуется доказательство, содержащее персональные данные других лиц, которые, очевидно, не давали согласия на такую обработку их персональных данных. В связи с этим встает вопрос о соотношении норм, направленных на защиту персональных данных, и норм, регулирующих порядок рассмотрения и разрешения дел судами, в частности положений о правах и обязанностях лиц, участвующих в деле, в области доказывания.

Собирание информации в целях формирования доказательственной базы по делу — процессуальное право и одновременно бремя стороны, выполнение которого зависит не только от инициативы заинтересованного лица, но и от фактического доступа к тем или иным данным, не находящимся в его распоряжении или в свободном доступе. В связи с этим нормы Закона № 152-ФЗ не раз оспаривались в КС РФ как ограничивающие, по мнению заявителей, процессуальные права участников процесса[1].

К примеру, в связи с подготовкой документов для обращения в суд с иском о признании недействительными результатов межевания

---

[1] См.: определения КС РФ от 29 января 2009 г. № 3-О-О «Об отказе в принятии к рассмотрению жалобы гражданина Глушкова Николая Петровича на нарушение его конституционных прав статьями 3, 5, 6 и 9 Федерального закона "Об информации, информационных технологиях и о защите информации "» и статьями 8 и 9 Федерального закона "О персональных данных"», от 17 ноября 2011 г. № 1585-О-О «Об отказе в принятии к рассмотрению жалобы гражданки Клещ Елены Владимировны на нарушение ее конституционных прав частью четвертой статьи 5 и частью первой статьи 12 Федерального закона "Об оперативно-розыскной деятельности"», от 29 сентября 2011 г. № 1063-О-О «Об отказе в принятии к рассмотрению жалобы гражданина Багадурова Магомеда Магомедовича на нарушение его конституционных прав подпунктом 1 пункта 3 статьи 6 Федерального закона "Об адвокатской деятельности и адвокатуре в Российской Федерации", статьей 10 Федерального закона "О персональных данных" и частью второй статьи 57 Гражданского процессуального кодекса Российской Федерации"», от 28 февраля 2017 г. № 244-О "Об отказе в принятии к рассмотрению жалобы гражданина Мошкина Михаила Игоревича на нарушение его конституционных прав подпунктом 1 пункта 3 статьи 6 Федерального закона "Об адвокатской деятельности и адвокатуре в Российской Федерации" во взаимосвязи с положением пункта 1 части 2 статьи 227 Кодекса административного судопроизводства Российской Федерации"».

конкретного земельного участка М.И. Мошкин направил адвокатский запрос в местную администрацию муниципального образования о предоставлении ему заверенной копии решения о выделении земельного участка, принадлежащего другому лицу. В предоставлении данного документа ему было отказано, отказ был обжалован в порядке административного судопроизводства, но суды общей юрисдикции такие действия должностного лица местной администрации признали законными. Было установлено, что запрашиваемая информация относится к сведениям ограниченного доступа, которые не могут быть предоставлены по запросу адвоката, не имеющего доверенности от правообладателя; в то же время копия истребуемого документа имеется в распоряжении административного истца.

В связи с данным делом М.И. Мошкин обратился с жалобой в КС РФ. По мнению заявителя, оспариваемое действующее регулирование предоставляет правоприменителям возможность определять по своему усмотрению то, какие сведения являются необходимыми адвокату для оказания юридической помощи, что противоречит Конституции Российской Федерации.

КС РФ отказал в принятии указанной жалобы к рассмотрению, при этом указав, что «в силу статьи 24 (часть 2) Конституции Российской Федерации любая затрагивающая права и свободы гражданина информация должна быть ему доступна при условии, что законодателем не предусмотрен специальный правовой статус такой информации в соответствии с конституционными принципами, обосновывающими необходимость и соразмерность ее особой защиты; при этом Конституция Российской Федерации допускает возможность установления в отношении той или иной информации специального правового режима, в том числе режима ограничения свободного доступа к ней со стороны граждан (определения от 12 мая 2003 г. № 173-О, от 29 января 2009 г. № 3-О-О и др.), что, однако, не лишает адвоката возможности при рассмотрении судом конкретного дела с участием его доверителя обратиться к суду с ходатайством об истребовании доказательств, в том числе сведений, содержащих конфиденциальную информацию (определение от 29 сентября 2011 г. № 1063-О-О)».

Правовая позиция КС РФ, изложенная в указанном определении, а также в ряде других актов, основывается на том, что невозможность самостоятельно «получить» необходимое доказательство, содержащее персональные данные, и, как следствие, затруднительность осуществления своих процессуальных прав по доказыванию компенсируется правом лиц, участвующих в деле, ходатайствовать перед судом в истребовании доказательств. Таким образом, по общему правилу

документы, содержащие персональные данные, могут быть предоставлены только по запросу суда.

Право адвоката запрашивать информацию, в том числе и содержащую персональные данные, предусмотрено п. 1 ч. 3 ст. 6 Федерального закона от 31 мая 2002 г. № 63-ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации» (далее — Закон об адвокатуре). Наличие такого права корреспондирует с обязанностью предоставить запрашиваемую информацию, если к этому нет законодательных запретов или препятствий. КС РФ пришел к выводу, что законодательство, направленное на защиту персональных данных, является специальным по отношению к нормам, регулирующим статус и полномочия адвоката, а значит, составляет тот случай, когда в доступе к информации, необходимой для осуществления целей адвокатской деятельности, может быть правомерно отказано, если такая информация содержит персональные данные лица, не являющегося его доверителем.

Вместе с тем практика судов общей юрисдикции демонстрирует отсутствие единообразия в решении данного вопроса.

Так, в рамках дела о расторжении брака и взыскании алиментов в качестве доказательства была представлена копия трудовой книжки, которая была получена от бывшего работодателя истицы адвокатом ответчика.

Адвокат, представляя интересы супруга истицы, обратился к генеральному директору организации, в которой работала истица, с письменным запросом в порядке п. 1 ч. 3 ст. 6 Закона об адвокатуре о предоставлении сведений, касающихся ее трудовой деятельности, и соответствующих документов для предъявления в суд в качестве доказательств по гражданскому делу, рассматриваемому в закрытом судебном заседании. В запросе адвокатом было гарантировано соблюдение режима конфиденциальности представленных сведений и документов. Данный запрос был удовлетворен, сведения о трудовой деятельности были направлены адвокату ответчика, при этом было указано на возможность использования полученных персональных данных работника исключительно для целей, указанных в запросе, с соблюдением режима секретности (конфиденциальности).

Истица обратилась с иском к своему бывшему работодателю с требованием о признании действий по передаче персональных данных при отсутствии ее согласия третьим лицам незаконными, обязании обеспечить защиту персональных данных, взыскании компенсации морального вреда. По мнению истицы, бывший работодатель в нарушение требований Закона № 152-ФЗ и ТК РФ не обеспечил

сохранность ее персональных данных, неправомерно передав их без согласия и судебного запроса не уполномоченным в установленном порядке третьим лицам, а потому должен понести ответственность за данные незаконные действия и обеспечить защиту персональных данных.

Суд первой инстанции отказал в удовлетворении заявленных требований, с чем согласились вышестоящие суды — апелляционной и кассационной инстанций. При этом суды исходили из того, что предоставление адвокату копии трудовой книжки соответствует действующему законодательству, поскольку обработка персональных данных истца осуществлялась бывшим работодателем в целях обеспечения права на представления доказательств по гражданскому делу, предусмотренного статьей 35 ГПК РФ, а истцом не представлено доказательств того, что работодатель, осуществляя обработку персональных данных при ответе на запрос адвоката, не соблюдает принципы и правила обработки персональных данных, предусмотренные Законом № 152-ФЗ, не соблюдает конфиденциальность, не обеспечивает безопасность персональных данных при их обработке, а также того, что указанные действия ответчика повлекли нарушение прав и свобод истца[1].

Неопределенность в вопросе о соотношении законодательства о персональных данных, которое безусловно направлено на обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, и законодательства об адвокатской деятельности, а также процессуального законодательства, предоставляющего право адвокату и иному лицу, осуществляющему доказательственную деятельность, собирать и представлять доказательства в целях обоснования своей позиции по делу, порождает в судебной практике чрезмерное судейское усмотрение в решении аналогичных вопросов и, как следствие, двойные стандарты в вопросе признания допустимости и относимости доказательств, содержащих персональные данные.

В изложенном деле суд исходил из необходимости обеспечения права на представление доказательств по гражданскому делу, а не из требования защиты данных о частной жизни, в связи с чем признал допустимым доказательством по делу информацию, содержащую персональные данные, полученную не на основании судебного за-

---

[1] См.: Апелляционное определение Московского городского суда от 24 декабря 2014 г. по делу № 33-41576/2014, кассационное определение Московского городского суда от 5 июня 2015 г. № 4г/2-6343/15.

проса, а самим представителем лица, участвующего в деле. При этом специальный правовой режим такой информации, на который ссылался в своих постановлениях КС РФ, не был принят во внимание судами.

Аналогичный подход сложился в отношении арбитражных управляющих. Суды исходят из того, что законодательство о банкротстве является специальным по отношению к законодательству, регулирующему вопросы распространения персональных данных.

Так, Арбитражный суд Московского округа указал, что «предоставление по запросу конкурсного управляющего информации о членах ликвидационной комиссии, являющихся должностными лицами органа местного самоуправления, не является разглашением персональных данных физических лиц, так как в силу п. 3 ч. 1 ст. 6 Закона № 152-ФЗ представляет собой "обработку" персональных данных, которая в том числе допускает их передачу (распространение, предоставление, доступ), если это необходимо для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации». Кроме того, суд пояснил, что «арбитражный управляющий действует на основании судебного акта арбитражного суда о его утверждении в связи с введением арбитражным судом процедуры банкротства, и предоставление ему информации, необходимой для осуществления полномочий вызвано исполнением соответствующего судебного акта арбитражного суда»[1]. Таким образом, правовым основанием для доступа к доказательствам по делу, содержащим персональные данные лиц, не дававших согласия на их обработку, может служить судебный акт об утверждении арбитражного управляющего.

Возможны коллизии Закона № 152-ФЗ и процессуального законодательства ввиду ограничения доступа к персональным данным не только на этапе собирания доказательств, но и при их исследовании. Так, судья может отказать в ознакомлении с доказательствами, представленными другими лицами, участвующими в деле, ввиду того, что они содержат персональные данные и их правообладатель не давал согласия на обработку.

Такой подход противоречит основам процессуального законодательства, свидетельствует о неправильном толковании Закона № 152-ФЗ, нормы которого не могут рассматриваться в качестве специального правового регулирования общественных отношений,

---

[1] Постановление Арбитражного суда Московского округа от 13 сентября 2018 г. № Ф05-14343/2018 по делу № А41-10789/18.

складывающихся при рассмотрении и разрешении дел судами и выступающих предметом регулирования процессуального права.

Принципы цивилистического процесса не могут быть ограничены отраслевым законодательством о защите персональных данных. В силу действия принципов состязательности и равноправия стороны имеют равные права знакомиться с материалами дела, делать выписки из них, снимать копии, заявлять отводы, участвовать в исследовании доказательств и заявлять свои доводы на представленные доказательства, в том числе заявлять об их подложности, и Закон № 152-ФЗ не может их ограничивать, по сути изменять установленные процессуальными кодексами правила исследования и оценки доказательств.

Цивилистический процесс — процесс гласный. В целях же сохранения охраняемой законом тайны в процессуальных кодексах предусмотрено правило о закрытом судебном заседании, которое проводится не только в случаях, предусмотренных федеральным законом, но и допускается при удовлетворении ходатайства лица, участвующего в деле и ссылающегося на необходимость сохранения коммерческой или иной охраняемой законом тайны, неприкосновенность частной жизни граждан или иные обстоятельства, гласное обсуждение которых способно помешать правильному разбирательству дела либо повлечь за собой разглашение указанных тайн или нарушение прав и законных интересов гражданина. Именно в случае потенциальной угрозы разглашения персональных данных, способного повлечь нарушение прав и свобод лиц, участвующих в деле, суд может принять решение о проведении судебного разбирательства в закрытом судебном заседании.

Таким образом, процессуальное законодательство предусматривает механизмы, позволяющие защитить персональные данные участников процесса, и в этом плане является самодостаточным. Иными словами, применение норм Закона № 152-ФЗ, направленных на защиту прав граждан на неприкосновенность частной жизни, личную и семейную тайну, не может приводить к ограничению гарантий, установленных Конституцией РФ и процессуальными кодексами и обусловленных правом каждого на судебную защиту своих прав и охраняемых законом интересов.

Глава 4
РОЛЬ СУДЕБНОЙ ПРАКТИКИ В ФОРМИРОВАНИИ ПОДХОДОВ К ПРАВОВОМУ РЕГУЛИРОВАНИЮ КОММЕРЧЕСКОГО ОБОРОТА ПЕРСОНАЛЬНЫХ ДАННЫХ

§ 1. Коммерческий оборот персональных данных: проблемы правового регулирования

Принятие на государственном уровне Стратегии развития информационного общества[1] предполагает решение ряда фундаментальных научных задач, связанных с осмыслением феномена информационного общества (декларированного в глобальных масштабах[2]) и его ключевых составляющих. Одной из таких составляющих является использование новых экономических возможностей, которые возникают в связи с развитием информационно-телекоммуникационных технологий, а именно включение в коммерческий оборот больших объемов информации, которая приобретает свойства товара. По мнению некоторых ученых, это едва ли не единственный ключевой признак информационного общества, поскольку остальные — всего лишь «информатизации устоявшихся отношений»[3].

Современная дискуссия о признании информации товаром с точки зрения гражданского права[4] и соответственно о выборе применимого к ней оптимального правового режима не препятствует фактическому возмездному обмену информацией между коммерческими организациями — субъектами предпринимательской деятельности, обладающими достаточными техническими ресурсами для осуществления подобных действий.

---

1 Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // СЗ РФ. 2017. № 20. Ст. 2901.

2 Окинавская хартия глобального информационного общества.

3 Подробнее об этом см.: Уэбстер Ф. Теории информационного общества. М., 2004.

4 См., например: Терещенко Л.К. Правовой режим информации: монография. М., 2007; Мефодьева К.В. Цифровые данные как объект гражданско-правового регулирования в Германии, США и России: дис. ... канд. юрид. наук. М., 2019.

Логику использования такой возможности подтверждают официальные документы, в частности, в упомянутой Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы указано, что цифровая экономика представляет собой хозяйственную деятельность, ключевым фактором производства в которой являются данные в цифровой форме, и способствует формированию информационного пространства с учетом потребностей граждан и общества в получении качественных и достоверных сведений.

При этом данные становятся новым активом, причем главным образом за счет их альтернативной ценности, то есть по мере применения данных в новых целях и их использования для реализации новых идей[1]. Определение данных в стратегическом документе в качестве актива[2] предполагает возможность их использования в предпринимательских целях, с учетом не только их альтернативной, но и традиционной, коммерческой ценности.

В юридической науке еще до начала такого стремительного развития интернет-ресурсов и монетизации информационного обмена был обоснованно поставлен вопрос о том, какая информация может стать объектом гражданских прав, в частности купли-продажи. Констатировалось, что существуют границы, за пределами которых статус объекта гражданских прав для информации недопустим[3], при этом возможности включения информации в экономический оборот

---

1 Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы».

2 Некоторые организации в качестве одного из главных своих активов имеют именно накопленные данные. Например, на момент выхода компании Facebook на IPO (initial public offering) совокупная стоимость ее активов оценивалась в 6,6 млрд долл. США. Однако во время первичного размещения акций на фондовом рынке совокупная стоимость акций компании составила 104 млрд долл. США. По мнению аналитической компании Gartner, разницу между рыночной стоимостью и стоимостью традиционных активов компании составили как раз данные (порядка 2,1 трлн единиц «монетизируемого контента»: пометок «нравится», опубликованных материалов, комментариев, из чего был сделан вывод, что каждый такой элемент, рассматриваемый как отдельная единица данных, стоил около 4 центов). Учитывая тенденцию к возрастанию экономической роли накопленных данных, обладающих потенциальной коммерческой ценностью, в общей стоимости компании, становится очевидным, что это может стать возможным только при условии обеспечения их адекватной оборотоспособности и возможности коммерциализации. Подробнее об этом см.: Савельев А.И. Направления эволюции свободы договора под влиянием современных информационных технологий // Свобода договора: сборник статей / А.А. Амангельды, В.А. Белов, А.А. Богустов и др.; отв. ред. М.А. Рожкова. М., 2016; СПС «КонсультантПлюс».

3 Подробнее об этом см.: Терещенко Л.К. Правовой режим информации: монография. М., 2007. С. 48.

и выполнения функции экономического блага были поставлены в зависимость от ее содержания и установленного правового режима[1].

Выделяется два основных режима информации: императивный и диспозитивный, характер которых зависит от степени обязательности для участников правоотношений составляющих его правил поведения. Если эти правила поведения участники отношений не могут изменить по своему усмотрению, то правовой режим информации является императивным. Если же правила поведения, составляющие правовой режим информации, участники отношений могут менять по своему усмотрению, то такой режим является диспозитивным[2]. Для реализации гражданско-правовых отношений, по нашему мнению, должен подходить диспозитивный режим информации, предполагающий возможность изменения правил поведения в процессе обмена информацией и ее свободное использование.

Полагаем, что применению именно этого режима способствуют развитие информационно-телекоммуникационных технологий, тенденции более свободного перемещения персональных данных, что в свою очередь влечет широкое использование данных пользователей частными компаниями и органами государственной власти, а также сильный государственный акцент на стимулирование развития информационного общества и цифровой экономики.

Вместе с тем использование в коммерческом обороте персональных данных пользователей Интернета вызывает определенные проблемы, поскольку для персональных данных установлен законодательный режим, который обязаны соблюдать все субъекты, действующие в информационном пространстве. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее — Закон о персональных данных) закрепляет ряд требований, направленных на обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Необходимо упомянуть и о новом Регламенте (ЕС) № 2016/679 Европейского Парламента и Совета ЕС о защите физических лиц при обработке персональных данных и о свободном обращении таких данных[3], признанном одним из наиболее жестких документов в этой области. Он касается прав физических лиц, имеет целью обеспечить упрощенный доступ лиц к их персональным данным, в частности,

---

1 Там же.

2 См.: Терещенко Л.К. Модернизация информационных отношений и информационного законодательства: монография. М., 2013. С. 22.

3 Принят в г. Брюсселе 27 апреля 2016 г., применяется с 25 мая 2018 г.

возможность следить за тем, как они используются (ст. 15 Регламента); детализацию права на уничтожение персональных данных (ст. 17 Регламента); право быть информированным в кратчайшие сроки о несанкционированном доступе к персональным данным (ст. 34 Регламента)[1] и других аспектов обработки персональных данных и может применяться к российским компаниям, осуществляющим деятельность на территории Европейского Союза.

Полагаем, что в целях реализации преимуществ информационного общества требуется сбалансированное применение императивного (в части обеспечения защиты персональных данных) и диспозитивного (в части получения максимального эффекта от коммерческого использования информации) режимов, возможно, их сочетание в процессе развития информационно-телекоммуникационных правоотношений.

При этом важно учитывать и свойства информации, которые отличаются от свойств товаров, находящихся в коммерческом обороте, что может существенным образом повлиять на гарантии прав субъектов персональных данных, а также на степень доверия пользователей к информационным ресурсам, от которой зависит ценность этих ресурсов и возможность их использования.

Так, в исследовании Л.К. Терещенко, обобщающем большое количество определений, сформулированы в том числе следующие свойства информации: нематериальная сущность; физическая невозможность отчуждения информации от ее обладателя (поскольку информация остается известной тому субъекту, который ее передает тем или иным способом); субстанциональная несамостоятельность (необходимость закрепления на каком-либо носителе); неуничтожимость (это свойство особенно четко проявляется в условиях Интернета, поскольку сама глобальная сеть задумывалась как система, в которой невозможно уничтожить информацию даже при повреждении и уничтожении определенных носителей); возможность неограниченного тиражирования, копирования, воспроизведения и преобразования форм фиксации, что собственно и составляет основное преимущество сети Интернет как глобального носителя информации[2].

По мнению другого исследователя, необходимым и достаточным условием для проявления информацией вышеперечисленных свойств является ее нахождение внутри информационной системы.

---

[1] Подробнее об этом см.: Постникова Е.В. Некоторые аспекты правового регулирования защиты персональных данных в рамках внутреннего рынка Европейского союза // Право. Журнал Высшей школы экономики. 2018. № 1. С. 234–254.

[2] См.: Терещенко Л.К. Правовой режим информации: монография. М., 2007. С. 26.

Реализация совокупности свойств информации в информационной системе приводит к тому, что процесс воспроизводства, трансляции и мультипликации полезной информации остановить невозможно без разрушения самой информационной системы[1]. Полагаем, что при решении вопросов о возмездном и правомерном использовании информации в сети Интернет должны учитываться оба указанных фактора, т.е. и свойства информации, и свойства глобальной сети.

Эти качества информации и информационной системы (Интернета) затрудняют определение:

– возможностей и пределов реализации права свободно получать и распространять информацию, в том числе контроля за личной информацией со стороны ее обладателя;

– субъектов, ответственных за ее распространение, хранение, искажение либо восстановление, уничтожение и т.д., что для интернет-сферы в настоящее время является ключевым вопросом правового характера;

– соотношения гарантированных конституционных прав на свободу предпринимательской деятельности и на защиту личной жизни.

Кроме того, целесообразно уточнение понятия самого коммерческого оборота и возможности участия в нем не только коммерческих организаций, но и физических лиц, а также юридических лиц различных организационно-правовых форм.

Судебная практика может сыграть в решении этих вопросов одну из ключевых ролей, поскольку зачастую субъекты интернет-отношений, в частности субъекты обработки персональных данных, находятся в ситуации неопределенности в связи с отсутствием четких законодательных формулировок или условий правового режима, т.е. их действия нельзя заранее точно оценить как правомерные или неправомерные.

Ученые констатируют, что в целом наличие рынка данных является необходимым условием для развития технологий больших данных, которые, в свою очередь, играют важную роль в обеспечении эффективного функционирования иных инновационных технологий (интернета вещей, расширенной реальности, когнитивных вычислений и т.д.)[2]. Тем не менее отмечается, что в настоящее время как

---

[1] Будник Р.А. Эволюция системы авторских и смежных прав в информационном обществе: от исключительного к инклюзивному праву автора. М., 2013. С. 15.

[2] Савельев А.И. Направления эволюции свободы договора под влиянием современных информационных технологий.

таковой рынок данных в России еще не сложился — в том числе и потому, что неясна юридическая сторона взаимодействия[1].

Можно согласиться с тем, что рынок данных не сложился, однако он находится в стадии формирования и развивается, что подтверждает дело № А40-18827/17-110-180, рассмотренное российскими судами по иску общества с ограниченной ответственностью «ВКонтакте» к обществу с ограниченной ответственностью «ДАБЛ», о защите исключительных смежных прав на базу данных.

Указанный случай рассматривается во многих правовых исследованиях применительно к различным проблемам цифровизации общества и является своего рода знаковым, поскольку оно стало первым судебным делом, которое позволило сделать однозначный вывод о том, что информация, курсирующая в сети Интернет, продается и покупается, т.е. вовлекается в коммерческий оборот. При этом уточняется форма обмена данными (в частности, прямое копирование либо программное обеспечение доступа к ним, степень обработки и актуализации при возмездной передаче, их режим, а также правовой статус участников такого коммерческого информационного оборота, что в дальнейшем может способствовать развитию теоретических исследованиий в области правового регулирования общественных отношений в сети Интернет). Полагаем, что подобные случаи судебной практики позволят в дальнейшем прояснить юридическую сторону взаимодействия между субъектами коммерческого оборота, а также между основными поставщиками информации — пользователями в условиях технологии Web 2.0[2].

Окончательного решения по этому делу еще не вынесено, однако из фабулы дела можно вычленить несколько тематических блоков, которые представляют интерес с точки зрения формирования юридических основ коммерческого оборота информации, в частности персональных данных. Более того, в ходе рассмотрения указанного дела происходит поиск ответов на вопросы, связанные с концептуальными проблемами правового регулирования виртуального пространства. Одним из таких вопросов, на наш взгляд, является опре-

---

[1] Кирьянова А.В России будет создана первая биржа данных. URL: http://www.cnews.ru/news/top/index.shtml?2014/10/01/587454

[2] Напомним, что возможности формирования больших объемов данных появились с внедрением технологии web 2.0 и развитием социальных сетей, предполагающих общение и обмен информацией между пользователями, которые в данном случае могут рассматриваться и как участники информационного наполнения ресурсов (поставщики контента), при этом от числа и активности таких участников фактически зависит ценность самих интернет-ресурсов, а следовательно, и баз данных, которые потом поступают в оборот.

деление правового статуса субъекта, задействованного в интернет-отношениях.

§ 2. Определение правового статуса субъекта, задействованного в коммерческом обороте персональных данных в Интернете

Социальная интернет-сеть как относительно новое, массовое общественное явление — предмет внимания правовой науки[1], вокруг которого, в частности, развивается дискуссия относительно того, является ли она субъектом или объектом правового регулирования[2]. В указанном судебном деле социальная сеть в лице администрации выступает в качестве субъекта права, является стороной дела, защищает не только свои интересы, но и интересы своих пользователей, а также позиционирует себя как участника коммерческого оборота, что, в свою очередь, предполагает получение материальной отдачи от своей деятельности (несмотря на то, что указана символическая сумма возмещения ущерба).

Общество с ограниченной ответственностью «ВКонтакте» в лице администрации социальной сети (далее — Истец) обратилось с рядом требований к обществу с ограниченной ответственностью «Дабл» (далее — Ответчик), основное из которых состояло в прекращении нарушения Ответчиком исключительных прав Истца на базу данных пользователей социальной сети «ВКонтакте». Истец определяет свой статус как статус изготовителя базы данных пользователей этой социальной сети, требует прекратить извлечение и неоднократное использование информационных материалов этой базы данных, уничтожить со всех информационных носителей информационные эле-

---

[1] См., например: Перчаткина С.А., Черемисинова М.Е., Цирин А.М., Цирина М.А., Цомартова Ф.В. Социальные интернет-сети: правовые аспекты // Журнал российского права. 2012. № 5(185). С. 14–24; Монахов В.Н. Социальные сети как объект регулирования // Эволюция государственных и правовых институтов в условиях развития информационного общества / отв. ред. И.Л. Бачило. М., 2012; Молотников А.Е., Архипов Е.В. Социальные сети и компании-агрегаторы: правовые аспекты деятельности // Предпринимательское право. 2017. № 4. С. 38–47.

[2] Якушев М.В. Социальные сети как объект правового регулирования // Правовые инновации в сфере противодействия коррупции: материалы Первого Евразийского антикоррупционного форума и VII Международной школы-практикума молодых ученых-юристов (Москва, 30–31 мая 2012 г.) / отв. ред. Л.В. Андриченко, А.М. Цирин. М.: ИЗиСП, 2012. С. 591–605; Черемисинова М.Е. Социальная интернет-сеть в качестве субъекта правоотношений // Право в сфере Интернета: сборник статей. Сер. «Анализ современного права» / отв. ред. М.А. Рожкова. М., 2018. С. 375–386.

менты, ранее извлеченные из этой базы данных, а также взыскать 1 руб. компенсации.

Полагаем, важно обратить внимание на то, что Истцу в этом деле приходится обосновывать и доказывать свой правовой статус, который в настоящее время не определен. Термин «владелец сайта в сети Интернет» (п. 14 ст. 2 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», далее — Закон об информации) в данном деле не применяется, что объясняется сложным многосубъектным составом всей социальной сети, каждый пользователь которой может считаться владельцем своей официальной учетной записи (аккаунта), которую можно рассматривать как страницу сайта и на которую могут распространяться какие-либо имущественные права.

В результате отстаивания своих прав Истец обозначает как минимум одну составляющую такого сложного с точки зрения правовой оценки явления, как социальная интернет-сеть, — разработчика информационно-коммуникационного ресурса. При этом общество с ограниченной ответственностью уже наделено правосубъектностью в силу гражданско-правовых норм и выступающее в процессе и как «разработчик» программного обеспечения, и как «владелец» базы данных (персональной информации пользователей) в связи с условиями пользовательского соглашения, и как администрация ресурса, ответственная за выполнение законодательства в области защиты персональных данных. Не в последнюю очередь Истец апеллирует к обязательствам перед своими пользователями (принятым судом во внимание), обеспечившими наполнение базы данных сведениями, обладающими коммерческой ценностью.

Это подчеркивает тесную структурную и правовую взаимосвязь между Истцом и участниками социальной сети, которая впоследствии может обусловить постановку вопроса об условиях участия в коммерческом обороте информации не только юридических, но и физических лиц, сталкивающихся с гражданско-правовыми последствиями использования их персональных данных.

В настоящее время принцип сбора сведений о лицах, использующих социальные интернет-сети для различных целей, прост: информация предоставляется в обмен на сервисы, которые настолько удобны и разнообразны, что пользователи охотно соглашаются с условиями администрации. Вместе с тем появление права на забвение, вопросов, связанных с наследованием персональных аккаунтов или многоступенчатой (в том числе возмездной) передачей данных показывает, что в ходе развития и распространения интернет-ресурсов возможно возникновение большого числа проблем частноправового

характера, которые нельзя предвидеть или оценить на стадии присоединения к глобальному интернет-сервису, т.е. заключения пользовательского соглашения.

Примечательно, что Истцу из открытых источников стало известно о деятельности Ответчика о предложении третьим лицам услуг на основе собственных технологических методов и алгоритмов поиска, хранения и интеллектуального анализа данных из социальных сетей, включая социальную сеть Истца, функционирование которых основано на сборе и обработке в автоматическом режиме данных о пользователях для оценки кредитоспособности потенциальных и существующих заемщиков кредитных организаций, являющихся пользователями таких социальных сетей. Это означает, что какое-то время Ответчик действовал без ведома Истца, а также большинства пользователей.

Хотя один из пользователей социальной сети Истца обратился в полицию по факту сбора Ответчиком данных из социальной сети «ВКонтакте» и отображения таких данных на сайте АО «Национальное бюро кредитных историй» (далее — «НБКИ») (http://dd.nbki.ru). По результатам рассмотрения его заявления и анализа собранной в ходе проверки информации отделом МВД России по Хорошевскому району г. Москвы было установлено, что Ответчиком разработано программное обеспечение, с помощью которого он в автоматическом режиме собирает (извлекает) данные обо всех пользователях социальной сети «ВКонтакте». В результате этого Ответчиком сформирована собственная база данных пользователей с целью использования таких данных в коммерческих целях. Однако, по мнению Ответчика, сам факт отказа в возбуждении уголовного дела по ст. 272 Уголовного кодекса РФ, зафиксированный в постановлении, свидетельствует об отсутствии в его действиях состава неправомерного доступа к охраняемой законом компьютерной информации и дальнейшего ее копирования.

Одним из партнеров Ответчика значилось «НБКИ», на сайте которого указано о сотрудничестве с ООО «Дабл» и предложениях кредитным организациям сервисов на основе Big Data технологий, разработанных Ответчиком, позволяющих провести оценку кредитоспособности потенциальных и существующих заемщиков, используя данные из социальных сетей, включая социальную сеть Истца.

В связи с изложенным в адрес указанных лиц были направлены претензии с требованием прекратить незаконный сбор (извлечение) данных о пользователях социальной сети Истца и последующее их использование в коммерческих и иных целях.

Необходимо отметить, что Истец и «НБКИ» (ответчик 2) заключили мировое соглашение, которое определением от 15 августа 2017 г.

было утверждено судом. «НБКИ» также подтвердило факт оказания услуг третьим лицам (банкам) на основе данных из социальных сетей, включая социальную сеть Истца. Производство по делу в отношении «НБКИ» прекращено, несмотря на то, что решение по делу в первой инстанции состоялось не в пользу Истца, поскольку на той стадии он не смог доказать факт создания базы данных, соответствующей признакам, установленным ст. 1260 ГК РФ, а также факт возникновения исключительных прав на базу данных.

Вместе с тем заключение такого мирового соглашения (т.е. фактически наличие согласия «НБКИ» с основной позицией Истца) на стадии рассмотрения дела в первой инстанции в определенной мере подтверждает право Истца на учет его интересов при многоступенчатой и возмездной передаче данных, собранных изначально по его инициативе и с привлечением его материальных, технических и интеллектуальных ресурсов.

В решении по делу отмечается утверждение Истца о том, что на создание, работу по сбору, обработку и расположение информационных элементов, составляющих обновленную на 13 января 2017 г. базу данных Истца, за весь период ее формирования Истцом были понесены существенные финансовые, организационные и иные затраты, включая затраты на создание и поддержание инфраструктуры, закупку необходимого оборудования и серверов, а также затраты на человеческие ресурсы. Этот факт является одним из ключевых при доказывании наличия у субъекта смежного права, каким является исключительное право на базу данных.

Как следует из п. 14 Постановления Пленума Верховного Суда Российской Федерации от 19 июня 2006 г. № 15 «О вопросах, возникших у судов при рассмотрении гражданских дел, связанных с применением законодательства об авторском праве и смежных правах» и подтверждается судебной практикой по делам о защите авторского права или смежных прав, Истец должен подтвердить факт принадлежности ему авторского права и (или) смежных прав или права на их защиту, а также факт использования данных прав Ответчиком.

Однако суд первой инстанции посчитал факт создания базы данных Истцом не доказанным, хотя впоследствии данное решение было пересмотрено судом апелляционной инстанции[1] и подтверждено Судом по интеллектуальным правам[2].

---

[1] Постановление Девятого арбитражного апелляционного суда от 6 февраля 2018 г. № 09АП-61593/2017-ГК по делу № А40-18827/17 // СПС «КонсультантПлюс».

[2] Постановление Суда по интеллектуальным правам от 24 июля 2018 г. № С01-201/2018 // СПС «КонсультантПлюс».

Важное значение для определения правового статуса Истца и в итоге для решения суда имели Правила пользования сайтом, разработанные и размещенные Истцом на своем сайте. Так, в соответствии с п. 5.12. Правил пользования сайтом «ВКонтакте» Истец не принимает участия в формировании содержания персональной страницы пользователя, то есть пользователи сами публикуют на сайте информацию о себе. Согласно п. 8.2 и 8.5 указанных Правил Истец не изменяет формат материала, не переводит на другой язык, не корректирует, не редактирует его, пользователи сами систематизируют информацию, выбирая подходящие поля для заполнения на Сайте. Следовательно, в силу особенностей функционирования социальной сети «ВКонтакте» Истец не несет расходов на приобретение информации, ее проверку и обработку с целью создания обособленной базы данных.

Пунктом 5.12 Правил пользования сайтом установлено, что обладателями информации, размещаемой на персональных страницах социальной сети «ВКонтакте», являются пользователи сайта, разместившие подобную информацию, при этом пользователь как обладатель информации, размещенной на собственной персональной странице, «...осознает, что администрация сайта не принимает участие в формировании содержания и контроле доступа к персональной странице пользователя, пользователь также соглашается с тем, что указанная информация может быть доступна другим пользователям сети Интернет с учетом особенностей архитектуры и функционала Сайта».

Обладателями информации, представленной на персональных страницах пользователей Сайта, являются сами пользователи, а опубликованная ими информация является (путем установления пользователем соответствующего режима доступа) закрытой или общедоступной, т.е. открытой для использования любыми лицами согласно п. 2 ст. 7 Закона об информации.

Эти положения, а также тот факт, что затраты, на которые ссылался Истец в обоснование своей деятельности по формированию базы данных, должны были иметь целевое назначение и быть направленными исключительно на создание базы данных, не позволили ему выйти победителем из рассматриваемого спора в суде первой инстанции.

Ответчик настаивал на том, что база данных пользователей социальной сети является «побочным продуктом» (spin off) деятельности общества «ВКонтакте» по администрированию социальной сети. Суд апелляционной инстанции, отменяя решение суда первой инстанции, указал, что вывод суда об отсутствии базы данных пользователей как таковой противоречит имеющимся в материалах дела доказатель-

ствам и пришел к выводу о существовании базы данных пользователей социальной сети «ВКонтакте», обладающей всеми признаками базы данных по смыслу п. 2 ст. 1260 ГК РФ.

Также суд апелляционной инстанции не согласился с выводом суда первой инстанции относительно отсутствия существенных затрат на создание спорной базы данных и установил, что извлечение и использование даже несущественной части базы данных в данном случае признается нарушением исключительного права в силу п. 3 ст. 1335.1 ГК РФ, поскольку действия Ответчика противоречат нормальному использованию базы данных и ущемляют необоснованным образом законные интересы ее изготовителя.

Данный вывод суд апелляционной инстанции сделал на основании того, что у Истца имеются обязательства перед всеми пользователями социальной сети по обеспечению защиты персональных данных пользователей от неправомерного или случайного доступа к ним, копирования, распространения, воспроизведения, сбора, систематизации, хранения, передачи информации из социальной сети в коммерческих целях и/или в целях извлечения базы данных социальной сети в коммерческих или некоммерческих целях, или ее использования полностью или в любой части любым способом без согласия пользователя (п. 7.1 Правил защиты информации о пользователях, установленных администрацией «ВКонтакте»).

Несмотря на то что обеспечение защиты персональных данных не входит в обязанности изготовителя базы данных, указанное положение принято судом во внимание при решении вопроса о правомерности действий Ответчика, а также подчеркивает некую общность, которая формируется на интернет-платформе за счет договорного объединения разработчика ресурса и неопределенного круга лиц, от числа и активности которых зависит ценность этого ресурса. Так, в постановлении Суда по интеллектуальным правам от 24 июля 2018 г. по рассматриваемому делу отмечается, что создание базы данных пользователей социальной сети, как указывает общество «ВКонтакте», является для общества важной задачей, поскольку существование социальной сети без пользователей (и базы данных о них) невозможно.

По нашему мнению, данные выводы судов имеют важное значение для последующего решения принципиального вопроса о правовом статусе как владельца сетевого ресурса (в данном случае — Истца, получившего возможность проанализировать уязвимости в правилах, установленных им самим), так и пользователя социальной сети, который становится не просто потребителем информации (по существующей законодательной терминологии) или пользователем интернет-ресурса (что определяет его статус по Закону о защите прав

потребителей), а полноправным и активным участником информационного обмена, набирающего «коммерческие обороты».

Кроме того, ссылка в материалах дела на Правила пользования сайтом также имеет существенное значение для развития судебной практики, связанной со спорами в сети Интернет, поскольку зачастую именно такие документы являются своеобразным связующим звеном между реальным и виртуальным мирами, позволяющим субъектам, в том числе коммерческой деятельности, отстаивать свои права в сфере, характеризующейся правовой неопределенностью и отсутствием стабильности как для самих участников интернет-процессов, так и для инстанций, призванных поддерживать правопорядок в обществе. Роль пользовательских соглашений, правил использования сайтов и т.п. документов еще предстоит проанализировать в ходе определения правовых статусов и направлений развития деятельности субъектов релевантных общественных отношений.

Итак, судом апелляционной инстанции установлено, что база данных пользователей социальной сети «ВКонтакте» является базой данных по смыслу п. 2 ст. 1260 ГК РФ, поскольку представлена в объективной форме, содержит совокупность самостоятельных материалов о пользователях социальной сети, систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью ЭВМ.

Истец признан изготовителем базы данных в соответствии со ст. 1333 и 1334 ГК РФ, из которых следует, что он является лицом, организовавшим создание базы данных и работу по сбору, обработке и расположению составляющих ее материалов. При этом указанные нормы не ставят обязательным условием самостоятельное наполнение базы данных ее изготовителем: создание третьим лицам соответствующих условий для наполнения базы данных с осуществлением последующей обработки и расположения получаемых от этих лиц материалов также квалифицируется действующим законом в качестве действий, образующих правовой статус изготовителя базы данных.

Судебная коллегия согласилась с доводами общества «ВКонтакте» относительно того, что п. 1 ст. 1334 ГК РФ содержит опровержимую презумпцию существенности финансовых, материальных, организационных или иных затрат, произведенных в целях создания базы данных, если такая база содержит не менее десяти тысяч самостоятельных информационных элементов (материалов), составляющих содержание базы данных.

Согласно указанной норме необходимо исследовать не субъективное намерение лица на инвестирование непосредственно в базу данных, а объективную необходимость существенных затрат на ее создание.

На основании изложенного Суд по интеллектуальным правам согласился с выводами суда апелляционной инстанции о том, что из материалов дела усматривается наличие как объекта смежного права (базы данных пользователей социальной сети), так и исключительного права Истца на указанный объект.

В ходе указанного дела был рассмотрен вопрос и о правовом статусе Ответчика. Как пояснил Ответчик, его программное обеспечение обращается к общедоступной информации, размещенной пользователями в сети Интернет. Подобные «поисковые роботы» действуют по схеме, схожей с работой обычного браузера, переходя по определенным ссылкам и считывая содержимое страницы. При этом «поисковый робот» не получает непосредственного доступа к каким-либо базам данных, расположенным на серверах владельцев сайтов и не способен получать информацию, которая не отобразилась бы на странице пользователя при работе с ней при помощи обычного браузера.

Таким образом, программное обеспечение Ответчика не способно обработать информацию, которая отнесена в раздел закрытой и не является общедоступной в соответствии с выбранными пользователями настройками уровней конфиденциальности. Обрабатывая открытую информацию, опубликованную на разных сайтах в сети Интернет, программное обеспечение Ответчика является по сути поисковой системой (аналогичное программное обеспечение используется, в частности, такими поисковыми сервисами, как Google и Yandex).

Однако в суде апелляционной инстанции этот довод был оспорен. Так, Истец отмечает, что ссылки Ответчика на технические алгоритмы работы программного обеспечения, аналогичные действиям глобальных поисковых систем, не означают отсутствия состава нарушения исключительного права на базу данных, поскольку поисковые системы освобождаются от ответственности за нарушение исключительных прав правообладателей не в силу статуса «поисковика», а благодаря распространению на них нормы ст. 1253.1 ГК РФ и применению к ним статуса информационного посредника. Ответчик же, приравнивая свои действия к деятельности поисковых систем, не признает за собой статуса информационного посредника и не доказывает обстоятельства, способные при таком статусе освободить его от ответственности[1].

[1] Примечательно, что при повторном рассмотрении этого дела в суде первой инстанции 15 ноября 2019 г. суд определил назначить дополнительную судебную техническую экспертизу и поставить перед экспертами вопросы, в частности, о том, можно ли считать принцип работы Double Search (программное обеспечение Ответчика) аналогичным техническими принципами работы универсальных поисковых систем (таких как Яндекс, Гугл и т.п.) и можно ли признать, что с технической точки зрения Double Search является поисковой системой. Такое решение суда

Из материалов дела четко не усматривается, признает ли Ответчик себя информационным посредником, но примечательно, что в рамках одного дела поднимается вопрос об определении специального правового статуса сторон, который фактически может повлиять на исход дела. Действительно, правовой статус информационного посредника предполагает определенные особенности его ответственности (п. 2 ст.1253.1), в частности освобождение от ответственности при соблюдении совокупности законодательно закрепленных условий.

В пункте 77 Постановления Пленума Верховного Суда РФ от 23 апреля 2019 г. № 10 «О применении части четвертой Гражданского кодекса Российской Федерации»[1] указано, что особенности ответственности информационного посредника, предусмотренные ст. 1253.1 ГК РФ, являются исключением из правил, установленных п. 3 ст. 1250 ГК РФ, о применении мер ответственности (в виде возмещения убытков и выплаты компенсации) за нарушение интеллектуальных прав, допущенное нарушителем при осуществлении им предпринимательской деятельности, независимо от вины нарушителя.

Вместе с тем в литературе отмечается, что определения информационного посредника законодатель не дал, указав лишь на то, какие действия он может совершать[2]. Данный пробел также в некоторой степени восполнен в указанном постановлении Пленума Верховного Суда РФ, где говорится, что суд с учетом характера осуществляемой конкретным лицом деятельности устанавливает, является ли это лицо информационным посредником. Если лицо осуществляет деятельность, которая указана в ст. 1253.1 ГК РФ, то такое лицо признается информационным посредником в части осуществления данной деятельности.

В пункте 1 ст. 1253.1 ГК РФ указано, что лицо является информационным посредником, если оно предоставляет возможность доступа к материалу в информационно-телекоммуникационной сети, что соответствует описанию деятельности Ответчика. При этом в целях освобождения от ответственности за нарушение интеллектуальных прав ему как информационному посреднику, осуществляющему передачу материала в информационно-телекоммуникационной сети, предстоит доказать одновременное соблюдение условий, сформулированных в п. 2 ст. 1253.1 ГК РФ, а именно то, что:

отражает сложности в применении п. 20 ст. 2 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», где сформулировано законодательное определение поисковой системы.

[1] Российская газета. 2019. № 96.

[2] См.: Терещенко Л.К., Тиунов О.И. Информационные посредники в российском праве // Журнал зарубежного законодательства и сравнительного правоведения. 2016. № 6. С. 46–51.

1) он не является инициатором этой передачи и не определяет получателя указанного материала;

2) он не изменяет указанный материал при оказании услуг связи, за исключением изменений, осуществляемых для обеспечения технологического процесса передачи материала;

3) он не знал и не должен был знать о том, что использование соответствующих результата интеллектуальной деятельности или средства индивидуализации лицом, инициировавшим передачу материала, содержащего соответствующие результат интеллектуальной деятельности или средство индивидуализации, является неправомерным.

Таким образом, в процессе рассматриваемого дела не только уточняется правовой статус конкретных лиц, способный оказать влияние на исход дела, но и определяются признаки субъектов общественных отношений в сети Интернет, которые затем могут дополнить законодательные определения либо выявить новые грани правового статуса этих субъектов.

§ 3. Коммерческий оборот и правовые проблемы использования открытого доступа к персональным данным

В процессе судебного разбирательства Ответчик отстаивал свою позицию относительно правомерного использования данных пользователей социальной сети «ВКонтакте». Извлечение сведений из базы данных Истца осуществлялось Ответчиком по таким графам (полям) пользователей, как: фамилия, имя, сведения о месте работы, месте учебы, анкеты друзей, о населенном пункте рождения и регионе проживания, фотоизображения пользователя (т.н. аватар), а также сведения о частоте посещений страницы и типе устройства, которые используются пользователями для входа в социальную сеть. По мнению Истца, эти сведения составляли существенную часть базы данных пользователей социальной сети Истца, а в ходе объяснений генеральный директор Ответчика, по мнению Истца, подтвердил факт периодического обновления уже сформированной базы данных путем неоднократного и регулярного автоматизированного обращения к базе данных Истца и извлечения обновленных данных. Суд кассационной инстанции, однако, не согласился с тем, что извлечение данных из базы доказано, и это стало решающим моментом в направлении дела на новое рассмотрение.

Ответчик в суде первой инстанции обосновал тот факт, что поиск и обработка информации в его базе данных, созданной им на основе материалов из базы данных Истца, осуществляется с помощью про-

грамм для ЭВМ, разработчиком которых также является сам Ответчик: Программа для ЭВМ Social Attributes («Программа для получения скоринговых[1] переменных на основе информации о человеке, размещенной в общедоступных источниках данных сети Интернет) и Программа для ЭВМ Social Link («Программа для получения сводной информации о человеке, размещенной в общедоступных источниках данных сети Интернет, в едином веб-интерфейсе).

Общедоступные источники персональных данных определены в ст. 8 Закона о персональных данных как справочники, адресные книги. В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных. Перечисленные данные можно отнести к информации, идентифицирующей субъекта. В связи с этим возникает вопрос, можно ли базу данных, сформированную социальной интернет-сетью, рассматривать как своего рода «справочник» с набором идентификационных данных, когда очевидно, что информация в социальной сети намного разнообразней, включает массив очень личных данных, в том числе о состоянии здоровья, впечатлениях, предпочтениях, эмоциях и т.д., т.е. так или иначе отражает личную жизнь пользователя.

Мнения о доступности таких данных и возможностях их обработки — диаметрально противоположные. В литературе отмечается, что общедоступный источник данных представляет собой объект, где располагаются общедоступные данные (в том числе справочники, адресные книги)[2]. При этом в ст. 10 Закона № 152-ФЗ законодатель определяет действие субъекта персональных данных, которое должно выражаться либо в просьбе кому-либо разместить личные данные в месте, доступном для неограниченного круга лиц, либо в самостоятельном размещении этой информации. То есть действие субъекта персональных данных должно быть направлено на придание информации о себе общедоступности[3].

---

1 Скоринг — это система распределения базы клиентов на основании статистических данных. Это своеобразный финансовый помощник в определении потенциальной платёжеспособности клиента и оперативного оценивания, который сегодня широко применяется в банковской сфере. URL: https://bank-explorer.ru/kredity/skoring-chto-eto.html

2 См.: Федеральный закон «О персональных данных»: научно-практический комментарий (постатейный). Вып. 11 / под ред. А.А. Приезжевой // Российская газета. 2015; СПС «КонсультантПлюс».

3 Там же.

На основании п. 2 ч. 2 ст. 10 Закона № 152-ФЗ можно сделать вывод о том, в социальной интернет-сети персональные данные сделаны общедоступными самими субъектами персональных данных, если субъектом персональных данных не были активированы соответствующие настройки приватности. В этом случае доступ к личной информации разрешен для неограниченного круга лиц, такая информация будет являться общедоступной[1]. Это утверждение используется и в Правилах использования сайта «ВКонтакте», где указывается: поскольку Администрация Сайта осуществляет обработку персональных данных Пользователя в целях исполнения указанных Правил, в силу положений законодательства о персональных данных согласие Пользователя на обработку его персональных данных не требуется (п. 5.8).

Следует отметить, что в Правилах пользования сайта «ВКонтакте» указана возможность распоряжения персональными данными участника социальной сети со стороны администрации сайта. Так, п. 7.1.5 Правил устанавливает, что пользователь предоставляет Администрации Сайта неисключительное право использовать на безвозмездной основе размещенный на Сайте и принадлежащий ему на законных основаниях Контент в целях обеспечения Администрацией Сайта функционирования Сайта в объеме, определяемом функционалом и архитектурой Сайта, и отображения Контента в промоматериалах Администрации Сайта, в том числе в рамках изображений интерфейса Сайта, в том числе путем доведения таких промоматериалов до всеобщего сведения.

Таким образом, можно констатировать наличие согласия субъекта, который, присоединяясь к социальной интернет-сети, соглашается с условиями ее использования и получает услуги (сервисы) в обмен на свою информацию.

При этом следует подчеркнуть, что практика по использованию данных пользователей социальной интернет-сети была сочтена Роскомнадзором и судами противоречащей законодательству о персональных данных. В качестве аргумента было указано, что при отсутствии письменного согласия от пользователей нельзя гарантировать, что персональные данные были сделаны общедоступными именно с их согласия или по их воле, а следовательно, данные в социальных сетях не являются общедоступными и их обработка не может осу-

[1] Там же. Аналогичное мнение изложено и в работе «Научно-практический постатейный комментарий к Федеральному закону «О персональных данных» / А.И. Савельев. М., 2017 // СПС «КонсультантПлюс».

ществляться без согласия субъекта и в соответствии с п. 10 ч. 1 ст. 6 Закона о персональных данныхо»[1].

В Определении Верховного Суда РФ от 29 января 2018 г. № 305-КГ17-21291 отмечено: суды правомерно указали, что не являются общедоступными персональные данные, содержащиеся в открытых источниках (социальных сетях: ВКонтакте, Одноклассники, МойМир, Instragram, Twitter; интернет-порталов Авито и Авто.ру).

Размещение персональных данных в таких открытых источниках, исходя из положений Закона о персональных данных не делает их автоматически общедоступными. Таким образом, доводы о том, что согласия клиентов на обработку персональных данных не требуется, обоснованно отклонены судами.

Судами с учетом приведенных норм права и установленных по делу обстоятельств сделан обоснованный вывод о том, что персональные данные, обрабатываемые в социальных сетях не были сделаны общедоступными субъектом персональных данных в связи с чем, в действиях заявителя усматриваются нарушения ч. 3 ст. 22 и п. 1 ч. 1 ст. 6 Закона о персональных данных.

Таким образом, вывод судов о правомерности п. 1 и 4 предписания Управления Роскомнадзора по ЦФО № П-77/07/524-нд/1/230 соответствует фактическим обстоятельствам по делу и основан на правильном применении норм материального права.

Помимо согласия пользователей на обработку их персональных данных для обоснования правомерности использования их в коммерческом обороте важно учитывать также еще два условия:

1) цели использования персональных данных;

2) информированность пользователей о третьих лицах, которые могут иметь доступ к их персональным данным.

Позиция о необходимости учета целей, которые преследовал субъект, делая свои данные общедоступными, находит свое отражение в отечественной судебной практике. Так, суд признал недопустимым использование размещенного в сети Интернет номера телефона для звонков с целью погашения его задолженности по кредитному договору[2].

---

[1] См.: решение Арбитражного суда г. Москвы от 5 мая 2017 г. по делу № А40-5250/17-144-51, оставленное в силе в ходе последующих рассмотрений дела, в том числе в Верховном Суде РФ (Оопределение Верховного Суда РФ от 29 января 2018 г. № 305-КГ17-21291).

[2] Подробнее об этом см.: Савельев А.И. Направления регулирования Больших данных и защита неприкосновенности частной жизни в новых экономических реалиях // Закон. 2018. № 5. С. 122–144.

В литературе справедливо отмечается, что пользователи социальных сетей предоставляют свои данные социальной сети для целей общения со своими друзьями и другими участниками сети, а не для того, чтобы эти данные использовались впоследствии для определения их кредитного рейтинга. Такая обработка данных явно противоречит их разумным ожиданиям и принципу осуществления обработки на справедливой основе (ч. 1 ст. 5 Закона о персональных данных)[1].

Перечень третьих лиц, которым будут передаваться персональные данные, должен быть конкретным. В спорах банков с управлениями Роспотребнадзора апелляционные суды заняли одинаковую позицию: в тексте согласия на обработку персональных данных необходимо указать лиц, которым оператор вправе их передавать[2].

Таким образом, формально пользователь должен быть осведомлен о том, что его информация может быть передана третьим лицам. Проблема заключается в том, что узнать о них довольно затруднительно, если данные попадают в разряд общедоступных и сам сетевой ресурс не всегда знает, кто ими пользуется и на каких условиях. Более того, отзыв неисключительного права, упомянутый в п. 7.1.6 Правил, не учитывает свойства самой информации, распространение которой в сети ограничить практически невозможно, равно как и гарантировать защиту от искажения. Иными словами, отзыв неисключительного права, если и повлечет определенные последствия для тех, кто начал это право использовать, не повлияет на фактическую ситуацию с распространением (в частности, на коммерческой основе) данных пользователей.

По мнению представителей бизнес-сообщества, в силу особенностей закона — обязанности оператора доказывать наличие согласия субъекта на обработку данных — фактически нелегальным стал весь бизнес, связанный с продажей услуг и товаров через сеть Интернет, поскольку доказать авторство лица, заполнявшего веб-форму для получения запрашиваемой услуги, в условиях анонимности сети

---

1 См.: Савельев А.И. Направления регулирования Больших данных и защита неприкосновенности частной жизни в новых экономических реалиях // Закон. 2018. № 5. С. 122–144.

2 Постановление Девятого арбитражного апелляционного суда от 22 января 2018 г. № 09АП-66369/2017 по делу № А40-155310/17; постановление Одиннадцатого арбитражного апелляционного суда от 28 апреля 2018 г. № 11АП-4544/2018 по делу № А65-35933/2017; постановление Тринадцатого арбитражного апелляционного суда от 20 февраля 2018 г. № 13АП-34099/2017 по делу № А56-56720/2017; постановление Двадцатого арбитражного апелляционного суда от 11 января 2018 г. № 20АП-7785/2017 по делу № А09-12418/2017 // СПС «КонсультантПлюс».

Интернет, практически невозможно. Невыполнимыми представляются требования об оповещении оператором лица в случае, если персональные данные получены не от него, а от третьих лиц. Кроме того, условия трансграничной передачи персональных данных, определенные законом, полностью игнорируют современные реалии бизнеса, будь то бронирование авиабилетов в международных системах, передача вычислений «в облако» или получение приложения по запросу (SaaS). Особенности законодательства делают практически каждое юридическое или физическое лицо, обрабатывающее персональные данные, потенциальным нарушителем закона[1].

Еще одна проблема, сопутствующая коммерческому обороту информации, выявляется в процессе реализации ч. 2 ст. 8 Закона о персональных данных, где установлено, что сведения о субъекте персональных данных должны быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов. Однако при передаче (а в рассматриваемом деле при самовольном использовании) персональных данных третьими лицами обостряется проблема, связанная с использованием информационно-телекоммуникационной сети Интернет, а именно отсутствие возможности исключить какую-либо информацию по требованию субъекта персональных данных, равно как и по требованию любого другого субъекта, в частности изготовителя базы данных.

Это нашло отражение и в процессе рассмотрения спора ООО «ВКонтакте» и ООО «Дабл», когда суд апелляционной инстанции посчитал, что требование общества «ВКонтакте» об уничтожении со всех информационных носителей элементов, ранее извлеченных из базы данных пользователей социальной сети «ВКонтакте», не подлежит удовлетворению как неисполнимое.

В деле ООО «ВКонтакте» против ООО «Дабл» оценка правомерности обработки персональных данных не входила в предмет рассмотрения, однако в процессе исследования фактических обстоятельств возникло немало вопросов, которые имеют значения для решения принципиального вопроса о том, на каких основаниях, кем, в каком объеме данные участников социальной сети могут использоваться в коммерческом обороте. При этом происходит уточнение терминологии, соотнесение определений, закрепленных законодательно и

---

[1] Интервью с В.А. Сердюком, генеральным директором ЗАО «ДиалогНаука» и М.Ю. Емельянниковым, директором по развитию бизнеса компании «Информзащита» // СПС «КонсультантПлюс».

используемых субъектами предпринимательской деятельности в том числе для обоснования своих позиций в спорных ситуациях.

§ 4. Рынок персональных данных и вопросы антимонопольного регулирования в правоприменительной практике

В протокольном решении Экономического совета СНГ «О формировании конкурентной политики в государствах — участниках СНГ в условиях развития цифровой экономики»[1] со ссылкой на журнал The Economist отмечается, что новый сырьевой товар порождает привлекательную, быстрорастущую отрасль, наводя антимонопольных регуляторов на мысль вступить в игру и ограничить тех, кто контролирует его потоки. Подобные опасения вызывают гиганты, занимающиеся данными, — «нефтью цифровой эпохи» — Alphabet (материнская компания Google), Amazon, Apple, Facebook и Microsoft[2].

Следует отметить, что в отечественной правоприменительной практике уже имеются дела, в которых решаются вопросы, связанные с доминированием определенных интернет-ресурсов на рынке данных.

При рассмотрении дела между ООО «ВКонтакте» и ООО «Дабл» уже в суде кассационной инстанции Ответчик ссылается на злоупотребление Истцом своим правом и на неприменение судом апелляционной инстанции ст. 10 ГК РФ. Злоупотребление правом, по мнению Ответчика, выражается в попытке присвоения Истцом данных пользователей и ущемлении их прав, в противоречии публичного пользовательского соглашения общества «В Контакте» его действительному поведению, в нарушении права неопределенного круга лиц на общедоступную информацию. Кроме того, Ответчик полагает, что действия Истца направлены на монополизацию рынка пользовательских данных и являются недобросовестной конкуренцией.

Относительно этого довода о злоупотреблении Истцом правом при использовании базы данных пользователей социальной сети судебная коллегия отметила, что указанный довод ранее не заявлялся и не был предметом судебной оценки. При этом учитывая, что в

---

1 Принято в г. Москве 7 декабря 2018 г.

2 Если в 2011 г. список крупнейших компаний возглавляли четыре компании сырьевого сектора, то в 2018 г. все пять лидеров по капитализации — цифровые компании. Ежегодный рост капитализации цифровых гигантов составляет от 28% у Facebook до 58% у Alibaba Group (DogsoftheDow.com).

кассационной инстанции установлены основания для отмены судебных актов с направлением дела на новое рассмотрение в суд первой инстанции, Ответчик не лишен права заявить указанный довод при новом рассмотрении дела по существу.

Вопрос об определении объема рынка в сфере Интернета рассматривается в научной литературе. В частности, отмечается, что актуальным становится вопрос, по каким показателям следует определять объем товарного рынка и доли хозяйствующих субъектов в условиях цифровой реальности и нового типа услуг. Потребители-пользователи не платят за использование большинства крупных социальных сетей, следовательно, невозможно определить объем рынка и доли хозяйствующих объектов в денежном эквиваленте и традиционными методами. В связи с этим ставится вопрос о расширении видов показателей, по которым определяется объем товарного рынка применительно к рынку цифровой экономики[1].

В литературе встречается мнение о том, что в современной экономике многие сектора, в том числе социальные сети (важно, что они уже рассматриваются именно как сложившийся сектор экономики), не могут быть поняты, если смотреть на них через призму свободной конкуренции. В этих секторах преобладающей формой конкуренции является олигополия[2].

Примечательно, что при решении проблем монополии или олигополии на рынке информации речь идет не об увеличении числа интернет-площадок, которые могут предоставить пользователям конкурентоспособные сервисы для общения, самовыражения и т.д., а о доступе к данным, уже аккумулированным в готовых базах. С определенной долей условности можно утверждать, что современные социальные интернет-сети представляют собой некое подобие естественной монополии, а на практике решается вопрос о том, кто имеет право использовать ее преимущества и как при этом соблюсти правильный баланс интересов между участниками информационных процессов.

Помимо определения объемов рынка и его монополизации крупными интернет-компаниями возникает и другой вопрос — о недобросовестной конкуренции, который решается правоприменителями. Так, Федеральная антимонопольная служба выявила признаки

---

[1] Подробнее об этом см.: Писенко К.А., Гаспарян Э.Г. Актуальные вопросы правового обеспечения антимонопольной политики на цифровых финансовых рынках // Финансовое право. 2018. № 8. С. 34–38.

[2] См.: Stiglitz J.E. Monopoly's New Era // Project Syndicate. 2016. 13 May. URL: https://project-syndicate.org/commentary/high-monopoly-profits-persist-in-markets-by-joseph-e--stiglitz-2016-05.

недобросовестной конкуренции в действиях ООО «Айриэлтор». 12 февраля 2018 г. ФАС России выдала ООО «Айриэлтор», администрирующему сайт www.cian.ru, предупреждение о прекращении действий (бездействия), содержащих признаки нарушения п. 8 ст. 14 Федерального закона от 26 июля 2006 г. № 135-ФЗ «О защите конкуренции». В Федеральную антимонопольную службу поступило заявление ООО «КЕХ еКоммерц», которое также осуществляет деятельность по администрированию интернет-сайта Авито. На основании представленных документов Заявитель полагает, что общество копировало размещенные на сайте Авито объявления в сфере недвижимости и размещало их на сайте ЦИАН. Из материалов усматривается, что время размещения одних и тех же объявлений на обоих сайтах совпадает, а это может свидетельствовать об автоматическом форматировании и размещении объявлений (а не о самостоятельных действиях пользователей).

Также были выявлены и зафиксированы случаи, когда прикрепленные к объявлениям на Циан фотографии содержали полные либо частично затертые цифровые водяные знаки Авито. Антимонопольное ведомство пришло к выводу, что перечисленные в заявлении действия ООО «Айриэлтор» направлены на копирование сайтом Циан с сайта Авито объявлений с целью их последующего размещения. Это может предоставить Циану конкурентное преимущество и приводить к увеличению доходов. При этом могут сокращаться доходы и клиентская база Авито, поскольку спрос перетекает на копирующую платформу. На основании установленных фактов ФАС России выдала ООО «Айриэлтор» предупреждение о прекращении действий (бездействия), содержащих признаки нарушения антимонопольного законодательства, и принятии мер по устранению последствий такого нарушения[1].

Данный вопрос нашел отражение в законодательной инициативе, которая разрабатывалась Центром компетенций автономной некоммерческой организации «Цифровая экономика» (ЦЭ), возглавляемый фондом «Сколково». По мнению авторов концепции, любое юридическое ограничение доступа к общедоступной информации создаст неравные условия для отечественных и зарубежных игроков рынка данных. Как говорится в концепции, закрытие данных и присвоение их площадкам фактически приведет к монополизации рынка, поскольку площадки сами являются активными игроками рынка данных[2].

---

1 URL: https://fas.gov.ru/news/24285

2 URL: https://ria.ru/20181119/1533052756.html

В результате можно констатировать дуализм в отношении оценок рынка данных, который обусловливает неопределенность правового положения участников коммерческого оборота, разработчиков информационно-телекоммуникационных сервисов, пользователей и государственных структур. Полагаем, что именно развивающаяся судебная и иная правоприменительная практика будет способствовать преодолению этой неопределенности и поиску подходов к сбалансированному регулированию, направленному на защиту прав и свобод участников рынка.

* * *

Таким образом, в рассмотренных примерах, в частности в деле по иску ООО «ВКонтакте» к ООО «Дабл», изначально направленном на защиту прав субъекта предпринимательской деятельности в части использования информации (персональных данных) в коммерческом обороте, выявляются следующие проблемы, сопутствующие дальнейшему развитию коммерческого оборота персональных данных и технологии big data (суть которых — обработка персональных данных):

1) решение вопроса о том, должен ли субъект коммерческого оборота, который инициировал сбор и агрегацию персональных данных, вложив при этом собственные финансовые и иные средства, обладать особым правовым статусом, позволяющим ему, по крайней мере, информировать пользователей/участников своего ресурса о том, кем и каким образом используются их персональные данные, поскольку такое требование заложено в законодательстве о защите персональных данных;

2) уточнение определения и правового режима общедоступных данных, обработка и коммерческий оборот которых субъектами предпринимательства на равных условиях в настоящее время ставит под сомнение возможность исполнения законных требований относительно защиты персональных данных. В литературе этот вопрос уже поднимался. В частности, по мнению Л.К. Терещенко, юридические и технические требования, устанавливаемые в целях защиты персональных данных, прав физических лиц и законных интересов юридических лиц, должны быть сбалансированы и адекватны, чтобы не создавать помех развитию рынка, с одной стороны, и нарушения интересов субъектов персональных данных — с другой[1];

---

[1] См.: Терещенко Л.К. Государственный контроль в сфере защиты персональных данных // Право. Журнал Высшей школы экономики. 2018. № 4. С. 142–161; Ее же. Правовой режим персональных данных и безопасность личности // Закон. 2013. № 6. С. 36–43; Ее же. О соблюдении баланса интересов при установлении мер защиты персональных данных // Журнал российского права. 2011. № 5. С. 5–11.

3) совершенствование условий пользовательского соглашения или иных документов, устанавливающих правила пользования сайтами (возможно введение обязательных унифицированных условий), которые могут играть важную роль при разрешении конкретных судебных дел;

4) решение вопроса о соотношении права на свободу предпринимательской деятельности и права на защиту персональных данных как составляющей фундаментального права на неприкосновенность частной жизни, личную и семейную тайну в условиях расширяющихся технологических возможностей;

5) определение положения хозяйствующих субъектов на современном рынке персональных данных, поиск правовых регуляторов, способных обеспечить баланс интересов участников коммерческого оборота, защиту их прав и свобод, а также дальнейшее развитие информационно-телекоммуникационных ресурсов, имеющих важное значение в становлении информационного общества.

Глава 5
СУДЕБНАЯ ЭКСПЕРТИЗА ПО ДЕЛАМ О ЗАЩИТЕ ИНТЕЛЛЕКТУАЛЬНЫХ ПРАВ НА БАЗУ ДАННЫХ

По делам о защите исключительных прав на базу данных, связанным с обработкой, содержащейся в них информации с использованием технологий Big Data, особое внимание следует уделить судебным экспертизам. В рамках упомянутого дела по иску «Вконтакте» против ООО «Дабл» (А40-18827/17-110-180) Суд по интеллектуальным правам отметил: «При возникновении у судов сомнений в технических принципах работы программы общества «ДАБЛ» при квалификации действий указанного общества в качестве нарушения исключительного права изготовителя базы данных суды, рассматривающие дело по существу, могли предложить к обсуждению сторон, в том числе, вопрос о назначении экспертизы». По состоянию на ноябрь 2019 г. до сих пор ведутся споры о кандидатурах экспертов, при этом экспертам было поставлено 59 вопросов, большая часть из которых направлена на квалификацию Dubble Search, системы обработки информации с сайта «Вконтакте», в качестве поисковой системы[1]. Множество поставленных вопросов по данному делу носит сугубо технический характер, что вытекает из роли эксперта как лица, обладающего специальными знаниями. При этом для прогнозирования дальнейшего порядка разрешения подобных дел следует проанализировать, как суды смотрят на экспертные заключения, которые они в силу процессуальных норм должны оценивать наряду с другими доказательствами и оценку которым они могут дать в судебном акте.

Во всех случаях нарушения авторских прав истец в силу распределения бремени доказывания между сторонами должен доказать, что ответчик скопировал исходный код истца, который защищен авторским правом. Это основной момент, потому что копирование не всегда является нарушением: часть того, что скопировано, может быть просто идеями, процессами, фактами, находящимися в общественном достоянии и потому разрешенными к копированию. Из-за специфики программного обеспечения, его разработки, внедрения, применения суду зачастую не просто установить тот или иной факт

[1] Подробнее об этом см.: § 4 настоящего комментария.

по делу без проведения экспертизы. Задачей экспертизы является точное установление сведений о фактах, имеющих значение для правильного разрешения дела, и фактических обстоятельств, данные о которых требуют специальных познаний эксперта. Для экспертного исследования привлекаются квалифицированные специалисты, которые на основании этого исследования выдают обоснованное заключение о причастности исследуемого программного комплекса к нарушению законодательства. Согласно п. 1 ст. 82 Арбитражного процессуального кодекса (далее — АПК РФ) экспертиза назначается по ходатайству лица, участвующего в деле. Если же экспертиза предписана законом или предусмотрена договором либо необходима для проверки факта фальсификации представленных доказательств арбитражный суд может назначить экспертизу по своей инициативе. Повторная и дополнительная экспертиза также может быть назначена судом.

Экспертизы в сфере интеллектуальной собственности в большинстве своем не вошли в Перечень родов (видов) экспертиз, выполняемых в судебно-экспертных учреждениях Минюста России, приведенный в приложении № 1 к приказу Минюста России от 27 декабря 2012 г. № 237 «Об утверждении Перечня родов (видов) судебных экспертиз, выполняемых в федеральных бюджетных судебно-экспертных учреждениях Минюста России, и Перечня экспертных специальностей, по которым предоставляется право самостоятельного производства судебных экспертиз в федеральных бюджетных судебно-экспертных учреждениях Минюста России»[1]. При назначении экспертиз в ходе разрешения спора о защите базы данных чаще других применяются: судебная компьютерно-техническая экспертиза, судебная техническая комиссионная экспертиза, комплексная судебная экспертиза, патентная экспертиза.

§ 1. Судебная компьютерно-техническая экспертиза

Суд по интеллектуальным правам рассмотрел дело № А56-46858/2017[2]. ООО «Марин Трейдинг» (далее — истец) обратилось в Арбитражный суд города Санкт-Петербурга и Ленинградской области с заявлением, уточненным в порядке ст. 49 АПК РФ, к ООО «Промарин» (далее — ответчик) об обязании ответчика удалить с сайта https://promarine.ru элементы, совпадающие с элементами на

---

1 Российская газета. 2013. № 24. 6 февраля.

2 Постановление Суда по интеллектуальным правам от 22 января 2019 г. по делу № А56-46858/2017 // СПС «Консультант Плюс».

сайте http://nwmotors.ru, и прекратить нарушение прав истца, в том числе 93 фотографий обозначенных в протоколе осмотра от 23 января 2018 г. и экспертном заключении от 1 июня 2017 г., а также о взыскании 5 млн руб. компенсации и 30 тыс. руб. расходов на проведение экспертизы. На основании заключения специалистов от 1 июня 2017 г. № 2577/10/И истец установил, что оформление сайта, база данных и структура сайта ответчика аналогична оформлению, структуре сайта и базе данных истца. Суд удовлетворил требования частично, присудив 100 тыс. руб. компенсации и 6 957 руб. расходов по оплате государственной пошлины[1].

Тринадцатый арбитражный апелляционный суд[2] на основе компьютерно-технической экспертизы изменил решение Арбитражного суда города Санкт-Петербурга и Ленинградской области.

Апелляционным судом по делу была назначена судебная компьютерно-техническая экспертиза, по результатам ее проведения представлено заключение от 26 марта 2018 г. № 18-2-Т-А56-46858/2017, согласно которому установлено наличие в оформлении сайта https://promarine.ru среди графических изображений товаров каталога элементов, визуально совпадающих с оформлением сайта http://nwmotors.ru. При этом элементы, выявленные в процессе исследования, появились ранее на сайте http://nwmotors.ru[3]. Суд обязал общество ответчика удалить со своего сайта элементы, совпадающие с элементами на сайте истца. Также суд обязал взыскать ответчика пользу истца 930 тыс. руб. компенсации и 14 928 руб. расходов по оплате государственной пошлины. В остальной части в удовлетворении иска отказал.

Не согласившись с размером компенсации по настоящему делу, истец обратился в Суд по интеллектуальным правам, который изучив материалы дела и согласившись с доводами истца, отправив дело на новое рассмотрение в арбитражный суд первой инстанции.

На основании этого примера можно сделать следующие выводы:

1) судебная компьютерно-техническая экспертиза — это самостоятельный вид судебной экспертизы, проводимый для выявления и дальнейшего всестороннего изучения компьютерной информации (информационных объектов). В процессе изучения устанавливаются

---

1 Решение Арбитражного суда города Санкт-Петербурга и Ленинградской области от 31 мая 2018 г. по делу № А56-46858/2017 // СПС «Консультант Плюс».

2 Постановление Тринадцатого арбитражного апелляционного суда от 26 октября 2018 г. № 13АП-18252/2018 по делу № А56-46858/2017 // СПС «Консультант Плюс».

3 Там же.

закономерности и сходства исследуемых объектов, имеющие значение для рассмотрения дела, поскольку они могут свидетельствовать о копировании одного объекта другим. При помощи судебной компьютерно-технической экспертизы могут быть выявлены элементы, демонстрирующие первенство в разработке в сети Интернет одного из исследуемых объектов;

2) полученные благодаря судебной компьютерно-технической экспертизе результаты используются для установления истины по делу и могут способствовать установлению и увеличению размеров компенсации, а также возмещению расходов на оплату государственной пошлины.

С точки зрения проведения экспертизы и ее выводов интересно дело Суда по интеллектуальным правам № А56-21040/2015[1]. ООО «Дата МАТРИКС» обратилось в Арбитражный суд города Санкт-Петербурга и Ленинградской области с исковым заявлением к ООО «ДатаФлоу Солюшенс» с требованием о пресечении действий, нарушающих исключительное право истца на программу для электронно-вычислительных машин MATRIX EDC, а именно о запрете ответчику использовать программу для ЭВМ Dataflow EDC. Суд первой инстанции отказал в удовлетворении иска. Тринадцатый арбитражный апелляционный суд решение суда первой инстанции отменил, удовлетворив исковые требования в полном объеме[2]. Для разрешения вопроса о соотношении противопоставленных программ для ЭВМ по области применения, принципу действия, а также о наличии заимствований в их исходных кодах апелляционным судом была назначена судебная компьютерно-техническая экспертиза (далее — СКТЭ). С учетом выводов экспертизы суд установил, что в программе для ЭВМ MATRIX EDC воспроизведено как минимум 88% кода программы для ЭВМ Dataflow EDC, что фактически говорит о модификации ответчиком программы для ЭВМ, права на которую принадлежат истцу. Суд по интеллектуальным правам это решение поддержал. Примечательно, что СКТЭ путем сравнения исходных кодов истца и ответчика способна установить факт 88%-го совпадения программных кодов в данном деле.

Таким образом, СКТЭ позволяет установить схожесть изучаемых объектов и построить доказательную базу путем окончательного

---

1 Постановление Суда по интеллектуальным правам от 21 ноября 2016 г. № С01-328/2016 по делу № А56-21040/2015 // СПС «Консультант Плюс».

2 Постановление Тринадцатого арбитражного апелляционного суда от 14 июля 2016 г. № 13АП-20954/2015 по делу № А56-21040/2015 // СПС «Консультант Плюс».

разрешения большинства вопросов, связанных с компьютерной информацией. Задачами исследования являются поиск, выявление, изучение и оценка информации, подготовленной пользователем или созданной программами для организации информационных процессов в компьютерной системе.

§ 2. Судебная техническая комиссионная экспертиза

Судебная комиссионная экспертиза назначается по усмотрению суда с привлечением экспертов одной специальности. Комиссионная экспертиза назначается в особо сложных случаях или в случае проведения повторной экспертизы для повышения объективности.

ООО «Лайф» приобрело у ООО «НОРБИТ» права на пользование программы для ЭВМ «Портал «Интернет-факторинг», позволяющей осуществлять покупку и продажу дебиторской задолженности, путем проведения электронного аукциона уплатив сумму в размере 4 400 000 руб. При этом сумма вознаграждения за права пользования ЭВМ составляет 4 800 000 руб., ввиду чего ООО «НОРБИТ» обратилось в Арбитражный суд города Москвы с исковым заявлением к ООО «Лайф» (далее — общество, лицензиат) о взыскании суммы основного долга в размере 400 000 рублей. Общество «Лайф» обратилось со встречным исковым заявлением к обществу «НОРБИТ» с указанием на то обстоятельство, что ООО «НОРБИТ» ненадлежащим образом исполнил обязательство по передаче неисключительного права на использование программы ЭВМ, поскольку программа не соответствует характеристикам и функциональным возможностям, позволяющим получать результат, в котором ООО «Лайф» было заинтересовано при заключении договора, в связи с чем ему причинены убытки в размере перечисленной обществу «НОРБИТ» суммы.

Судом по делу была назначена судебная техническая комиссионная экспертиза, проведение которой было поручено экспертам С.А. Красинскому и Ю.В. Волкову.

По итогам проведения судебной технической комиссионной экспертизы С.А. Красинским были выявлены недостатки программы, которые делают ее непригодной для предусмотренного в договоре использования.

Экспертом были сделаны следующие выводы:

– программа не позволяет пройти процедуру регистрации и осуществлять ввод информации в систему от клиента по договорам дебиторской задолженности;

– программа не позволяет подписывать вносимую клиентом информацию электронной подписью (ЭП);

– программа препятствует получению доступа к информации ввиду невозможности первоначальной загрузки;

– система не позволяет осуществлять покупку дебиторской задолженности из-за отсутствия возможности создания учетной записи для участников торгов и договоров, сопровождающих процедуру сделки;

– невозможно сравнить функциональные возможности учетных записей с ролью заказчика и инвестора;

– программа не предоставляет возможность доступа к сведениям о дебиторской задолженности (Лоту), выставленной клиентом на торги, ввиду невозможности создания такого лота;

– система не позволяет осуществить подготовку к проведению электронного аукциона и т.д.

Общество «НОРБИТ» полагает, что эксперт С.А. Красинский пришел к неправильным выводам, поскольку элементы указанной программы им были установлены не в полном объеме.

Эксперт Ю.В. Волков на все вопросы, поставленные судом, дал положительные ответы, отметив, что программа для ЭВМ позволяет пройти процедуру регистрации, получить доступ к информации, осуществить покупку дебиторской задолженности и т.д. Но в то же время программа не позволяет осуществить подготовку к проведению электронного аукциона в связи с ограничениями, программа не содержит полей «минимальный размер первого платежа» и «максимальный размер комиссии» в объявлении о продаже, что является основным атрибутом подготовки электронного аукциона[1]. В материалах дела имеется сравнительная схема, позволяющая прийти к выводу, что в программе не реализован основной принцип торговли дебиторской задолженностью (принцип АУКЦИОНА)[2]. Ю.В. Волков также пришел к выводу, что функционал и основные бизнес-цели программы для ЭВМ не соответствуют требованиям, в связи с чем не позволяют получить того результата, в котором лицензиат был заинтересован.

Приведенный пример демонстрирует следующее:

1) комиссионная техническая экспертиза — производится не менее чем двумя экспертами одной специальности либо в одной области знания, применяющими разные методы исследования. Если по результатам проведенных исследований мнения экспертов по поставленным вопросам расходятся, то каждый из экспертов дает от-

---

[1] Постановление Девятого арбитражного апелляционного суда от 24 мая 2016 г. № 09АП-17465/2016-ГК по делу № А40-105969/14 // СПС «Консультант Плюс».

[2] Там же.

дельное заключение по вопросам, вызвавшим разногласие (ст. 83 ГПК РФ, ст. 200 Уголовно-процессуального кодекса РФ (далее — УПК РФ), ст. 84 АПК РФ, ст. 80 Кодекса административного судопроизводства РФ (далее — КАС РФ);

2) комиссионная техническая экспертиза позволяет взыскать убытки и установить факт ненадлежащего исполнения обязательств по передаче права на использование программы ЭВМ одной из сторон.

Особенностью производства технических комиссионных экспертиз является тот факт, что нескольким экспертам бывает тяжело прийти к единому мнению относительно предмета экспертизы. Вследствие чего особого внимания заслуживает решение суда в ситуации, когда эксперты придерживаются различных точек зрения и приходят к разным заключениям.

Суд по интеллектуальным правам рассматривал дело № А40-149313/2013[1], где истец является разработчиком и изготовителем компьютерного программного обеспечения, обладателем исключительных авторских прав на программу для электронно-вычислительных машин. По мнению истца, программы для ЭВМ, зарегистрированные за ответчиком, являются незаконно модифицированными версиями программы, правообладателем которой является истец.

Для разрешения дела была назначена судебная техническая комиссионная экспертиза с привлечением двух экспертов — И.И. Титовой и П.А. Богданова. Экспертам были предоставлены зарегистрированные в Роспатенте исходные коды спорных программ, которые являются надлежащими объективными доказательствами исходных текстов, для сравнения программ для ЭВМ истца и ответчика.

П.А. Богданов пришел к заключению о невозможности сделать вывод о том, являются ли программы для ЭВМ ответчика результатом самостоятельной разработки либо модификации программы для ЭВМ истца.

Эксперт И.И. Титова пришла к выводам о том, что представленные фрагменты программы для ЭВМ, право на которую зарегистрировано за ответчиком, «являются результатом самостоятельной разработки, так как элементы языка программирования, особенности их синтаксиса, особенности взаиморасположения элементов языка программирования в представленных на исследование фрагментах программного кода являются уникальными, в своей совокупности не совпадают с фрагментом программного кода программы для

---

[1] Постановление Суда по интеллектуальным правам от 1 марта 2016 г. № С01-1234/2015 по делу № А40-149313/2013 // СПС «Консультант Плюс».

ЭВМ»[1] истца. Суд по интеллектуальным правам пришел к выводу о недоказанности истцом использования ответчиком спорной программы.

§ 3. Комплексная судебная экспертиза

Комплексная экспертиза назначается, если установление обстоятельств по делу требует одновременного проведения исследований с использованием различных областей знания или с использованием различных научных направлений в пределах одной области знания.

Комплексная экспертиза поручается нескольким экспертам. В гражданском судопроизводстве по результатам проведенных исследований эксперты формулируют общий вывод об обстоятельствах и излагают его в заключении, которое подписывается всеми экспертами; эксперты, которые не участвовали в формулировании общего вывода или не согласны с ним, подписывают только свою исследовательскую часть заключения (ч. 2 ст. 82 ГПК РФ). В иных видах судопроизводства каждый эксперт, участвовавший в проведении комплексной экспертизы, подписывает ту часть заключения, которая содержит описание проведенных им исследований, и несет за нее ответственность (ч. 2 ст. 85 АПК, ч. 2 ст. 201 УПК РФ, ч. 3 ст. 81 КАС РФ).

Суд по интеллектуальным правам рассмотрел дело № А56-92673/2016. ООО «ВИАКАРД» обратилось в Арбитражный суд с иском к ООО «Терминал Сервис» о взыскании задолженности по договору процессинга, неустойки и убытков по указанному договору, а также о взыскании компенсации за нанесение вреда деловой репутации. Решением Арбитражного суда от 26 апреля 2018 г. исковые требования удовлетворены частично. Постановлением Тринадцатого арбитражного апелляционного суда от 11 июля 2018 г.[2] решение Арбитражного суда первой инстанции от 26 апреля 2018 г. изменено.

Из материалов дела следует, что ООО «ВИАКАРД» является правообладателем программно-аппаратного комплекса. На основании договора ООО «ВИАКАРД» произвел установку оборудования, а также оказал ООО «Терминал Сервис» услуги процессинга, но ООО «Терминал Сервис» не произвел оплату оказанных услуг. Кроме того, последний предоставил доступ к системе истца неограниченному

---

1 Постановление Суда по интеллектуальным правам от 1 марта 2016 г. № С01-1234/2015 по делу № А40-149313/2013 // СПС «Консультант Плюс».

2 Постановления Тринадцатого арбитражного апелляционного суда от 11 июля 2018 г. № 13АП-12611/2018, № 13АП-14220/2018 по делу № А56-92673/2016 // СПС «Консультант Плюс».

кругу лиц, тем самым нарушив договор о неразглашении конфиденциальной информации, заключенный между сторонами.

Материалами дела также установлено, что во исполнение условий договора процессинга на основании акта приема-передачи терминалов от 25 июня 2014 г. на точке обслуживания общества «Киришиавтосервис» ООО «ВИАКАРД» установлено оборудование (терминал № 81712374) с программным комплексом, блоком питания и sim-картами.

Между тем в период с 5 июля 2016 г. по 18 июля 2016 г. по sim-карте (МТС), установленной на терминале № 81712374, установлено изъятие из терминала и установка на иное устройство, с которого осуществлено потребление объема трафика передачи данных. При этом изъятие sim-карты является видоизменением программно-аппаратных средств, что является нарушением условий договора[1].

Данное изъятие подтверждено заключением судебной компьютерной технической экспертизы № 9619/Ц.

Экспертом установлено и отражено в заключении, что данные, содержащиеся в Системе ООО «ВИАКАРД», позволяют определить серийные номера терминалов, которые использовались ООО «Терминал Сервис» при исполнении договора процессинга. В заключении эксперт указал на использование 992 терминалов, из них 875 терминалов принадлежит ООО «ВИАКАРД» на праве собственности, что подтверждает соответствующая документация (договоры с поставщиками, счета-фактуры, товарные накладные, а также платежные поручения на оплату терминалов). ООО «ВИАКАРД» утверждает, что 875 терминалов 718 приобретено у ООО «Торговый дом «ЧИН-РУ», с чем не согласился ООО «Терминал Сервис», предоставив счет-фактуру в нижнем левом углу которого имеются две подписи, выполненные от имени генерального директора ООО «ВИАКАРД». В указанном счете-фактуре сказано, что ответчик получил всего 500 терминалов, которые в дальнейшем реализовал.

Директор ООО «ВИАКАРД» представил в суд заявление о фальсификации счета-фактуры. В целях проверки заявления о фальсификации доказательства судом назначена почерковедческая экспертиза с постановкой следующего вопроса: кем выполнена подпись от имени директора в счете-фактуре?

Согласно заключению эксперта две подписи директора на счете-фактуре выполнены не им самим, а иным лицом с подражанием подлинной подписи и предварительной тренировкой.

Требование ООО «ВИАКАРД» частично удовлетворено, поскольку установлен факт нарушения ООО «Терминал Сервис» условия

---

[1] Там же.

соглашения о конфиденциальности и исключительных прав истца на программно-аппаратный комплекс.

Таким образом, осуществляя комплексную экспертизу, каждый эксперт проводит исследования в пределах своих специальных знаний, указывает, какие исследования и в каком объеме были проведены, какие факты установлены и какие выводы были сделаны.

Качество заключения при проведении комплексной экспертизы напрямую зависит от ряда условий:

– полноты применения методических приемов, доступных экспертам различных специальностей. Объединение их усилий дает синергетический эффект в отношении анализа документальных и учетно-аналитических данных, зафиксированных при помощи средств автоматизации;

– всеобъемлющего характера исследования всей представленной информации для проведения экспертных действий в рамках процессуальных норм и правил;

– объективной оценки представленных для экспертного исследования материалов, исключающих неоднозначное понимание сделанных выводов.

§ 4. Патентная экспертиза

Следующая экспертиза относится к оценке патентоспособности изобретения. Патентная экспертиза — экспертиза, рассматривающая заявки на выдачу патента, а также споры о действительности патента.

Речь идет о методологических подходах Роспатента, который не относит компьютерную систему управления данными, результат при использовании которой достигается благодаря применению программы для ЭВМ (и используемого в ней алгоритма), к изобретениям. Роспатент отмечает, что данные изобретения не патентоспособны, поскольку признаки этого изобретения характеризуют работу компьютера, определяемую программой для ЭВМ.

Интерес представляет решение Суда по интеллектуальным правам № СИП-164/2013[1] с точки зрения задаваемых эксперту вопросов.

Экспертам, имеющим техническое образование, были заданы уточняющие вопросы о том, можно ли отнести отличительные признаки указанных изобретений к «представлению информации» и являются ли обеспечиваемые этими изобретениями результаты техническими?

---

[1] Постановление Президиума Суда по интеллектуальным правам от 6 марта 2014 г. № С01-422/2013 по делу № СИП-164/2013 // СПС «Консультант Плюс».

Один из специалистов, отвечая на этот вопрос, отметил, что изобретение не имеет технической характеристики. Второй эксперт ответил следующее:

«– формула изобретения не содержит сведений о каких-либо технических решениях, связанных со структурой и принципом функционирования систем, обеспечивающих такое хранение;

– форма представления информации, указанная автором как совместная, реализуется решениями, не относящимися к предъявленному изобретению, значит и не гарантируется данным изобретением;

– помимо этого уже существуют и предъявлены для всеобщего доступа информационные системы, хранящие темпоральные данные, представленные в формуле изобретения;

– заявка не соответствует требованиям достижимости технического результата, поскольку в ней не приведена неразрывная причинно-следственная связь между предложенным способом хранения и составом темпоральных данных и результатом: функциональностью изделия, скоростью доступа к данным, скоростью разработки управляющих программ, объемом памяти, поддержки целостности данных»[1].

Разъяснения второго специалиста можно оценить как имеющие отношение к сущности данного спора только в первой и четвертой из перечисленных позиций»[2].

По справедливому замечанию В.А. Мещерякова, из перечисленных позиций эксперта к сущности данного спора можно отнести только первую и четвертую позицию.

Некорректно заданные вопросы экспертам с техническим образованием в сфере патентного права противоречат доктринальной презумпции «судьи знают право»[3], поэтому считается, что не должна назначаться экспертиза для познания вопросов права.

§ 5. Правовая экспертиза: практика привлечения специалистов

Устанавливая круг и содержание вопросов, по которым необходимо провести экспертизу, суд исходит из того, что недопустима постановка перед экспертом вопросов права, правовых последствий

---

1 Постановление Президиума Суда по интеллектуальным правам от 6 марта 2014 г. № С01-422/2013 по делу № СИП-164/2013 // СПС «Консультант Плюс».

2 Мещеряков В.А. Первые итоги работы Суда по интеллектуальным правам: взлеты и падения, общий вектор развития. Ч. 2 // Журнал Суда по интеллектуальным правам. 2016. № 11. С. 118–119.

3 Треушников М.К. Судебные доказательства. М., 1997. С. 320.

и оценки доказательств[1]. Однако на практике часто бывает, что эксперту задаются вопросы правового характера наряду со специальными. В учебном пособии[2] по расследованию правонарушений о нарушении авторских и смежных прав на произведения, охраняемые авторским правом, приводятся вопросы, взятые из реальных судебных дел: «являются ли экземпляры произведений... контрафактными?», «кому принадлежат авторские права на использование данного произведения», «кто является субъектом авторского права (владелец или составитель журнала)», «были ли нарушены права патентообладателя при изготовлении представленных образцов или хотя бы одного из них», «если патентные права были нарушены, то каков размер причиненного материального ущерба».

Указанные вопросы не носят узкоспециального характера, а имеют вполне конкретное правовое содержание и должны быть адресованы не специалисту, а суду. Чтобы исключить правовое содержание, эти же вопросы должны быть сформулированы иначе. К сожалению, на практике экспертам приходится в рамках экспертизы заниматься анализом правоустанавливающих документов, прослеживать в предоставленных материалах правовую связь (правопреемство) от первоначального владельца прав к лицу, предъявляющему претензию, либо запрашивать недостающие документы через суд, например, когда в материалах дела присутствуют незаверенные копии договоров, вызывающие сомнение, отсутствуют доверенности, нет документов, подтверждающих наличие прав или отдельных правомочий. И если эксперт при проведении экспертизы не обратит внимание на отсутствие необходимых для установления фактов документов возможно возникновение оснований для оспаривания решения суда.

В.А. Мещеряков отмечает, что привлекая экспертов с техническим образованием к экспертизе необходим компетентный «консультант — корректор», который сумеет правильно сформулировать вопросы, исключая установление юридических фактов, по которым необходимо подготовить ответы. Автор также считает, что привлечение в Суд по интеллектуальным правам судей-специалистов, имеющих двойное образование — техническое и юридическое, может стать выходом из сложившейся ситуации[3]. Хотелось бы отметить, что

---

1 Постановление Пленума ВАС РФ от 4 апреля 2014 г. № 23 (п. 8) // Вестник ВАС РФ. 2014. № 6.

2 Расследование преступлений о нарушении авторских и смежных прав. Особенности / под общ. ред. Т.А. Боголюбовой. М., 2001. С. 64.

3 Мещеряков В.А. Указ. соч. С. 119.

выводы автора заслуживают внимания, поскольку, например, в Роспатенте решения о выдаче или об отказе в выдаче патента принимают люди, обладающие квалификацией и специальными знаниями. Вместе с тем излишняя специализация судей не встраивается в логику развития российской судебной системы.

Еще в 2015 г. Л.А. Новоселова отмечала, что следует уточнить норму закона — «лица, участвующие в деле, не должны задавать эксперту вопросы о содержании права»[1]. При этом эксперту должны быть заданы вопросы только специального характера. Однако на практике это требование по-прежнему не соблюдается[2].

Возможно, частично решить проблему поможет привлечение специалиста. Согласно Постановлению Пленума ВАС РФ от 8 октября 2012 г. № 60[3] «Суду по интеллектуальным правам как специализированному арбитражному суду на основании части 1.1 статьи 16 АПК РФ в целях получения разъяснений, консультаций и выяснения профессионального мнения ученых, специалистов и прочих лиц, обладающих теоретическими и практическими познаниями по существу разрешаемого специализированным арбитражным судом спора, предоставлено право направлять запросы»[4]. В Справке о некоторых вопросах привлечения специалистов и направления запросов Судом по интеллектуальным правам[5] также говорится, что специалист как самостоятельная процессуальная фигура, обладающая специальными познаниями, может оказывать независимую помощь Суду по интеллектуальным правам в понимании обстоятельств дела, требующих специализированных теоретических и практических знаний[6]. А.В. Ковалева отмечает, что специалистом может быть любое дееспособное лицо, обладающее необходимыми специальными зна-

---

1 Суд по интеллектуальным правам в системе органов государственной власти Российской Федерации: монография / И.А. Близнец, К.Ю. Бубнова, О.В. Видякина и др.; под ред. И.А. Близнеца, Л.А. Новоселовой. М., 2015. С. 60.

2 См., например: Постановление Арбитражного суда Западно-Сибирского округа от 14 сентября 2018 г. № Ф04-3571/2018 по делу № А27-554/2017 // СПС «Консультант Плюс»; Постановление Арбитражного суда Центрального округа от 25 апреля 2019 г. № Ф10-1108/2019 по делу № А08-6080/2016 // СПС «Консультант Плюс».

3 Журнал Суда по интеллектуальным правам. 2013. Октябрь.

4 Постановление Пленума ВАС РФ от 8 октября 2012 г. № 60 // Журнал Суда по интеллектуальным правам. 2013. Октябрь.

5 СПС «Консультант Плюс».

6 См.: Справка о некоторых вопросах привлечения специалистов и направления запросов судом по интеллектуальным правам // СПС «Консультант Плюс».

ниями, соответствующей квалификацией и опытом практической работы[1].

Так, например, в деле № СИП-926/2014[2], в рамках которого оспаривалась правомерность отказа в выдаче патента, был привлечен специалист, доктор юридических наук, обладающий специальными знаниями в области права.

Роспатент отказал в выдаче патента на полезную модель «Система автоматического определения нарушений правил парковки», руководствуясь тем, что полезная модель в совокупности представляет собой распределительную информационную систему, части которой не находятся в конструктивном единстве, поскольку указанные средства, а именно входящие в состав системы видеокамера, электронно-вычислительное устройство и база данных, представляют собой не единую конструкцию.

При рассмотрении дела специалисту были поставлены следующие вопросы в области права:

1) что следует понимать под устройством в смысле п. 1 ст. 1351 ГК РФ;

2) как следует трактовать понятие «единой конструкции или изделия» применительно к положениям ст. 1351 ГК РФ;

3) понимается ли под этим термином необходимость физического совмещения в единый корпус нескольких устройств, объединенных для совместного использования;

4) возможна ли выдача патента на полезную модель на систему устройств (объединенных для совместного использования, размещенных в разных местах, в том числе на значительном удалении друг от друга, но соединенных между собой посредством проводной либо беспроводной связи, как находящихся в конструктивном единстве и функциональной взаимосвязи) или же подобным техническим решениям может быть предоставлена правовая охрана только как изобретениям;

5) если возможна выдача патента на полезную модель на систему устройств, то приводит ли совместное использование таких устройств к созданию нового устройства с новой функцией? Не является ли оценка того, появилось ли новое устройство, элементом экспертизы заявки на полезную модель по существу[3].

---

1 Ковалева А.В. Ответ на запрос специализированного арбитражного суда (ч. 1.1 ст. 16 АПК РФ) как особая форма участия специалиста и его доказательственное значение // Вестник гражданского процесса. 2017. № 6. С. 197–211.

2 Постановление Президиума Суда по интеллектуальным правам от 1 июня 2015 г. № С01-139/2015 по делу № СИП-926/2014 // СПС «Консультант Плюс».

3 Постановление Президиума Суда по интеллектуальным правам от 1 июня 2015 г. № С01-139/2015 по делу № СИП-926/2014 // СПС «Консультант Плюс».

Специалист, аргументированно и полно ответив на все вопросы[1], пришел к выводу, что отказ Роспатента в выдаче патента на полезную модель является правомерным.

Президиум Суда по интеллектуальным правам с учетом мнения специалиста оставил жалобу без удовлетворения.

В спорах по интеллектуальным правам экспертиза как способ защиты исключительных прав на базы данных играет определяющую роль, поскольку суды при возникновении вопроса, требующего специальных знаний, не способны разрешить дело по существу, так как не обладают необходимыми знаниями и инструментами. В свою очередь, экспертиза помогает получить едва ли не единственное доказательство, имеющее решающее значение по делу. Несмотря на оговорки о том, что заключение эксперта оценивается наряду с другими доказательствами, затруднительно найти дело в исследуемой сфере, где ему не придавалось бы приоритетное значение.

Отдельно следует остановиться на роли специалиста в разрешении споров по интеллектуальным правам. Ученые-процессуалисты единодушны во мнении, что в российском законодательстве не наблюдается единства по вопросу о процессуальном положении специалиста[2]. Однако очевидным является то, что функциональная роль специалиста при рассмотрении дел Судом по интеллектуальным по защите исключительных прав на базу данных является значительной, поскольку именно специалист оказывает помощь суду при осуществлении процессуальных действий, а также предоставляет информацию в виде заключения, которая необходима для правильного разрешения судом дела по существу.

---

1 Подробнее об этом см.: Тарасов Н.Н. Президиум Суда по интеллектуальным правам озадачен, находится ли «Система автоматического определения нарушений правил парковки» в конструктивном единстве ...» // Журнал Суда по интеллектуальным правам. 2015. № 9. С. 64–66.

2 См., например: Боннер А.Т. Специалист в гражданском и арбитражном процессе: законодательное регулирование и судебная практика // Закон. 2010. № 6.

Глава 6
ВОПРОСЫ СУДЕБНОЙ ЗАЩИТЫ ПЕРЕДАЧИ И РАСПРОСТРАНЕНИЯ ДАННЫХ В СЕТИ «ИНТЕРНЕТ»(НА ПРИМЕРЕ ДЕЛ О ПРОТИВОДЕЙСТВИИ ЭКСТРЕМИЗМУ)[1]

§ 1. Общие подходы к судебной защите «свободы информации» в Интернете

Современное право, становящееся все более многомерным и поливариантным по способам и формам проявления, испытывает на себе устойчивое влияние информационно-цифровых факторов, связанных с пространством виртуальной реальности.

Цифровая среда воспринимается уже довольно естественной и необходимой, поэтому кажется очевидным, что «ограничение или отсутствие доступа к информационным и коммуникационным технологиям может лишить людей возможности полностью реализовывать свои гражданские права»[2].

Тем не менее сфера правового положения личности как участника информационно-телекоммуникационных отношений в сети «Интернет» относится к числу наименее определенных направлений развития правового регулирования. Зачастую неочевидно, как могут и должны трактоваться различные аспекты свободы индивида, получающие выражение или реализацию в пространстве Интернета и иных сферах цифрового мира.

В частности, идея неприкосновенности частной жизни и информационного самоопределения, предполагающая конкретные границы в физической среде, становится во многом неопределенной (не идентифицируемой) в виртуальной среде, в рамках которой возможность контроля частного пространства в основном утрачивается (в ракурсе обычных средств, способов такого контроля). Вряд ли покажется неоправданным вопрос, можно ли обеспечить конфиденциальность

---

[1] Материал подготовлен в рамках научного проекта РФФИ № 18-29-16051 (по теме «Основные тенденции в правовом регулировании цифровых технологий. Сравнительно-правовое исследование»).

[2] Из преамбулы Декларации Комитета министров о правах человека и верховенстве права в информационном обществе. CM (2005)56. 2005. 13 мая.

сообщения сведений, переписки в пределах конкретного интернет-сообщества, например группы по интересам, или получает ли информация статус публично выраженной при ее опубликовании не в «общих» блогах, а на интернет-страницах личного пользования. Налицо проблема разграничения частных и публичных интернет-данных.

Вопрос произвольного вмешательства тем более актуализируется, когда речь заходит о таком значимом в контексте идеи информационного общества и цифровой коммуникации праве, как право на свободу информации (в том числе при выражении мнений, убеждений)[1]. Данное право служит родовым по отношению к ряду новых признаваемых и легитимируемых прав, таких как право на свободу коммуникации, право на доступ к сети «Интернет»[2], при этом связь между этими правами предполагалась еще ранее международными документами[3].

Отметим, что такой значимый аспект свободы информации, как возможность ее выражения в публичном интернет-пространстве (которой предположительно корреспондирует, прежде всего, негативное обязательство невмешательства в осуществление), получает все чаще «ограничительное» регулирование на национальном уровне. Это нередко позволяет говорить о появлении подобия интернет-цензуры.

Таким образом, с одной стороны, Интернет оказывается беспрецедентным инструментом утверждения ст. 19 Всеобщей декларации прав человека, которой признается возможность искать, получать и распространять информацию и идеи любыми средствами и незави-

---

1 См., например: Талапина Э.В. Право на информацию в свете теории субъективного публичного права // Сравнительное конституционное обозрение. 2016. № 6; Celeste Ed. The Irish Constitution and the Challenges of the Digital Age. Is it Time for a Bunreacht na hEireann 2.0?. URL: https://ulsites.ul.ie/law/papers-constitution-80-conference; Roudik P. Freedom of speech, Internet, Protest and dissent, Right of privacy. URL: http://www.loc.gov/law/foreign-news/article/russia-new-legislation-restricts-anonymity-of-internet-users/

2 В частности, принимается подход, согласно которому «право на доступ к интернету считается неотъемлемой частью права на информацию и связь, защищаемого конституциями государств-членов, и включает в себя право каждого на участие в информационном обществе и обязанность государств гарантировать своим гражданам доступ к Интернету. Соответственно, общие гарантии, защищающие свободу выражения мнения, позволяют сделать вывод, что также следует признать право на беспрепятственный доступ к Интернету» (Постановление ЕСПЧ от 18 декабря 2012 г. (жалоба № 3111/10) по делу «Ахмет Йилдырым (Ahmet Yildirim) против Турции»).

3 Например, ст. 19 Всеобщей декларации прав человека, ст. 10 Европейской конвенции по правам человека, Декларация Совета Европы 1982 г. «О свободе выражения мнения и информации».

симо от государственных границ[1], с другой — внимание к вопросу ограничения свободы выражения в Интернете обусловлено рисками, вызванными в первую очередь масштабами информационной взаимосвязи в этой среде. Согласимся с тем, что Интернет создает новые возможности для осуществления и использования свободы выражения мнения, поскольку в отличие от других средств коммуникации он позволяет легко искать, получать и распространять информацию через границы государств[2]. Очевидно и то, что «влияние информации усиливается, когда ее можно найти в Интернете или даже когда она указана на носителе в общественном месте со ссылкой на адрес сайта в Интернете» — «каждый, включая несовершеннолетних, сможет получить доступ к соответствующему сайту»[3].

В приведенном контексте и складывается практика судебного обеспечения положения личности в связи с развитием цифровой среды: «Хотя... современное развитие Интернета и других новых информационных технологий в большей мере сопряжено с возможными нарушениями права на уважение личной и семейной жизни, "вторжением" в информационную безопасность и неприкосновенность личности, чем с ограничением права на свободу выражения мнения"»[4], поток дел по ст. 10 [Европейской Конвенции по правам человека], связанный с высказываниями в социальных сетях, комментариями под постами в интернет-СМИ, сообщениями по мобильной связи, постепенно увеличивается»[5].

Публикации в Интернете подпадают под сферу действия ст. 10 Конвенции о защите прав человека и основных свобод и ее общих принципов, при этом, как отмечено в специальном исследовательском отчете Европейского Суда по правам человека, особая форма этого средства передачи информации привела Страсбургский Суд к

---

1 См.: Celeste Ed. The Irish Constitution and the Challenges of the Digital Age. Is it Time for a Bunreacht na hEireann 2.0? URL: https://ulsites.ul.ie/law/papers-constitution-80-conference

2 См.: Ягланд Т. О состоянии демократии, правах человека и верховенстве права // Прецеденты Европейского Суда по правам человека. 2018. № 1.

3 Интернет: прецедентная практика Европейского Суда по правам человека. Отчет Отдела по проведению исследований ЕСПЧ, 2011. URL: https://www.echr.coe.int/Documents/Research_report_Internet_RUS.pdf

4 Ефремов А. Новые информационные технологии в практике Европейского Суда по правам человека // Прецеденты Европейского Суда по правам человека. 2016. № 6 (30)

5 Соболева А.К. Свобода выражения мнения в практике Европейского суда: старые подходы и новые тенденции в толковании статьи 10 ЕКПЧ. Т. 21 // Вестник РУДН. Серия: Юридические науки. 2017. № 2.

принятию определенных ограничений в отношении свободы выражения мнения в Интернете[1].

Выделим некоторые значимые подходы к оценке возможности ограничения свободы выражения согласно практике ЕСПЧ (обзорно обозначенные в упомянутом исследовательском отчете).

Ограничения свободы, предусмотренные ст. 10 (п. 2) Конвенции по правам человека, должны толковаться узко. Вмешательство со стороны государств в осуществление этой свободы возможно при условии, что оно является «необходимым в демократическом обществе», то есть согласно прецедентной практике Европейского Суда должно отвечать «настоятельной общественной необходимости», быть соразмерным преследуемой правомерной цели по смыслу п. 2 ст. 10 и быть обоснованным судебными решениями, содержащими соответствующую и достаточную мотивировку. Хотя у национальных властей есть определенная свобода усмотрения, она не является неограниченной и сопровождается европейским контролем, проводимым ЕСПЧ.

Европейский Суд также указывал, что ст. 10 (п. 2) оставляет мало возможностей для ограничения свободы выражения мнения при обсуждении политических или общественно значимых вопросов. В отношении прессы, значительная часть которой публикуется в Интернете, свобода передачи и получения информации и ее гарантии имеют особое значение, на прессе лежит обязанность передавать информацию и идеи по общественно значимым вопросам.

Вместе с тем разжигание розни не защищается ст. 10 Конвенции (дело «Гюндюз против Турции»[2]), и согласно ст. 17 высказывания, которые являются несовместимыми с провозглашенными и гарантированными конвенцией ценностями, не получают защиты по ст. 10.

Свобода выражения мнения, хотя и имеет особую ценность для демократии, не позволяет пропагандировать расовую дискриминацию и вражду независимо от использованных средств. Осуждение в уголовном порядке владельца сайта в Интернете, который также являлся политическим лидером и который опубликовал ксенофобские высказывания, может отвечать настоятельной общественной необходимости защиты прав других лиц (дело «Фере против Бельгии»[3]).

Весьма противоречивым по оценкам оказалось дело «Делфи АС против Эстонии»[4]. В связи с данным делом ЕСПЧ, как было под-

---

1 Интернет: прецедентная практика Европейского Суда по правам человека...

2 Постановление ЕСПЧ от 4 декабря 2003 г. (жалоба № 35071/97).

3 Постановление ЕСПЧ от 16 июля 2009 г. (жалоба № 15615/07).

4 Постановление ЕСПЧ от 16 июня 2015 г. (жалоба № 64569/09).

черкнуто в особом мнении (судей А. Шайо, Н. Цоцория) по делу, одобрил систему ответственности активных интернет-посредников (поставщиков услуг по размещению информации, публикующих собственные материалы и предлагающих свои промежуточные услуги третьим лицам для комментирования этих материалов), предусматривающую презумпцию осведомленности. ЕСПЧ согласился с позицией Государственного суда Эстонии, согласно которой активные посредники обязаны удалять комментарии сразу же после их опубликования, а не по обращению заинтересованных лиц и не по другим основаниям, связанным с фактической осведомленностью.

В этом же мнении судьями обозначено, что потенциальные последствия, которые может повлечь за собой этот критерий, вызывают опасения. Государства не всегда осуществляют цензуру напрямую, но, оказывая давление на тех, кто контролирует технологическую инфраструктуру (интернет-провайдеров), и привлекая их к ответственности, они создают ситуацию, в которой субъектом цензуры неизбежно становятся частные лица. Таким образом, активных посредников подталкивают к предварительному ограничению интернет-свобод. Более того, этому примеру придется последовать и государствам-участникам, так как иначе, по логике постановления по делу, невозможно обеспечить эффективную защиту прав тех, кому кажется, что комментарии посягают на их честь[1].

А.К. Соболева, анализируя данное постановление ЕСПЧ, обоснованно указывает на три ключевых вопроса, несущих риски такой свободе в интернет-среде[2]. Во-первых, речь идет о проблеме ответственности именно интернет-порталов, которые эстонскими судами были фактически приравнены к «издателю» (не учтя позицию заявителя о рассмотрении ресурса лишь как «посредника» в передаче информации). Во-вторых, ЕСПЧ — применительно к комментариям пользователей — не провел в данном случае различия между диффамационными высказываниями, языком вражды и другим незаконным контентом. В-третьих, национальные суды Эстонии, поддержанные Европейским Судом, требовали удалять контент немедленно, без уведомления об этом автора комментария.

В связи с приведенным делом можно выделить основные проблемы, находящиеся в центре внимания в свете регулирования и ограничения свободы информации в Интернете: определение содержания (характеристик) противоправного материала, обозначе-

---

1 Постановление ЕСПЧ от 16 июня 2015 г. (жалоба № 64569/09).

2 См.: Соболева А.К. Указ. соч.

ние субъекта ответственности и порядок привлечения к ответственности.

§ 2. Проблема оценочных суждений при ограничении свободы информации в связи с российской судебной практикой по делам экстремистской направленности

Тенденцией российского правового развития является увеличение объема законодательного регулирования в области информационно-сетевой коммуникации, затрагивающего многие аспекты правового положения личности[1]. Обращает на себя внимание расширение круга критериев отнесения публично выраженной информации к «противоправной» и мер ответственности в связи с этим. Например, принят закон, получивший условное наименование «о неуважении к государственной власти»[2], уточняющий перечень информации, распространение которой в Российской Федерации запрещено[3].

Особое внимание уделяется проблеме распространения в сети «Интернет» материалов экстремистской направленности.

Согласно п. 23 Указа Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» первоочередным направлением обеспечения информационной безопасности в области государственной и общественной безопасности является «противодействие использованию информационных технологий для пропаганды экстремистской идеологии... в целях подрыва суверенитета, политической и соци-

---

1 Внесены многочисленные изменения в федеральные законы «Об информации, информационных технологиях и защите информации», «О связи», в гражданское законодательство в части определения «цифровых прав». Обсуждаются законопроекты о цифровых финансовых активах (паспорт проекта № 419059-7), о правовом регулировании деятельности социальных сетей (паспорт проекта № 145507-7).

2 Федеральный закон от 18 марта 2019 г. № 30-ФЗ «О внесении изменения в Федеральный закон «Об информации, информационных технологиях и о защите информации». Законом вводится статья, предусматривающая возможность принятия мер по ограничению доступа к информации (материалам), предназначенной (предназначенным) для неограниченного круга лиц, выражающей (выражающих) в неприличной форме явное неуважение к обществу, государству, официальным государственным символам Российской Федерации, Конституции РФ и органам, осуществляющим государственную власть в Российской Федерации. См.: Комментарий к вопросу применения «пакета Клишаса». URL: http://ilpp.ru/news/events/2019/03/26/events_1092.html

3 К настоящему времени уже приняты судебные решения о штрафных мерах в связи с законом о неуважении к власти. URL: https://pravo.ru/news/211101/

альной стабильности, насильственного изменения конституционного строя, нарушения территориальной целостности Российской Федерации».

Обозначим, что ответственность по российскому праву за размещение экстремистских материалов наступает в рамках как административного, так и уголовного законодательства.

Проблема экстремизма стала связываться с интернет-отношениями преимущественно с 2012 г., когда в информационное законодательство (ФЗ № 149-ФЗ, № 126-ФЗ) были внесены соответствующие изменения[1]. В связи с изменениями был создан Единый реестр доменных имен и (или) универсальных указателей страниц сайтов в сети «Интернет» и сетевых адресов сайтов в сети «Интернет», содержащих информацию, запрещенную к распространению на территории Российской Федерации федеральными законами.

Наибольшую известность в связи с административными делами по вопросам экстремизма получил Федеральный закон от 28 декабря 2013 г. № 398-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации». Как следует из пояснительной записки к проекту данного закона, он был разработан в целях совершенствования механизмов защиты общества от противоправной информации, распространяемой в информационно-телекоммуникационных сетях (в том числе в сети «Интернет»). Под такой информацией понимается информация, содержащая призывы к массовым беспорядкам, осуществлению экстремистской деятельности, разжиганию межнациональной и (или) межконфессиональной розни, участию в террористической деятельности, а также в публичных массовых мероприятиях, проводимых с нарушением установленного порядка.

При обнаружении соответствующей информации в Интернет предусматривается возможность внесудебной блокировки информационного ресурса, распространяющего ее. Так, Генеральный прокурор РФ или его заместители направляют требование в федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, о принятии мер по ограничению доступа к информационным ресурсам, распространяющим такую информацию. После получения требования фе-

---

[1] См., например: Федеральный закон от 28 июля 2012 г. № 139-ФЗ «О внесении изменений в Федеральный закон "О защите детей от информации, причиняющей вред их здоровью и развитию" и отдельные законодательные акты Российской Федерации» // СЗ РФ. 2012. № 31. Ст. 4328.

дерального органа исполнительной власти о принятии мер по ограничению доступа оператор связи, оказывающий услуги по предоставлению доступа к информационно-телекоммуникационной сети «Интернет», обязан незамедлительно ограничить доступ к информационному ресурсу, в том числе к сайту в сети «Интернет», или к информации, размещенной на нем.

В связи с этим также отмечается создание правовых условий для массовой блокировки интернет-ресурсов (прежде всего, по причине оверблокинга, когда «технически заодно» блокируется доступ к сайтам с легальным контентом). По исследованиям проекта «РосКомСвобода», на 3 апреля 2014 г. был ограничен доступ к 58 940 сайтам, размещенным на одном IP-адресе с сайтами, внесенными в единый реестр запрещенных сайтов[1]. В 2016 году в соответствии с указанным законом было заблокировано не менее 87 000 URL (интернет-адресов)[2].

Такие возможности «произвольного ограничения» свободы информации в Интернет в силу одного только порядка применения таких ограничений обозначают по меньшей мере проблему соразмерности используемых средств преследуемым целям ограничения и, соответственно, судебного контроля применения введенного порядка блокирования интернет-ресурсов.

Как следует из специального доклада Комиссара СЕ о верховенстве права в Интернете, для предупреждения возможных злоупотреблений большое значение имеет предоставление гарантий судебного контроля. Национальные суды должны установить, является ли мера по блокированию необходимой, эффективной и соразмерной, а также носит ли она целевой характер, чтобы воздействовать лишь на конкретный контент, требующий блокирования.

Это становилось предметом рассмотрения КС РФ, который ответил на обращение определением об отказе в принятии обращения к рассмотрению (от 17 июля 2014 г. № 1759-О)[3]. КС РФ не стал давать оценку конституционности изменений информационного законодательства (определивших возможность блокировки сетевого адреса, по которому осуществляется доступ к сайту, содержащему противоправную информацию), послуживших основанием к широкому ограничению доступа к интернет-ресурсам. По гарантиям прав владельцев сайтов, не содержащих запрещенной к распространению информации, но технически попавших под блокировку, суд указал

---

1 URL: http://rublacklist.net/7524/

2 URL: https://www.hrw.org/report/2017/07/18/online-and-all-fronts/russias-assault-freedom-expression

3 Определение КС РФ от 22 декабря 2015 г. № 3024-О.

на ответственность за ограничение доступа к таким сайтам обслуживающего их провайдера[1].

Данное дело показательно с точки зрения проблемы пропорциональности ограничения права на получение и распространение информации, ограничения доступа к сторонним ресурсам и информации, в последнее время попадающей в сферу деятельности ЕСПЧ[2]. Неудивительно, что обращение по соответствующему вопросу впоследствии было коммуницировано ЕСПЧ[3].

При рассмотрении ранее аналогичного дела в отношении Турции (по оверблокингу)[4] ЕСПЧ указал на то, что последствия рассматриваемой меры были произвольными, а судебный контроль недостаточным для того, чтобы предотвратить злоупотребления, в связи с чем признал нарушение ст. 10 Европейской конвенции по правам человека. При принятии решений национальный суд сослался на указание уполномоченного органа, не уточнив, можно ли было принять менее масштабную меру, чтобы заблокировать доступ к конкретному сайту; также не было никаких признаков того, что суд предпринял какие-либо попытки сопоставить различные интересы. По мнению ЕСПЧ, этот недостаток был обусловлен внутренним законодательством, которое не накладывало каких-либо обязательств перед судами на проверку обоснованности полной блокировки. Суды должны были учесть тот факт, что такая мера сделает большие объемы информации недоступными, что напрямую повлияет на права пользователей Интернета и будет иметь значительный побочный эффект.

В течение некоторого времени обозначалась и проблема «личной ответственности» операторов связи по ст. 20.29 КоАП РФ в свете вопроса о предоставлении ими технической возможности работы сайтов, размещающих экстремистскую информацию.

Так, суды разных уровней судебной системы приходили к выводу, что предоставление технической возможности доступа к запрещенной законом информации, фактически ее распространение и непринятие мер по ограничению доступа к интернет-сайтам, содержащим видеоматериалы с такой информацией, образуют состав администт-

---

1 Там же.

2 В Постановлении по делу Yildirim v. Turkey ЕСПЧ указал на то, что ограничение доступа к сторонним сайтам нарушает положения Европейской конвенции по правам человека.

3 URL: https://www.echr.coe.int/Documents/FS_Access_Internet_ENG.pdf

4 См.: Постановление ЕСПЧ от 18 декабря 2012 г. «Дело "Ахмет Йилдырым (Ahmet Yildirim) против Турции"» (жалоба № 3111/10).

ративного правонарушения, предусмотренного ст. 20.29 КоАП РФ. При этом соответствующее должностное лицо подлежит административной ответственности в связи с необеспечением соблюдения требований Федерального закона от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» (далее —Федеральный закон № 114-ФЗ). ВС РФ в свою очередь мог постановить отменить соответствующие судебные решения, прекратить производство по такому делу об административном правонарушении в связи с недоказанностью обстоятельств, на основании которых были вынесены указанные судебные постановления[1].

Помимо проблемы «соразмерности ограничений», несомненно, определяющее значение имеет другой вопрос — об определенности оснований (материальных и процессуальных) вмешательства, введения таких ограничений. В докладе Комиссара СЕ о верховенстве права в Интернете справедливо констатировано, что государства-члены должны гарантировать, чтобы любые ограничения доступа к интернет-контенту, которые затрагивают пользователей под их юрисдикцией, основывались на ясных и предсказуемых правовых нормах; сфера действия любых ограничений также должна быть четко урегулирована.

В этом выражено требование законности вмешательства, определенного Конвенцией по правам человека в формуле «предусмотрено законом». По мнению ЕСПЧ, правовую норму нельзя считать «законом» по смыслу положений п. 2 ст. 10 конвенции, если она не сформулирована достаточно четко, чтобы позволить гражданину скорректировать свои действия, у него должна быть возможность, в случае необходимости прибегнув к соответствующей консультации, предвидеть в разумной в обстоятельствах дела степени возможные последствия того или иного действия. Эти последствия необязательно должны быть предсказуемы с абсолютной определенностью (например, постановления по делам «Лендон, Очаковский-Лоран и Жюли против Франции», «Делфи против Эстонии»[2]).

Обращаясь к легальной дефиниции понятия «экстремизм», в Федеральном законе № 114-ФЗ можно обнаружить широкий перечень материалов, которые могут быть отнесены к экстремистским, — от содержащих информацию о насильственном изменении основ конституционного строя, нарушении целостности Российской Федерации, возбуждении социальной, расовой, национальной, религиозной

---

1 См., например, постановление ВС РФ от 29 сентября 2014 г. №31-АД14-7.

2 См.: Постановления ЕСПЧ от 22 октября 2007 г. (жалобы № 21279/02 и № 36448/02); от 16 июня 2015 г. (жалоба № 64569/09).

розни, пропаганду исключительности, превосходства либо неполноценности человека до информации о публичном заведомо ложном обвинении лица, замещающего государственную должность Российской Федерации, государственную должность субъекта Российской Федерации, в подстрекательстве к осуществлению деяний. При этом в основном такая «экстремистская» информация плохо поддается точной идентификации с точки зрения параметров ее определения и тем самым создает основу для многообразия оценочных суждений в правоприменительной практике[1].

В связи с этим обоснована оценка понятия «экстремизм» как широко трактуемого правоприменителем[2]. Соответственно судебная практика по таким делам складывается неодинаково и уже становилась объектом внимания КС РФ.

По одному из дел в КС РФ заявитель обращался о признании отдельных положений Федерального закона № 114-ФЗ не соответствующими Конституции РФ в той части, в какой они позволяют признавать материал экстремистским лишь потому, что в нем провозглашается истинность излагаемого в нем учения наряду с утверждением о ложности иных учений, а также предоставляют правоприменительным органам чрезмерные полномочия по оценке таких материалов (например, по определению сходства того или иного символа с нацистским без учета контекста их использования)[3].

Суд в определении по данному делу обозначил ранее выраженные им позиции в решении от 2 июля 2013 г. № 1053-О, указав на обязан-

---

[1] Например, в комментарии к названному закону подчеркнуто, что формулировка п. 4 ч. 1 ст. 1, предполагающая отнесение к экстремистской деятельности «пропаганды исключительности, превосходства...» содержит слишком много возможностей для ее расширенного толкования. По сути под данную норму можно подвести большинство анекдотов про русских, чукчей, молдаван, евреев, украинцев. Она легко распространяется, например, на религиозную агитацию, пропагандирующую избранность последователей определенной религии или религиозного течения, и т.д. См.: Комментарий к Федеральному закону от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности (постатейный)» / сост. А.Б. Смушкин. 2015 // СПС «КонсультантПлюс».

[2] См., например: Нардина О.В. Ограничение конституционного права на доступ к получению и распространению информации в сети «Интернет» в связи с противодействием экстремизму и терроризму // Наука. Общество. Государство (электронный журнал). 2017. Т. 5. № 4 (20); Султанов А.Р. Защита прав, свобод и законных интересов граждан при рассмотрении дел о признании информационных материалов экстремистскими // Арбитражный и гражданский процесс. 2012. № 1. С. 26–32.

[3] См. определение КС РФ от 17 февраля 2015 г. № 347-О «Об отказе в принятии к рассмотрению жалобы гражданина Синицына Михаила Владимировича на нарушение его конституционных прав положениями пункта 1 статьи 1 Федерального закона «О противодействии экстремистской деятельности».

ность судов исходить из того, что обязательным признаком указанной разновидности экстремизма (экстремистских материалов) является явное или завуалированное противоречие соответствующих действий (документов) конституционным запретам возбуждения ненависти и вражды, разжигания розни и пропаганды социального, расового, национального, религиозного или языкового превосходства. Наличие такого противоречия должно определяться с учетом всех значимых обстоятельств каждого конкретного дела (форма и содержание деятельности или информации, их адресаты и целевая направленность, общественно-политический контекст, наличие реальной угрозы, обусловленной в том числе призывами к противоправным посягательствам на конституционно охраняемые ценности, обоснованием или оправданием их совершения, и т.п.). При этом ограничение посредством антиэкстремистского законодательства свободы совести и вероисповедания, свободы слова и права на распространение информации не должно иметь места в отношении какой-либо деятельности или информации на том лишь основании, что они не укладываются в общепринятые представления, не согласуются с устоявшимися традиционными взглядами и мнениями, вступают в противоречие с морально-нравственными и (или) религиозными предпочтениями.

КС РФ было отмечено, что иное означало бы отступление от конституционного требования необходимости, соразмерности и справедливости ограничений прав и свобод человека и гражданина, которое обращено не только к законодателю, но и к правоприменителям, в том числе к судам.

Вместе с тем проблема ясности и достаточности правового регулирования в части «качества» оснований привлечения к ответственности по делам об экстремизме, полагаем, не получила разрешения.

Рассматриваемая проблема (определение критериев отнесения информации к экстремистской) обостряется в связи с делами об ответственности в уголовно-правовой сфере. Положения по делам экстремистской направленности предусмотрены рядом статей УК РФ: ст. 280 «Публичные призывы к осуществлению экстремистской деятельности» (ч. 2 определяет состав таких деяний с использованием средств массовой информации либо информационно-телекоммуникационных сетей, в том числе сети «Интернет»), ст. 282 «Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства», ст. 282.1 «Организация экстремистского сообщества», ст. 282.2 «Организация деятельности экстремистской организации».

Обозначим, что согласно п. 2 примечания к ст. 282.1 под преступлениями экстремистской направленности в УК РФ понимаются

преступления, совершенные по мотивам политической, идеологической, расовой, национальной или религиозной ненависти или вражды либо по мотивам ненависти или вражды в отношении какой-либо социальной группы.

В целом уголовно-правовое законодательство в части «экстремистских» преступлений справедливо характеризуется как не вполне соответствующее принципу правовой определенности (учитывая неполную ясность, какие именно действия запрещены уголовным законом, их оценочный характер). Данный вопрос изначально требовал особого внимания, учитывая его уголовно-правовой характер, предполагающий наиболее высокую степень вмешательства в осуществление конституционно гарантированных прав и свобод.

Данные Пленумом ВС РФ в 2011 г. разъяснения (постановление от 28 июня 2011 г. № 11 «О судебной практике по уголовным делам о преступлениях экстремистской направленности») не сразу способствовали достаточной ясности в оценке таких запретов, с одной стороны, а также в определении условий, способов их применения судами — с другой. Так, обозначим несколько позиций из постановления Пленума ВС РФ 2011 г.

Во-первых, при рассмотрении уголовных дел о преступлениях экстремистской направленности судам следует обеспечивать, с одной стороны, охрану публичных интересов (основ конституционного строя, целостности и безопасности Российской Федерации), а с другой — защиту гарантированных Конституцией РФ прав и свобод человека и гражданина.

Во-вторых, при производстве по уголовным делам о преступлениях экстремистской направленности судам необходимо иметь в виду, что согласно УПК РФ подлежат доказыванию мотивы совершения указанных преступлений.

В-третьих, под публичными призывами к осуществлению экстремистской деятельности следует понимать выраженные в любой форме (устной, письменной, с использованием технических средств, информационно-телекоммуникационных сетей общего пользования, включая сеть «Интернет») обращения к другим лицам с целью побудить их к осуществлению экстремистской деятельности. Вопрос о публичности призывов должен решаться судами с учетом места, способа, обстановки и других обстоятельств дела.

В-четвертых, преступление считается оконченным с момента публичного провозглашения (распространения) хотя бы одного обращения независимо от того, удалось побудить других граждан к осуществлению экстремистской деятельности или нет.

Тем самым судам было предоставлено достаточно много дискреции в случае применения уголовно-правовых норм по «экстремистским» делам, предполагающего и необходимость разрешения в каждом конкретном случае вопроса о соотношении публичных и частных конституционных ценностей.

По результатам сложившейся судебной практики по уголовным делам экстремистской направленности были приняты дополнительные изменения в постановление Пленума ВС РФ от 28 июня 2011 г. № 11 «О судебной практике по уголовным делам о преступлениях экстремистской направленности». Их необходимость обосновывалась сложившейся практикой, в связи с которой отмечалось, что 90% всех осужденных по преступлениям экстремистской направленности совершили их онлайн[1].

В постановление Пленума ВС РФ от 20 сентября 2018 г. № 32 «О внесении изменений в Постановление Пленума Верховного Суда РФ от 28 июня 2011 г. № 11 «О судебной практике по уголовным делам о преступлениях экстремистской направленности» нашли подробную проработку критерии рассмотрения и разрешения судами названной категории дел с учетом приоритетности гарантирования прав и внимания к так называемому тесту на пропорциональность при оценке допустимости ограничений.

Было обращено внимание судов на то, что гарантированные Конституцией РФ и международно-правовыми актами свобода мысли и слова, а также право свободно искать, получать, передавать, производить и распространять информацию любым законным способом могут быть ограничены только в исключительных случаях, прямо закрепленных в федеральном законе. Ограничение возможно в той мере, в какой это необходимо в демократическом обществе в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства, общественного порядка, территориальной целостности (п. 1).

Применительно к ст. 282 УК РФ Верховный Суд РФ указал, что судами учитывается не только сам факт размещения в сети «Интернет» или иной информационно-телекоммуникационной сети изображения, аудио- или видеофайла, содержащего признаки возбуждения вражды и ненависти, унижения достоинства человека либо группы лиц по признакам, содержащимся в данной статье, но и иные сведения, указывающие на общественную опасность деяния, мотив

---

[1] URL: http://www.supcourt.ru/press_center/news/27128/; https://pravo.ru/story/205404/?desc_tv_7=

его совершения (п. 2.1). При этом размещение лицом в сети «Интернет» или иной информационно-телекоммуникационной сети материала может быть квалифицировано по ст. 282 УК РФ только в случаях, когда установлено, что лицо осознавало направленность деяния на нарушение основ конституционного строя, а также имело цель возбудить ненависть или вражду либо унизить достоинство человека или группы лиц по признакам пола, расы, национальности, языка, происхождения, отношения к религии либо принадлежности к какой-либо социальной группе (п. 8). Доказывание умысла предполагает учет широкого контекста обстоятельств.

В связи с ч. 2 ст. 14 УК РФ также было отмечено, что не является преступлением действие (бездействие), хотя формально и содержащее признаки какого-либо деяния, предусмотренного уголовным законом, но в силу малозначительности не представляющее общественной опасности (п. 8.1).

Не менее важно то, что при оценке заключения эксперта по делам о преступлениях экстремистской направленности судам следует иметь в виду, что оно не имеет заранее установленной силы, не обладает преимуществом перед другими доказательствами и, как все иные доказательства, оценивается по общим правилам в совокупности с другими доказательствами. При этом вопрос о том, являются те или иные действия публичными призывами к осуществлению экстремистской деятельности или к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации, а также возбуждением ненависти либо вражды, а равно унижением человеческого достоинства, относится к компетенции суда (п. 23).

Соответствующие уточнения ВС РФ своих позиций по «экстремистским» делам соотносятся с идеей привлечения к уголовно-правовой ответственности в наиболее серьезных случаях при действительном наличии умысла, его направленности у лица, размещающего в Интернете материалы, считающиеся экстремистскими, и наличия реальных рисков, конкретных угроз правопорядку, идентифицируемых, в частности, ч. 5 ст. 13 Конституции РФ.

Полагаем уместно обратиться к особому мнению судьи К.В. Арановского по другому вопросу (при проверке КС РФ конституционности положений закона о СМИ)[1], но также вполне релевантному к анализируемой проблеме.

«Защита конституционных ценностей возможна как таковая лишь в паре с опасностью, т.е. в упреждение угроз и рисков на перспекти-

[1] См.: постановление КС РФ от 17 января 2019 г. № 4-П.

ву либо в ретроактивном исполнении — в ответ на причиняемый или причиненный вред...

Если угроза и опасность не самоочевидны, их нужно установить и доказать в конституционном судопроизводстве, причем в реально существующих опасностях, в действительных источниках риска. Иначе ограничения прав и свобод, не обусловленные целями и потребностями соответствующей защиты, изначально выйдут за допустимые конституционные рамки...

Законодательные решения, которые приводят к изъятиям в правах, мало обосновать лишь опасениями... Права и свободы человека и гражданина стали бы беззащитными, если бы часть 3 статьи 55 Конституции РФ позволяла трактовать как охранительную цель одно лишь субъективное намерение, мотивированное беспокойным предчувствием... Объективная угроза и реальная опасность конституционно охраняемым ценностям — это необходимое условие в обосновании правоограничений».

В то же время в силу оценочного характера понимания роли информации в Интернете и способов ее распространения проблема того, что есть конкретный риск или угроза, служащие идентификации такой информации как противоправной, вряд ли будет окончательно решена в ближайшей перспективе.

Подчеркнем, что и в практике ЕСПЧ с учетом оценочности характеристик информации, позволивших относить ее к категории противоправной, также прослеживается сохранение широкого поля усмотрения государств в оценке ее распространения, что, в частности, проявилось в деле «Делфи АС против Эстонии». Напомним, что в рамках дела объектом внимания были спорные комментарии в Интернете, содержащие «агрессивные высказывания и высказывания, прямо пропагандирующие акты насилия». При этом в рамках решения по делу было обращено внимание на то, что у понятия «агрессивные высказывания» до сих пор нет определения и общепризнанного определения понятия «агрессивные высказывания» не существует; данное понятие охватывает широкий спектр человеконенавистнических высказываний.

Признание ЕСПЧ нарушения Конвенции по соответствующим делам, как правило, обусловлено несоблюдением со стороны государства принципа законности вмешательства в части очевидных (а не оценочных) оснований привлечения к ответственности. Например, в деле «Касымахунов и Сайбаталов против Российской Федерации»[1] Суд не усмотрел нарушения ст. 9–11 Конвенции в связи с привлече-

[1] Постановление ЕСПЧ от 14 марта 2013 г. (жалобы № 26261/05 и 26377/06).

нием заявителей к уголовной ответственности за участие в организации, признанной экстремистской и террористической. При этом было обозначено нарушение ст. 7 конвенции, поскольку решение ВС РФ о запрете данной организации было опубликовано позже вступления второго заявителя в эту организацию и заявитель не мог предвидеть, что членство в ней может повлечь уголовную ответственность.

Подводя итог, признаем обоснованность мнения о том, что влияние цифровой эпохи должно повлечь соответствующее увеличение масштаба конституционной среды, поскольку «невозможно представить, что человеческая деятельность путем простого преодоления порога виртуального мира теряет конституционную защиту»[1]. Данная идея актуализируется в связи с наличием множества вопросов обеспечения свободы информации в Интернете, принимая во внимание увеличение числа критериев отнесения публично выраженной информации к категории противоправной и соответствующих мер ответственности. Центральной становится проблема судебной защиты рассматриваемой конституционной ценности, что сопряжено с ценностно-ориентированной трактовкой законодательства в случае предполагаемого отнесения информации к противоправной по оценочным основаниям.

---

[1] Celeste Ed. The Irish Constitution and the Challenges of the Digital Age. Is it Time for a Bunreacht na hEireann 2.0? URL: https://ulsites.ul.ie/law/papers-constitution-80-conference; Yannic Blaschke. Digital rights as a security objective: New gateways for attacks. URL: https://edri.org/donate/

Глава 7
НЕКОТОРЫЕ ПРОБЛЕМЫ СУДЕБНОЙ ПРАКТИКИ ПО ДЕЛАМ, СВЯЗАННЫМ С ОБРАБОТКОЙ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ В ТРУДОВЫХ ОТНОШЕНИЯХ

При приеме на работу каждый работник обязан предъявить работодателю документы, указанные в ст. 65 ТК РФ. Данные документы содержат персональные данные работника, то есть информацию, относящуюся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Федеральный закон «О персональных данных» регулирует отношения, связанные с обработкой персональных данных, которая подразумевает получение, хранение, использование и передачу персональных данных в трудовых отношениях работодателем.

В связи с этим нередко возникают конфликтные ситуации, заканчивающиеся судебными спорами. Глава 14 ТК РФ 2001 г. регулирует защиту персональных данных работника от неправомерного их использования или утраты работодателем. Вместе с тем нормы ТК РФ регулируют не все вопросы защиты персональных данных работника.

Потенциал судебной практики по данным вопросам имеет особое значение, потому что правовые пробелы в области персональных данных работника нередко восполняются нормами судебной практики.

Судебная практика по рассмотрению трудовых споров, связанных с обработкой персональных данных работника, представляет интерес с точки зрения:

– кому работодатель правомерен осуществлять передачу персональных данных работников, помимо субъектов, установленных законом;

– имеет ли право работодатель хранить копии документов работника, так как в копиях документов содержатся его персональные данные.

§ 1. Обработка работодателем персональных данных работника

Передача персональных данных является одним из действий, включенных в понятие «обработка персональных данных», кото-

рое дается в п. 3 ст. 3 Закона № 152-ФЗ. По смыслу ст. 7 закона и ст. 88 ТК РФ персональные данные работника можно передать только с его письменного согласия.

Вместе с тем законодательство устанавливает перечень лиц, которым работодатель обязан передавать персональные данные работников без их согласия, например в Пенсионный фонд РФ, Фонд обязательного медицинского страхования РФ, Фонд социального страхования РФ (ст. 9 Федерального закона от 1 апреля 1996 г. № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования»), в налоговые органы (ст. 24 НК РФ), по запросам правоохранительных органов и т.д.

В соответствии с ч. 1 ст. 17 Федерального закона от 12 января 1996 г. № 10-ФЗ «О профессиональных союзах, их правах и гарантиях деятельности» для осуществления уставной деятельности профсоюзы вправе бесплатно и беспрепятственно получать от работодателей, их объединений (союзов, ассоциаций), органов государственной власти и органов местного самоуправления информацию по социально-трудовым вопросам. Закономерно возникает вопрос, может ли соответствующий профессиональный союз запросить у работодателя информацию, которая содержит персональные данные работников, без их согласия.

Рассмотрим судебную практику, когда запрос персональных данных работников профессиональным союзом у работодателя связан с защитой коллективных прав работников.

Так, 9 марта 2011 г. председатель первичной профсоюзной организации «Разрез Лучегорский» Российского независимого профсоюза работников угольной промышленности Лучегорского топливно-энергетического комплекса Пожарского района обратился к директору филиала «Лучегорский угольный разрез» ОАО «Дальневосточная генерирующая компания» с запросом о предоставлении информации о привлечении работников указанного филиала к работе сверхурочно и в выходные дни поименно с указанием работника, даты его привлечения к работе, количества часов работы, оплаты за отработанный период по каждому подразделению филиала за периоды с 1 января по 31 декабря 2010 г. и с 1 января по 28 февраля 2011 г. Аналогичное требование о предоставлении информации было направлено тем же профсоюзным органом 10 мая 2011 г. тому же должностному лицу.

16 марта и 17 мая 2011 г. администрацией указанного филиала отказано профсоюзному органу в предоставлении запрошенной информации со ссылкой на то, что действующее законодательство ограничивает работодателя в возможности передачи персональных

данных работника третьим лицам, в том числе и представителям работников.

В соответствии с ч. 1 ст. 11 Федерального закона от 12 января 1996 г. № 10-ФЗ «О профессиональных союзах, их правах и гарантиях деятельности» профсоюзы, их объединения (ассоциации), первичные профсоюзные организации и их органы представляют и защищают права и интересы членов профсоюзов по вопросам индивидуальных трудовых и связанных с трудовыми отношениями, а в области коллективных прав и интересов — указанные права и интересы работников независимо от членства в профсоюзах в случае наделения их полномочиями на представительство в установленном порядке. Согласно ч. 3 ст. 13 указанного закона первичные профсоюзные организации, профсоюзы, их объединения (ассоциации) вправе осуществлять профсоюзный контроль за выполнением коллективных договоров, соглашений.

Разрешая спор, ВС РФ указал, что в соответствии со ст. 40, 41 ТК РФ коллективный договор — правовой акт, регулирующий социально-трудовые отношения в организации и заключаемый работниками и работодателем в лице их представителей. Содержание и структура коллективного договора определяются сторонами, и в него могут включаться обязательства работников и работодателя по вопросам формы, системы и размера оплаты труда, рабочего времени и времени отдыха, а также по другим вопросам, определенным сторонами.

В силу действия ст. 31 ТК РФ контроль за выполнением коллективного договора, соглашения осуществляется сторонами социального партнерства, их представителями, соответствующими органами по труду. При проведении указанного контроля представители сторон обязаны предоставлять друг другу необходимую для этого информацию не позднее одного месяца со дня соответствующего запроса.

Часть 3 ст. 13 Федерального закона «О профессиональных союзах, их правах и гарантиях деятельности» устанавливает, что первичные профсоюзные организации вправе осуществлять профсоюзный контроль за выполнением коллективных договоров и соглашений, и в соответствии с ч. 1 ст. 17 указанного закона профсоюзы вправе бесплатно и беспрепятственно получать от работодателя информацию по социально-трудовым вопросам.

Статья 88 ТК РФ предусматривает, что при передаче персональных данных работника работодатель должен соблюдать следующие требования: не сообщать персональные данные работника в коммерческих целях без его письменного согласия; предупредить лиц, по-

лучающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные работника, обязаны: соблюдать режим секретности (конфиденциальности) — данное положение не распространяется на обмен персональными данными работников в порядке, установленном ТК РФ и иными федеральными законами; осуществлять передачу персональных данных работника в пределах одной организации, у одного индивидуального предпринимателя в соответствии с локальным нормативным актом, с которым работник должен быть ознакомлен под роспись; разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций.

Таким образом, сведения о заработной плате, времени труда и отдыха относятся к вопросам, регулируемым коллективным договором, что, в свою очередь, отнесено к функциям профсоюзов, направленным на осуществление контроля за соблюдением трудового законодательства, коллективных договоров и соглашений. Аналогичные положения содержатся в ст. 2.4 Устава Российского независимого профсоюза работников угольной промышленности и в положениях коллективного договора от 3 декабря 2010 г., подписанного филиалом «Лучегорский угольный разрез» и истцом.

ВС РФ в определении от 20 июля 2012 г. № 56-КГ12-3 пришел к выводу о том, что согласие работников на передачу их персональных данных профессиональному союзу не требуется, так как коллективный договор заключен от имени всех работников, а профессиональный союз, запрашивая персональные данные, контролирует соблюдение коллективного договора.

Разрешая заявленные исковые требования, ВС РФ посчитал факт запроса информации профессиональным союзом необходимым для осуществления возложенных на него в силу закона функций запрашивать у работодателя информацию по вопросам исполнения коллективного договора как в отношении работников, являющихся членами профсоюза, так и в отношении работников, не относящихся к таковым. Работодатель не вправе отказать в предоставлении такой информации в связи с отсутствием доказательств, подтверждающих нарушение им условий коллективного договора.

К аналогичным выводам приходят и другие суды (например, определение Свердловского областного суда от 09.04.2014 г. по делу № 33-4961/2014).

§ 2. Направление запроса о предоставлении персональных данных работников, не связанного с защитой коллективных прав работников

Первичная профсоюзная организация работников ГБУЗ «Самарский областной наркологический диспансер» (далее — ГБУЗ «СОНД») обратилась в суд с иском о признании незаконными действий главного врача по непредоставлению профсоюзу информации о социально-трудовых вопросах в организации, которая содержится в многочисленных документах ГБУЗ «СОНД». К запрашиваемым профсоюзом документам относились устав, коллективный трудовой договор, правила внутреннего трудового распорядка ГБУЗ «СОНД»; положения об оплате труда работников с имеющимися приложениями; размеры должностных окладов, тарифных ставок, тарифных разрядов, квалификационных групп должностей, установленных и действующих в данное время в организации; штатное расписание на 2011–2012 гг., положения всех структурных подразделений о распределении денежных средств, полученных от предпринимательской деятельности (оказание платных медицинских услуг); копия положения об оплате (доплате) сотрудникам административно-хозяйственной службы за счет средств, полученных от предпринимательской деятельности (оказание платных медицинских услуг); перечень расходных статей резервного фонда диспансера; положения о начислении надбавки за классность водителям ГБУЗ «СОНД»; перечень работ с вредными и опасными условиями труда, на которые устанавливаются доплаты; перечень профессий работников диспансера, которым предоставляется дополнительный отпуск за работу во вредных и тяжелых условиях труда; информация о количестве дней дополнительного отпуска работникам ГБУЗ «СОНД» за работу во вредных и опасных условиях труда (по перечню); положение о премиальных выплатах и о порядке доплат за совмещение, замещение, расширение зоны обслуживания, увеличение объема работ, выполнение обязанностей временно отсутствующего работника; копия тарификационных списков по квалификационным уровням на 2011–2012 гг.; перечень профессий и должностей работников ГБУЗ «СОНД», которым положена бесплатная выдача спецодежды и обуви, санитарной одежды и обуви, других средств индивидуальной защиты; положение о бесплатной выдаче спецодежды, спецобуви и других средств индивидуальной защиты, смывающих и обезвреживающих средств в соответствии с установленными нормами работникам ГБУЗ «СОНД», занятым на работах с вредными и (или) опасными условиями труда, а также на работах связанных с загрязнением, и проч.

Суд постановил, что работодатель обязан предоставить профсоюзу документы, связанные с защитой социально-трудовых прав работников. В рассматриваемом случае этими документами являются устав организации, коллективный договор, правила внутреннего трудового распорядка, положение об оплате труда работников организации, перечень работ с вредными и опасными условиями труда, на которые устанавливаются доплаты, перечень профессий работников организации, которым предоставляется дополнительный отпуск за работу во вредных и опасных условиях труда. Предоставление остальных документов необходимо только с письменного разрешения работников, поскольку они содержат персональные данные работников, что не отвечает целям защиты их социально-трудовых прав[1].

§ 3. Предоставление персональных данных работников по запросу третьих лиц

Нередко к работодателю с запросом о предоставлении персональных данных работников обращаются его акционеры. Так, ООО «Новый капитал», ООО «Инвестиционная инициатива», ООО «Вега», являясь акционерами ОСАО «Ингосстрах», владеющими частью обыкновенных акций ОСАО «Ингосстрах», обратились в ОСАО «Ингосстрах» с требованием о предоставлении документов, предусмотренных п. 1 ст. 89 Федерального закона «Об акционерных обществах», в том числе копии действующего трудового договора, заключенного с генеральным директором общества.

Как следует из материалов дела, ООО «Новый капитал», ООО «Инвестиционная инициатива», ООО «Вега» считают, что акционеры в соответствии с Федеральным законом «Об акционерных обществах» имеют право на получение трудового договора с генеральным директором ОСАО «Ингосстрах».

ФАС Московского округа указал, что работодатель правомерно не представил акционерам общества копию трудового договора с генеральным директором, поскольку ст. 88 ТК РФ установлен запрет на передачу персональных данных работника третьей стороне, а в соответствии со ст. 90 ТК РФ лица, виновные в нарушении норм, регулирующих защиту персональных данных, несут административную, гражданско-правовую или уголовную ответственность[2].

---

[1] См.: постановление Куйбышевского районного суда г. Самары от 26 ноября 2012 г. № 2-1417.

[2] См.: постановление ФАС Московского округа от 14 января 2010 г. № КА-А40/14463-09 по делу № А40-38438/09-17-269.

Как следует из материалов дела, суд пришел к выводу о том, что предоставление персональных данных работника регулируется специальным законодательством. В рассматриваемом случае специальным законодательством является Федеральный закон «О персональных данных» и ТК РФ по отношению к Федеральному закону «Об акционерных обществах».

Итак, третьи лица не имеют права запрашивать персональные данные работника, если это прямо не установлено законодательством, регулирующим предоставление персональных данных работника.

Исходя из правовых позиций, высказанных различными судами Российской Федерации, можно заключить, что когда запрос информации, содержащей персональные данные работников, исходит от профессионального союза, работодателю следует учесть цели запроса информации. При осуществлении запроса, связанного с защитой профессиональным союзом коллективных трудовых прав работников, работодатель обязан выдать профсоюзу необходимые документы без согласия работников (например, коллективный договор); когда речь идет не о защите социально-трудовых прав работников, работодатель должен получать согласие каждого работника на передачу его персональных данных.

§ 4. Хранение работодателем персональных данных работников, содержащихся в копиях документов

Статья 65 ТК РФ предусматривает предоставление документов при трудоустройстве на работу, но закон не устанавливает порядка ведения личного дела работника и не отвечает на вопрос о возможности хранения копий документов работника. Тем не менее копии документов работников содержат их персональные данные.

Так, ЗАО «Банк Русский Стандарт» обратилось в арбитражный суд Ростовской области с заявлением о признании недействительным предписания Управления Федеральной службы по надзору в сфере связи информационных технологий и массовых коммуникаций по Ростовской области № П-61–0036 от 15 апреля 2013 г. об устранении нарушений ч. 5 ст. 5 и ч. 1 ст. 10 Закона № 152-ФЗ.

При исследовании доказательств по делу судом было установлено, что в период с 8 апреля 2013 г. по 15 апреля 2013 г. на основании приказа руководителя Управления Роскомнадзора от 14 марта 2013 г. № 227 управлением была проведена плановая выездная проверка в отношении ЗАО «Банк Русский Стандарт» (филиала ЗАО «Банк Русский Стандарт» в г. Ростове-на-Дону). В ходе проверки установлено, что филиал банка без письменного согласия субъектов персо-

нальных данных или иного законного основания обрабатывает специальную категорию персональных данных — национальность, указанную в копиях свидетельства о заключении брака, свидетельства о рождении ребенка, что является нарушением ч. 1 ст. 10 Закона № 152-ФЗ.

Управление Роскомнадзора в обоснование своей позиции ссылалось на то, что обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением случаев, когда субъект персональных данных дал согласие на обработку своих персональных данных (ч. 2 ст. 10 Закона № 152-ФЗ).

Банк предоставил суду в качестве доказательства локальный нормативный акт — Положение банка о персональных данных, которым определялось место хранения персональных данных работников и устанавливался перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ в лице сотрудников соответствующих подразделений банка. Кроме того, судом установлено, что в отношении всех выявленных сотрудников имеется письменное согласие на обработку персональных данных и хранение копий документов, в которых содержатся персональные данные работников.

Заявитель ссылался на то, что копии указанных документов работника были необходимы для назначения выплаты последнему государственных пособий. Так, в соответствии с ч. 1 ст. 13 Федерального закона от 29 декабря 2006 г. № 255-ФЗ «Об обеспечении пособиями по временной нетрудоспособности, по беременности и родам граждан, подлежащих обязательному социальному страхованию, назначение и выплата пособий по временной нетрудоспособности, по беременности и родам, ежемесячного пособия по уходу за ребенком осуществляются страхователем по месту работы (службы, иной деятельности) застрахованного лица.

Согласно приказу Минздравсоцразвития России от 23 декабря 2009 г. № 1012н «Об утверждении Порядка и условий назначения и выплаты государственных пособий гражданам, имеющим детей» для назначения и выплаты ежемесячного пособия по уходу за ребенком представляются:

а) заявление о назначении пособия;

б) свидетельство о рождении (усыновлении) ребенка (детей), за которым осуществляется уход, и его копия либо выписка из решения об установлении над ребенком опеки; свидетельство о рождении ребенка, выданное консульским учреждением Российской Федера-

ции за пределами территории Российской Федерации, — при рождении ребенка на территории иностранного государства и его копия, а в случаях, когда регистрация рождения ребенка произведена компетентным органом иностранного государства, и т.д.

Для назначения единовременного пособия беременной жене военнослужащего, проходящего военную службу по призыву, представляются в том числе:

а) заявление о назначении пособия;

б) копия свидетельства о браке.

Постановлением Правительства РФ от 6 июля 1998 г. № 709 «О мерах по реализации Федерального закона «Об актах гражданского состояния» утверждены формы свидетельства о браке и свидетельства о рождении ребенка. Указанные формы свидетельств предусматривают графу «национальность», заполняемую по желанию супругов (родителей).

Получение филиалом банка, являющимся страхователем, копий свидетельств о рождении, о заключении брака в целях назначения и выплаты работникам государственных пособий в обозначенных выше случаях, предусмотренных законодательством об обязательном социальном страховании, связано с необходимостью исполнения требований указанного законодательства, а представление указанных документов филиалу банка работниками основано на волеизъявлении последних. Учитывая, что действующим законодательством предусмотрена обязанность застрахованных лиц представить страхователю (работодателю) копии указанных свидетельств для назначения и выплаты им государственных пособий, гражданин при принятии решения о раскрытии сведений о национальной принадлежности в получаемых им свидетельствах осознает, что указанные сведения в дальнейшем могут стать известными третьим лицам, а именно работодателю (страхователю) и органам обязательного социального страхования.

На основании вышеизложенного арбитражный суд Ростовской области в решении от 28 августа 2013 г. по делу № А53-13327/13 признал недействительным предписание Управления Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Ростовской области № П-61–0036 от 15 апреля 2013 г., выданное ЗАО «Банк Русский Стандарт».

Управление Роскомнадзора по Ростовской области обратилось в апелляционную, а затем и в кассационную инстанцию. Суд апелляционной инстанции сделал вывод о том, что для идентификации личности при приеме на работу достаточно фамилии, имени и отчества, при условии предъявления лицом документа, удостоверяюще-

го личность, в котором содержатся все необходимые сведения. Хранение копий паспорта, страниц военного билета, свидетельства о заключении брака, свидетельства о рождении ребенка на рабочем месте действующим законодательством не предусмотрено, нарушает права и свободы гражданина, снижает уровень прав и гарантий работника, противоречит федеральному законодательству, поскольку превышает объем обрабатываемых персональных данных работника. При проведении проверки Управление Роскомнадзора сделало правильный вывод о том, что банк производит обработку избыточных персональных данных по сравнению с теми, которые определены к заявленным целям их обработки, что является нарушением ч. 5 ст. 5 Закона № 152-ФЗ.

Однако постановлением от 17 декабря 2013 г. № 15АП-16132/2013 по делу № А53-13327/2013 Пятнадцатый арбитражный апелляционный суд отменил решение суда первой инстанции.

В отзыве на кассационную жалобу банка постановление ФАС Северо-Кавказского округа от 21 апреля 2014 г. по делу № А53-13327/2013 оставило решение апелляционной инстанции без изменения как законное и обоснованное, а кассационную жалобу — без удовлетворения.

В аналогичном случае общество с ограниченной ответственностью «МЕТРО Кэш энд Керри» обратилось в суд с заявлением к Управлению Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Ростовской области о признании недействительным предписания № П-61-0031 от 5 апреля 2013 г. об устранении выявленных нарушений. Управление Роскомнадзора при проверке установило, что в личных делах работников ООО «МЕТРО Кэш энд Керри» хранились копии паспортов.

Исследовав все обстоятельства дела, судом первой инстанции сделан вывод о том, что для идентификации личности при приеме на работу достаточно фамилии, имени и отчества при условии предъявления лицом документа, удостоверяющего личность. Сбор информации о серии и номере паспорта, годе и месте рождения, о поле является избыточным. И конечно, копирование страниц паспорта также порождает дополнительные риски для общества.

Собирая и храня в документах по кадровому учету копии страниц паспортов работника, общество превысило объем обрабатываемых персональных данных работника, установленный Конституцией РФ, ТК РФ и иными федеральными законами.

Решением суда от 14 ноября 2013 г. обществу в удовлетворении заявленных требований отказано по причине того, что к незаконно

обрабатываемым персональным данным работников относятся копии страниц паспорта, фотографии работников.

Пятнадцатый арбитражный апелляционный суд в постановлении от 14 марта 2014 г. по делу № 15АП-22502/13 оставил решение суда первой инстанции в силе.

Аналогичные судебные решения принимались и другими судебными инстанциями (например, постановление Семнадцатого арбитражного апелляционного суда от 10 июня 2015 г. № 17 АП-5329/15, постановление Девятого арбитражного апелляционного суда от 20 октября 2016 г. № 40 АП-195209/16).

Таким образом, хранение копий документов работников работодателем не должно превышать объем обрабатываемых персональных данных работника, установленный Конституцией РФ, ТК РФ и иными федеральными законами. Судебная практика в отношении правомерности хранения документов исходит из того, что работодатель не имеет права хранить копии документов работника, поскольку тем самым он превышает объем запрашиваемых персональных данных работника. При запросе необходимых документов у работника работодателям следует ознакамливаться с оригиналами либо копиями этих документов, своевременно уничтожая либо возвращая работнику копии его документов.

Глава 8
ДАННЫЕ ЭЛЕКТРОННОЙ ПЕРЕПИСКИ И ИНЫЕ ЭЛЕКТРОННЫЕ ДОКАЗАТЕЛЬСТВА

Верную тенденцию отметил судья Семнадцатого арбитражного апелляционного суда В.Г. Голубцов: «В настоящее время можно говорить о том, что идет процесс повсеместной конкуренции цифры и классики»[1]. Обосновывая материализовавшуюся в законе идею о приравнивании электронных документов к письменным доказательствам (ч. 3 ст. 75 АПК РФ, ч. 1 ст. 71 ГПК РФ, ч. 1 ст. 70 КАС РФ), он отметил наряду с ней две конкурировавшие ранее концепции: «электронный документ как вещественное доказательство» и «электронный документ как самостоятельное средство доказывания»[2]. При этом особенностью электронных документов является наличие в них дополнительной информации в виде метаданных: о дате, месте создания и редактирования, о лице, об отправителе и получателе сообщений, о факте внесения в метаданные изменений. Предполагается, что внедрение технологии распределенных реестров в систему шифрования электронной переписки позволит наделить ее метаданные свойствами неопровержимой идентификации[3]. В условиях, когда метаданные электронных документов получат статус неопровержимого с точки зрения технологической защищенности доказательства, они вполне могут быть наделены особым статусом в процессуальном законодательстве. Однако сейчас суды, рассматривая представляемые в материалы дела сторонами данные переписки, лог-файлы, распечатки свойств файла, сталкиваются с различными подходами, которые зависят от совокупности иных имеющихся по делу доказательств, а также от совершения или несовершения противоположной стороной определенных процессуальных действий. Поскольку использование таких данных против стороны судебного разбирательства подразумевает также обработку персональных данных, этот вопрос следует рассмотреть специально.

---

1 Голубцов В.Г. Электронные доказательства в контексте электронного правосудия // Вестник гражданского процесса. 2019. № 1. С. 170.

2 Там же. С. 179.

3 См.: Антонян Е.А., Аминов И.И. Блокчейн-технологии в противодействии кибертерроризму // Актуальные проблемы российского права. 2019. № 6. С. 167–177.

§ 1. Электронная переписка в мессенджерах

В удовлетворении ходатайства об истребовании логина и пароля электронного почтового ящика суды отказывают, поскольку в переписке содержатся персональные данные третьих лиц. Так, в постановлениях арбитражного суда Северо-Кавказского округа по делам об обжаловании определений об отказе в истребовании доказательств в виде данных логина и пароля почтовых ящиков должника по делу о банкротстве (от 16 августа 2019 г. по делу № А53-23516/2017, от 15 июля 2019 г. по делу № А53-23514/2017) отмечено: «Суды, оценив представленные в материалы дела пояснения об отсутствии технической возможности подтверждения соответствия личных данных физического лица в отношении должника какому-либо адресу электронного почтового ящика и поиска в системе электронного почтового ящика по регистрационным данным пользователя, принимая во внимание отсутствие обоснования необходимости получения доступа к аккаунтам, логина и пароля, распечатки переписки за последние пять лет, а также учитывая, что получение доступа к электронной переписке обеспечит доступ не только в отношении персональных данных, личной тайны должника, но и в отношении личной тайны и персональных данных третьих лиц, чьи права и законные интересы могут быть нарушены, принимая во внимание необходимость соблюдения баланса интересов должника, конкурсных кредиторов и третьих лиц, правомерно отказали в удовлетворении заявленных требований. Суды пришли к правильному выводу о том, что управляющим не приведены доказательства того, что испрашиваемая информация обеспечит формирование конкурсной массы должника. Основания для переоценки выводов судебных инстанций у суда кассационной инстанции отсутствуют (статьи 286 и 287 Арбитражного процессуального кодекса Российской Федерации)»[1].

Неправомерность получения доступа к электронной переписке и обработки содержащейся в ней информации была признана также в апелляционном определении Московского городского суда от 16 сентября 2015 г. по делу № 33-30344/2015, где отмечено: «ответчик, размещая рекламу в сообщении истца, руководствовался результатами мониторинга электронной корреспонденции истца, тем самым нарушил тайну его переписки. Доказательств об обратном со стороны ответчика судебной коллегии не представлено. Поскольку право

[1] Полагаем, указанный подход о необходимости баланса при решении вопроса об истребовании персональных данных корреспондирует обозначенному в определении КС РФ от 29 января 2009 г. № 3-О-О. См. § 2 гл. 1 настоящего комментария.

Б. на тайну переписки, закрепленное ч. 2 ст. 23 Конституции РФ, по средствам электронной почты продукта Google нарушено действиями ООО "Гугл", то судебная коллегия находит заявленные исковые требования Б. в части обязании ответчика ООО "Гугл" прекратить данное нарушение в отношении истца обоснованными и подлежащими удовлетворению».

Переписка в мессенджере или по электронной почте признается допустимым доказательством, если стороны ее признают (не оспаривают). В частности, при разрешении вопроса о факте признания долга в электронной переписке между хозяйствующими субъектами ВС РФ отметил необходимость по заявлению стороны проверить полномочия лица, признавшего долг, на осуществление данных действий от имени компании, несмотря на то, что электронное письмо с признанием долга исходило с электронного адреса, не относящегося к компании-стороне. При этом факт допустимости электронного письма о признании долга в качестве доказательства признавался в связи с тем, что вторая сторона его не оспаривала (определение Судебной коллегии по экономическим спорам ВС РФ от 17 января 2019 г. по делу № А84-130/2016).

В апелляционном определении Московского городского суда от 18 февраля 2019 г. по делу № 33-7640/2019 суд отметил, что «принял во внимание переписку из мобильного приложения для обмена электронными сообщениями "ВатсАп", содержание и факт участия в которой стороны не оспаривали. Исходя из указанной переписки суд установил, что намерения заявителя ... вселиться в спорную комнату, в которой она никогда не проживала, не имелось, а преследовались... иные цели, поскольку переписка содержит высказывания... подтверждающие доводы истца о том, что регистрация в спорной комнате была приобретена... за деньги с целью получения материальной выгоды в перспективе при сносе дома. Напротив, представленная в дело смс-переписка сторон, которая стороной ответчика не оспаривалась, свидетельствует об обратном». Таким образом, факт отсутствия возражений относительно приобщения к материалам дела спорной переписки, а также в части ее допустимости в качестве доказательства позволили суду на ее основании установить факт волеизъявления.

Переписка в мессенджере для допустимости ее использования должна быть согласована сторонами договора. На вытекающую из закона недопустимость использования электронной переписки в качестве доказательства по спорам, возникающим из договорных правоотношений, указал Тринадцатый арбитражный апелляционный суд в постановлении от 28 июля 2015 г. по делу № А56-60477/2014: «При этом доводы ООО "Сайтека" об обратном со ссылкой на пред-

ставленную в материалы дела переписку сторон правомерно не приняты судом первой инстанции во внимание, поскольку в силу части 3 статьи 75 АПК РФ документы, полученные посредством факсимильной, электронной или иной связи, в том числе с использованием информационно-телекоммуникационной сети «Интернет», а также документы, подписанные электронной подписью или иным аналогом собственноручной подписи, допускаются в качестве письменных доказательств в случаях и в порядке, которые установлены настоящим Кодексом, другими федеральными законами, иными нормативными правовыми актами или договором либо определены в пределах своих полномочий Верховным Судом Российской Федерации, что не имело место в рассматриваемом случае».

Восемнадцатый арбитражный апелляционный суд в постановлении от 8 февраля 2019 г. по делу № А76-24635/2018 разъяснил: «Несмотря на практичность и легкость использования электронной переписки в мобильных приложениях (Viber, WhatsApp и Telegram и др.), сторонам (в рассматриваемом случае — субъектам предпринимательской деятельности) необходимо помнить о доказательственной силе такой переписки в суде и заранее озаботиться фиксацией и сбором доказательств, в данном случае — факта создания программного обеспечения и передачи результата работ заказчику. Между тем данных доказательств не представлено. Как не представлено и доказательств того, что факт блокировки данного мессенджера препятствовал получению соответствующей информации со своего аккаунта. За содействием в получении доказательств к суду ответчик также не обращался, соответствующих ходатайств об истребовании доказательств не заявлено ни суду первой, ни суду апелляционной инстанции (статьи 9, 41, 66, 159 Арбитражного процессуального кодекса РФ)».

В определении Московского городского суда от 5 марта 2019 г. № 4г-0798/2019 по делу № 2-1623/18 указано: «скриншоты сообщений в мессенджере WhatsApp являются недопустимыми доказательствами в связи с отсутствием возможности установить отправителя сообщений; нотариально удостоверенный протокол осмотра электронной переписки в мобильном приложении не представлен; кроме того, переписка в мессенджере WhatsApp противоречит п. 5.7 спорного договора, в соответствии которым переписка между сторонами осуществляется путем направления корреспонденции заказными письмами с уведомлением».

В постановлении Двадцатого арбитражного апелляционного суда от 22 июля 2019 г. по делу № А68-9131/2018 также указано: «Ссылка заявителя на представленную в материалы дела электронную перепи-

ску в системе Viber правомерно не принята во внимание, поскольку не является допустимым доказательством, такой способ обмена документами, претензиями, уведомлениями между сторонами договором не согласовывался. Представленная ответчиком переписка не свидетельствует о направлении в адрес подрядчика каких-либо претензий в порядке, установленном договором за подписью официального лица компании, а является рабочей перепиской сотрудников в ходе исполнения договора. Из переписки невозможно установить, в чем именно выразилось ненадлежащее качество работы, по каким адресам, срок устранения и отсутствие факта такого устранения. Переписка не позволяет установить, что адресована представителю истца, уполномоченного принимать юридически значимые сообщения».

В постановлении Двадцатого арбитражного апелляционного суда от 4 марта 2019 г. по делу № А68-5552/2018 также подчеркивается: «пункт 5.1 договора содержит исчерпывающий перечень способов уведомления подрядчика о выявленных недостатка по качеству и периодичности оказания услуг, а именно: заказчик при обнаружении недостатков выполненных услуг обязан уведомить факсограммой/телефонограммой/письмом подрядчика о ставших ему известных фактах выявленных недостатков. Указанный пункт договора не содержит иных способов уведомления подрядчика. Таким образом, суд первой инстанции пришел к правильному выводу о том, что представленная в материалы дела электронная переписка в системе Viber по смыслу приведенных норм и условий договора не является допустимым доказательством, поскольку такой способ обмена документами, претензиями, уведомлениями между сторонами договором не согласовывался».

Девятый арбитражный апелляционный суд в постановлении от 11 марта 2019 г. по делу № А40-213949/18 отметил: «Доказательства переписки в интернет-мессенджере WhatsApp (мобильного приложения для обмена сообщениями и аудио-, видеофайлами) могут быть признаны судом в качестве допустимого письменного доказательства в случаях и порядке, предусмотренных законом, и в любом случае должны содержать обязательный признак: отправитель и получатель должны быть идентифицированы. Представленная истцом переписка в мессенджере WhatsApp не отвечает этим признакам. Из переписки не представляется возможным достоверно установить принадлежность телефонных номеров истцу и ответчику, в том числе то, что указанный ответчиком А. является представителем истца. Кроме того, ответчиком не представлено доказательств, что сторонами договора была предусмотрена возможность обмениваться сообщениями в мессенджере, с указаниями номеров телефона в самом догово-

ре. В этой связи достоверно установить, что сообщение исходит именно от контрагента, не представляется возможным. Факт ведения представленной переписки в мессенджере истец не подтвердил в ходе судебного разбирательства. Кроме того, представленная распечатка переписки также не может быть принята судом в качестве доказательства, так как не может быть признана допустимой без подтверждения подлинности. Более того, суд не может достоверно установить дату получения такого доказательства».

Таким образом, недостатком переписки в рамках рассмотрения дел о заключении договора или о его исполнении является отсутствие подтверждаемого ею необходимого юридического состава:

– о соблюдении существенных условий договора;

– о действительности волеизъявления лица, направившего сообщение;

– об идентификации адресата сообщения;

– о наличии у адресата сообщения полномочий на совершение юридически значимых действий;

– о согласовании порядка доставки юридически значимых сообщений посредством мессенджеров или электронной почты.

Вместе с тем встречаются ситуации, в которых указанные требования не соблюдаются. Например, в постановлении Седьмого арбитражного апелляционного суда от 9 января 2019 г. по делу № А03-3991/2018 суд постановил: «В связи с чем довод апелляционной жалобы о представлении истцом недопустимого доказательства в качестве подтверждения факта поставки некачественного товара — переписки в мессенджере WhatsApp, отклоняется апелляционной инстанцией, поскольку истцом представлена не только указанная переписка, но также и другие доказательства... что образует совокупность надлежащих доказательств, которая ответчиком по правилам статей 65, 67, 68 иными относимыми и допустимыми доказательствами не опровергнута».

В постановлении Седьмого арбитражного апелляционного суда от 23 января 2019 г. по делу № А27-15834/2018 по делу о взыскании задолженности и неустойки по договору поставки указано: «На протяжении всего вышеуказанного периода истец неоднократно предпринимал попытки урегулировать спор с представителями ответчика путем телефонных переговоров, переговоров посредством мобильного приложения WhatsApp (копии переписки, записи разговоров сторон с мобильного приложения WhatsApp прилагаются к материалам дела), однако ответчик, не определяя конкретных сроков, ссылался на допоставку товара в будущем, свои обязательства по государственному контракту не выполнял».

Следовательно, электронная переписка в рамках договора (хотя, возможно, это особенность правоотношений с государственными и муниципальными заказчиками) может быть принята в качестве допустимого доказательства даже при отсутствии необходимого согласования порядка ее использования сторонами на этапе подписания договора.

В постановлении Семнадцатого арбитражного апелляционного суда от 5 декабря 2018 г. по делу А50-10952/2018 судом в рамках электронной переписки в социальной сети «ВКонтакте» и мессенджере «Телеграм» в совокупности с содержанием и вложенными документами по согласованной сторонами электронной почте установлено, что таким образом стороны обменивались документами, удостоверяющими личность, и доверенностями, передача которых также согласовывалась по электронной почте. Суд отметил: «Достоверность сведений, отраженных в представленной переписке, истцом документально не опровергнута. Кроме того, как верно указал суд первой инстанции, представленные переписка и письменные пояснения ООО "Стил Пауэр Нутришн" позволяют соотнести ведущих данную переписку лиц и содержание переписки с обстоятельствами настоящего дела и участвующими в деле лицами».

В постановлении Седьмого арбитражного апелляционного суда от 7 апреля 2016 г. по делу № А67-8923/2015 также указано: «Между сторонами настоящего спора сложился электронный документооборот, что следует из электронной переписки, которая велась между Петроченко В., бизнес-аналитиком ООО "Сибэдж", с электронного почтового адреса PetrochenkoVA@ sibedge.com и А.В. Высоцкой, помощником директора ООО "МОЙЕ Керамик-Имплантате", с электронного почтового адреса annavysotskaya85@gmail.com, а также между А. Подлесных, руководителем отдела продаж ООО "Сибэдж", с электронного почтового адреса podlesnykhav@sibedge.com и А.В. Высоцкой, помощником директора ООО "МОЙЕ Керамик-Имплантате" с электронного почтового адреса vysotskaya_a_v@moje-keramik.ru. Суд первой инстанции с учетом предусмотренных договором условий и обстоятельств дела пришел к обоснованному выводу о том, что представленная электронная переписка позволяет установить факт оказания исполнителем заказчику услуг, является достоверным доказательством передачи и получения заказчиком указанных материалов по электронной почте».

Таким образом, допустимость электронной переписки подтверждается, если возможно идентифицировать адресатов такой переписки. Подобная идентификация может быть подтверждена однородностью сообщений, полученных путем использования согласованных договором и не согласованных способов ведения переписки.

Достоверность переписки может подтверждаться показаниями свидетелей. В постановлении Шестнадцатого арбитражного апелляционного суда от 5 сентября 2018 по делу № А63-3050/2018 указано: «Поскольку сообщения в мобильном приложении были направлены от представителя ООО "Эко-Сити" в адрес ООО "Полигон Яр", названные сообщения являлись юридически значимыми сообщениями для последнего. Кроме того, из показаний свидетелей следует, что в сложившихся между сторонами правоотношениях существовала практика использования мобильного приложения WhatsApp для направления документов либо передачи сведений. В связи с чем довод ответчика о том, что переписка в мобильном приложении не является документом, представляет собой разговор двух лиц и не может считаться надлежащим доказательством, не принимается судом».

В рамках споров о признании договора заключенным электронная переписка была оценена в качестве допустимого доказательства в постановлении Восьмого арбитражного апелляционного суда от 26 июля 2019 г. по делу № А70-3154/2019: «Пунктом 3 статьи 434 ГК РФ закреплено, что письменная форма договора считается соблюденной, если письменное предложение заключить договор принято в порядке, предусмотренном пунктом 3 статьи 438 ГК РФ, согласно которому совершение лицом, получившим оферту, в срок, установленный для ее акцепта, действий по выполнению указанных в ней условий договора (отгрузка товаров, предоставление услуг, выполнение работ, уплата соответствующей суммы и т.п.) считается акцептом, если иное не предусмотрено законом, иными правовыми актами или не указано в оферте. Как установлено судом первой инстанции, договор от 23 июля 2018 г., подписанный со стороны предпринимателя, в материалы дела не представлен, стороны обменивались сообщениями относительно выполнения работ по производству стойки администратора посредством мессенджера, мобильного приложения Viber; соответствующая переписка нашла свое отражение в условиях указанного договора, дополнительном приложении к нему. Как разъяснено в пункте 7 информационного письма Президиума ВАС РФ от 25 февраля 2014 г. № 165 "Обзор судебной практики по спорам, связанным с признанием договоров незаключенными", при наличии спора о заключенности договора суд должен оценивать обстоятельства дела в их взаимосвязи в пользу сохранения, а не аннулирования обязательств, а также исходя из презумпции разумности и добросовестности участников гражданских правоотношений, закрепленной статьей 10 ГК РФ. Если стороны не согласовали какое-либо условие договора, относящееся к существенным, но затем совместными действиями по исполнению договора и его

принятию устранили необходимость согласования такого условия, то договор считается заключенным. Исходя из фактических обстоятельств спора, суд соглашается с квалификацией судом первой инстанции правоотношений сторон в качестве подрядных».

В судебной практике также встречаются дела, возникающие из трудовых правоотношений, в рамках которых стороны пытаются использовать переписку в мессенджерах в качестве доказательств. В апелляционном определении Московского городского суда от 16 мая 2017 г. № 33-13015/2017 также отмечено: «Из материалов дела следует, что в обоснование исковых требований и в подтверждение факта трудовых отношений Г.О.С., ссылалась на переписку по электронной почте с П.И., представлявшейся экспертом по развитию бизнеса компании BOX2BOX, и на переписку, сделанную с использованием мобильного приложения WhatsApp, не содержащую сведений об ООО "ЛИМ", а также на платежные документы, которые, по мнению истца, подтверждали изготовление визитных карточек для нее, трудовой договор, подписанный с ее стороны, письма иных организаций. Разрешая спор, суд первой инстанции обоснованно исходил из того, что со стороны истца не было представлено надлежащих и достаточных доказательств, с достоверностью подтверждающих наличие между сторонами трудовых отношений, а представленные документы не свидетельствуют о фактическом допуске истца к выполнению трудовой функции по определенной должности на постоянной основе в течение полного рабочего дня, при этом суд обоснованно учел, что допуск до работы уполномоченным лицом по указанной истцом должности в ООО "ЛИМ" не осуществлялся, в связи с чем, учитывая, что доказательств обратного представлено не было, пришел к верному выводу об отказе в удовлетворении заявленных исковых требований об установлении факта трудовых правоотношений и, как следствие, правомерно отказал в удовлетворении исковых требований в остальной части как производных. Судебная коллегия с указанными выводами суда соглашается, поскольку они подтверждаются материалами дела и не противоречат требованиям закона».

Следует отметить, что переписка в мессенджере может быть допустимым доказательством, если она засвидетельствована нотариально. При этом на практике суды хотя и принимают во внимание, что заверенный нотариусом документ является обстоятельством, не подлежащим доказыванию, но все же критически относятся к таким доказательствам, поскольку нотариальное заверение подтверждает факт и содержание переписки, но не его адресатов и допустимость такой переписки в правоотношениях сторон. Таким образом, при от-

сутствии других доказательств нотариальное заверение переписки не влечет за собой дополнительного доказательственного значения.

В постановлении Девятого арбитражного апелляционного суда от 18 апреля 2019 г. по делу № А40-220968/18 подчеркивается: «Скриншоты (снимки с экрана) электронной переписки рассматриваются судом наряду с другими доказательствами и при отсутствии нотариального заверения. Факт соответствия адреса электронной почты ответчику подтверждается содержанием сообщений (в тексте сообщения упоминается точное наименование договора, дата его заключения, даты заключения приложений к договору, а также точная стоимость услуг по договору, точные наименования юридических лиц истца и ответчика), а также доменом адреса электронной почты, который соответствует домену официального сайта ответчика. Данные сведения позволяют с точностью идентифицировать стороны электронной переписки».

Изложенное позволяет заключить, что при ссылках на данные электронной переписки следует делать акцент на совокупность иных косвенных доказательств, которые позволят принять во внимание такую переписку в качестве допустимого доказательства.

§ 2. Использование электронной переписки при рассмотрении уголовных дел

Полученная в ходе предварительного расследования переписка является допустимым доказательством, даже если в материалы дела не представлено сведений о порядке ее извлечения. Апелляционное определение Судебной коллегии по уголовным делам ВС РФ от 1 марта 2017 г. № 38-АПУ17-2 содержит такую формулировку: «Отказ свидетелей Б. и М. дать показания относительно технического способа получения ими информации о ведении Е. и Т. переписки в сети "Интернет" с использованием программы ICQ не противоречит положениям ст. 12 Федерального закона "Об оперативно-розыскной деятельности", в силу которых указанные данные составляют государственную тайну». Как видится, подобные доказательства, исследованные в рамках уголовных дел, могут использоваться в последующем и по связанным с ними гражданским делам.

В рамках уголовных дел судами также принимаются во внимание графические изображения, содержащиеся в памяти телефона либо иных устройств. Например, в апелляционном определении Московского городского суда от 6 августа 2019 г. по делу № 33-32729/2019 суд отметил, что «в памяти мобильных устройств, принадлежащих П., С. и М., сохранилась переписка, осуществляемая в сети "Интер-

нет". Содержание данной переписки и графические изображения свидетельствуют об участии П. и С. в незаконном сбыте наркотических средств. В частности, неустановленному лицу было известно, что родная сестра П. работает оператором в почтовом отделении, в которое поступали отправления с наркотиками. Переписка С. содержит фотоснимки оборудованных тайников, а также поручение о необходимости извлечения наркотического средства, сокрытого в тайнике у кафе "Дубрава"». В рамках данного дела не исследовались даты и время снимка. Сам факт фиксации мест, где впоследствии были обнаружены закладки с наркотиками, по мнению суда, в совокупности с иными доказательствами свидетельствовал о причастности подсудимого к совершению преступления.

Московский городской суд в определении от 21 февраля 2017 г. № 10-1672/2017 отметил, что доводы стороны защиты в жалобах и аналогичные доводы в ходе рассмотрения дела о том, что переписка в социальных сетях не является доказательством, что личный компьютер и телефон К.М. изъяты с нарушением УПК РФ, при изъятии вещей К.М. не составлялся протокол личного досмотра или протокол осмотра помещения, с момента фактического задержания К. до момента выемки телефона и ноутбука прошли сутки и у сотрудников полиции была возможность использовать телефон и компьютер с целью "подтасовки" переписки в смс-сообщениях, рассмотрены судом первой инстанции и верно признаны несостоятельными. Сам К. не отрицал наличия переписки и общения по телефону с потерпевшей К. При этом в указанном судебном акте не отмечено, что подсудимый подтвердил факт переписки.

Таким образом, собранные в рамках расследования уголовного дела органами предварительного расследования данные переписки могут быть исследованы и использованы в качестве доказательства по уголовному делу в силу закона. При этом порядок исследования такой переписки, извлечения сведений из памяти электронного устройства либо иным способом специально не регламентирован. Особое значение придается отрицанию факта переписки подсудимого на всех стадиях уголовного преследования.

В настоящее время у судов сохраняется критическое отношение к использованию материалов электронной переписки в качестве доказательств, если порядок ведения такой переписки не был согласован сторонами. При этом отсутствуют примеры, когда стороны в подтверждение относимости и допустимости к материалам дела представляли иные доказательства: подтверждение принадлежности номера телефона, на который зарегистрирован мессенджер, конкретному лицу путем запроса, направляемого оператору связи напрямую,

либо путем судебного истребования доказательств. Кроме того, встроенные в мессенджеры функции о предоставлении данных геолокации в ходе переписки, либо иные технологические средства определения адресата переписки также не встречались. Как представляется, развитие технологий идентификации адресатов переписки позволит в дельнейшем избегать проблем с допустимостью доказательств при условии соблюдения требований к содержанию юридически значимых сообщений, предусмотренных законом для конкретных правоотношений. Такие доказательства, как метаданные (подтверждающие факт совершения действий определенным лицом, а также даты создания и изменения файлов), лог-файлы (доказывающие время и продолжительность доступа к серверу) и т.д., использование которых является неотъемлемой частью правоприменительного процесса, нуждаются в дополнительных экспертных оценках, результаты которых позволят определить их доказательственное значение.

Глава 9
ЗАЩИТА ПЕРСОНАЛЬНЫХ МЕДИЦИНСКИХ ДАННЫХ: ОПЫТ РОССИИ И ЕВРОПЕЙСКОГО СОЮЗА

Современная медицина непрерывно развивается — разрабатываются новые лекарства, появляются революционные методы лечения, изменяются подходы к диагностике. Все это отражается не только на отрасли в классическом понимании, но и на соответствующих правовых отношениях. Так, в Российской Федерации наблюдается значительный рост правовой грамотности населения в области медицины, а на первый план выходит обеспечение приватности частной жизни и как следствие сохранность личных данных человека и гражданина, включая медицинские данные. Судами все чаще рассматриваются споры о неправомерном разглашении или отказе в предоставлении медицинских сведений, в том числе увеличивается количество подобных дел и в Суде ЕС. Российские суды тоже не оставляют без внимания вопросы правоприменения при нарушении гарантированного гражданину права на сохранение в тайне сведений, отнесенных законом к врачебной тайне, лицами, обязанными ее соблюдать.

При оказании тех или иных услуг частным и государственнымедицинским клиникам становятся известны личные данные пациентов. Понятие персональных данных содержится в п. 1 ст. 3 Закона № 152-ФЗ. Ими признается любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных). Внося информацию в медицинскую карту пациента или составляя договор на оказание медицинских услуг, медицинская организация получает доступ к персональным данным клиента, а значит, обязана обеспечить их защиту. Однако кроме стандартных категорий персональных данных, таких как фамилия, имя, отчество, адрес субъекта, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе и т. д., к персональным данным пациента — медицинским — относятся информация о состоянии его здоровья, диагнозе, заболевании, способе лечения, фактах обращения за медицинской помощью, а также иные сведения, полученные при обследовании и лечении гражданина. В соответствии

с Указом Президента РФ от 6 марта 1997 г. № 188[1] обозначенная информация относится к врачебной тайне. Понятие врачебной тайны расширяется Законом РФ от 2 июля 1992 г. № 3185-1 «О психиатрической помощи и гарантиях прав граждан при ее оказании»[2], который дополняет ее сведениями о наличии у гражданина психического расстройства, фактах обращения за психиатрической помощью и лечении в учреждении, оказывающем такую помощь, а также иными сведениями о состоянии психического здоровья. Разглашение обозначенных сведений может стоить пациенту места работы или даже жизни, поэтому в современном мире остро стоит вопрос о защите такой информации. В ЕС для обозначения медицинских данных используется термин «чувствительные данные» — sensitive data. Однако российские законодатель и суды по факту занимают позицию, согласно которой охраняются только те медицинские сведения, которые можно отнести к врачебной тайне. Разглашение сведений, составляющих врачебную тайну, лицами, которым они стали известны при обучении, исполнении профессиональных, служебных и иных обязанностей, запрещено, в том числе после смерти человека (ст. 13 Федерального закона от 21 ноября 2011 г. «Об основах охраны здоровья граждан в Российской Федерации», далее — Закон № 323-ФЗ). Отсюда следует, что медицинская организация в процессе своей деятельности должна соблюдать требования по защите персональных данных и сохранению врачебной тайны. Этот ограничительный подход к медицинским данным как к врачебной тайне существенно отличается от практики Суда ЕС, которая, на наш взгляд, также представляет интерес для российских правоприменителей и теоретиков.

Прежде чем перейти к анализу российской судебной практики, необходимо однозначно ответить на вопрос, относится ли врачебная тайна к персональным данным. Из положений закона становится понятно, что понятие «персональные данные» несколько шире, чем понятие «врачебная тайна», однако прямого указания в тексте закона на то, что медицинские сведения относятся к персональным данным, нет. Тем не менее это подтверждается судебной практикой. Так, в решении ВС РФ от 1 апреля 2013 г. № АКПИ13-161 указано, что информация о регистрации гражданина по месту пребывания в больнице прямо относится к определенному физическому лицу и входит в состав его персональных данных.

---

1 Указ Президента РФ от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера» // СПС «КонсультантПлюс».

2 Ведомости СНД и ВС РФ. 1992. № 33. Ст. 1913.

Начнем с рассмотрения вопроса о доступе субъекта или его законного представителя к персональным медицинским данным. Здесь необходимо выдерживать баланс — с одной стороны, доступ должен быть возможен без каких-либо препятствий при соблюдении определенных разумных требований, с другой — необходимо обеспечить безопасность таких данных, особенно от злоупотребления со стороны заинтересованных лиц. Показательным в этом отношении является апелляционное определение Московского городского суда от 10 июля 2013 г. по делу № 11-20430/13. Господин М.А.А. обратился в суд с иском к главному врачу городской психиатрической больницы № 14 г. Москвы об обязании выдать документы, ссылаясь на то, что он находился на лечении в указанной больнице с 23 февраля по 1 марта 2013 г. При выписке из больницы ему не был выдан выписной эпикриз. Его отец М.А.С. обратился к главному врачу больницы с просьбой о том, чтобы ему выдали выписку из истории болезни сына и копию истории болезни, однако ему было в этом отказано. Истец просил районный суд обязать главного врача выдать ему выписку из истории болезни и копию истории болезни, однако районный суд отказал в удовлетворении заявления. Тогда М.А.А. подал апелляционную жалобу с просьбой пересмотреть решение Нагатинского районного суда. Апелляционный суд еще раз подтвердил, что в силу ст. 22 Закона № 323-ФЗ пациент либо его законный представитель имеет право непосредственно знакомиться с медицинской документацией, отражающей состояние его здоровья, и получать на основании такой документации консультации у других специалистов. Однако в силу ч. 1 ст. 13 указанного закона сведения о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении, составляют врачебную тайну. Не допускается разглашение сведений, составляющих врачебную тайну. Апелляционный суд указал, что, разрешая исковые требования, районный суд правильно исходил из того, что документы, получения которых требовал представитель истца, содержат врачебную тайну и их выдача может быть осуществлена самому пациенту либо его законному представителю на основании письменного заявления. Из материалов дела усматривается, что к ответчику о выдаче медицинских документов письменно истец либо его представитель с надлежаще оформленными полномочиями не обращались. Суд пришел к выводу, что данные, свидетельствующие о нарушении прав истца, отсутствуют, и отказал в удовлетворении иска.

Таким образом, суды смогли выдержать основанный на законе баланс: с одной стороны, у пациента и его законного представителя

есть юридические инструменты для получения личных медицинских данных, с другой — для этого необходимо строго следовать предписанной процедуре, что позволяет в целом обеспечить надлежащий уровень охраны сведений, относящихся к врачебной тайне.

Наибольшую опасность для субъекта медицинских данных представляет разглашение такой информации. Разглашение врачебной тайны имеет место при опубликовании соответствующих сведений в печати, трансляции по радио-, теле- и видеопрограммам, демонстрации в кинохроникальных программах и других средствах массовой информации, изложении в судебных характеристиках (без специального судебного запроса или однозначно сформулированного судом требования в ходе судебного разбирательства дела), публичных выступлениях, заявлениях, адресованных должностным лицам, или сообщении в любой, в том числе устной, форме нескольким лицам или хотя бы одному лицу[1].

Для вынесения справедливого решения необходимо четко разграничивать, какие персональные медицинские данные составляют врачебную тайну и, следовательно, попадают под действие Закона № 152-ФЗ, а какие — нет. Данный вопрос нередко оказывается в центре внимания судебных разбирательств. Так, Московский городской суд в апелляционном определении от 8 июля 2013 г. по делу № 11-18450/2013[2] рассмотрел жалобу заявителя о нарушении врачебной тайны в отношении информации об отказе в признании его инвалидом. Проверяя доводы истца, суд руководствовался Законом № 323-ФЗ и постановлением Правительства РФ от 20 февраля 2006 г. № 95 «О порядке и условиях признания лица инвалидом»[3]. В соответствии с п. 28 постановления решение о признании гражданина инвалидом либо об отказе в признании его инвалидом принимается простым большинством голосов специалистов, проводивших медико-социальную экспертизу, на основе обсуждения результатов его медико-социальной экспертизы. Само решение объявляется гражданину, проходившему медико-социальную экспертизу (его законному представителю), в присутствии всех специалистов, проводивших медико-социальную экспертизу, которые в случае необходимости дают по нему разъяснения. Основываясь на данной аргументации, суд при-

---

1 См.: Зиновьева О. Врачебная тайна — порядок предоставления сведений и ответственность за их разглашение. URL: https://onegingroup.ru/press-tsentr/analitika/vrachebnaya-tayna-poryadok-predostavleniya-svedeniy-i-otvetstvennost-za-ikh-razglashenie/

2 Система «ГАРАНТ».

3 Российская газета. 2006. № 40. 28 февраля.

шел к выводу о том, что признание гражданина инвалидом либо отказ в признании его инвалидом, объявляемые гражданину, проходившему медико-социальную экспертизу в соответствии с Законом № 323-ФЗ, не являются врачебной тайной, а следовательно, не подлежат охране в соответствии с Законом № 152-ФЗ и Законом № 323-ФЗ.

Таким образом, в Российской Федерации для полноценной защиты персональных медицинских данных они должны быть квалифицированы судом как врачебная тайна. На наш взгляд, такой подход является слишком ограниченным и может мешать полноценной правовой защите персональных медицинских данных. Косвенно на это указывает и незначительное число судебных прецедентов, касающихся утечки медицинской информации. Иной подход прослеживается в практике Суда ЕС.

В отличие от отечественных судебных органов Суд ЕС уделяет особое внимание не только врачебной тайне, но и в принципе любой информации медицинского характера, которая стала известная третьим лицам или была ими разглашена.

Первой посвященной защите персональных данных стала Директива 95/46/ЕС Европейского парламента и Совета ЕС от 24 октября 1995 г. о защите физических лиц в отношении обработки личных данных и о свободном перемещении таких данных[1]. В 2000 году в ее развитие был принят Регламент Европейского парламента и Совета ЕС № 45/2001 от 18 декабря 2000 г. о защите отдельных лиц в отношении обработки персональных данных учреждениями и институтами Сообщества и о свободном перемещении таких данных[2] (далее — Регламент № 45/2001). Регламента не содержал определения «медицинских данных», что вызывало трудности при разрешении споров Судом ЕС, поэтому Суду пришлось давать разъяснения о том, попадают ли медицинские данные о субъекте в сферу действия документа.

Первый прецедент на данную тему был рассмотрен в 2003 г. (дело C-101/01, Lindquist, 6.11.2003)[3]. Заявитель обжаловал действия от-

---

1 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046

2 Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. URL: https://publications.europa.eu/en/publication-detail/-/publication/0177e751-7cb7-404b-98d8-79a564ddc629/language-en

3 Case C-101/01/ Criminal proceedings against Bodil Lindqvist. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62001CJ0101&from=EN

ветчика — миссис Линдквист, которая опубликовала в Интернете данные о своих 18 коллегах без их согласия (имена, место работы, хобби, номера телефонов, семейное положение), а также тот факт, что один из них повредил ногу и находился на больничном. Она удалила данные, как только кто-то из коллег выразил свое несогласие, однако ей все равно было предъявлено обвинение в нарушении законодательства о защите данных. Суду необходимо было ответить на вопрос, является ли информация на домашней странице о том, что упомянутый коллега повредил ногу и находится на больничном по медицинским показаниям, персональными медицинскими данными, которые согласно ст. 8 (1) директивы не могут быть обработаны. Европейский Суд постановил: «информация о том, что человек повредил ногу и находится на больничном, входит в понятие "персональные данные" по смыслу статьи 8 (1), так как это положение следует толковать широко, с тем чтобы охватить все аспекты как физического, так и психического здоровья человека».

Данный кейс дал толчок дальнейшему рассмотрению дел о неправомерном обращении с персональными медицинскими данными.

В деле F-46/09, V & EDPS v. European Parliament ответчик обжалует решение Европейского парламента об отказе заявителю в трудоустройстве на основании профессиональной непригодности. В период с февраля 1997 г. по март 2006 г. заявительница работала с перерывами в нескольких отделах Европейской комиссии (далее — Комиссия) на должности помощника или временного сотрудника совокупно около трех лет. Последняя должность, которую она занимала с сентября 2005 г. по март 2006 г., — помощник в Европейском бюро по борьбе с мошенничеством. 27 февраля 2006 г. заявительница получила уведомление о том, что она прошла отборочные испытания для занятия должности агента по полноценному рабочему контракту. В связи с этим ее имя было включено в окончательную базу данных кандидатов Европейского бюро по отбору персонала, успешно прошедших необходимые тестирования для занятия должности. Статус «успешного кандидата» сохраняется в течение трех лет.

В июне 2006 г. два главных управления Комиссии выразили желание принять на работу заявительницу. Она была приглашена для прохождения медицинского осмотра, по результатам которого должно было быть вынесено решение о ее пригодности для выполнения обязанностей в соответствии со ст. 83 Положений о персонале. 26 июня 2006 г. Медицинская служба Комиссии в Брюсселе (Бельгия) провела медицинское обследование: заявительницу осмотрел доктор К. Уже 29 июня 2006 г. заявительница отправила электронное письмо г-ну Ф., главе медицинской службы Комиссии, с жалобой на

предполагаемое ненадлежащее поведение д-ра К. по отношению к ней во время медицинского осмотра 26 июня 2006 г.

Г-н Ф. принял меры по расследованию жалобы, и несмотря на отсутствие доказательств в отношении фактов ненадлежащего поведения врача К. было решено поручить рассмотрение дела заявителя другому доктору. 26 сентября 2006 г. медицинский работник Комиссии опубликовал медицинское заключение о том, что заявительница физически непригодна для занятия должности. Заявительница попыталась обжаловать данное решение, однако жалоба была отклонена.

Спустя два года заявительница была приглашена для занятия контрактной должности в парламенте. Для окончательного утверждения кандидатуры также было необходимо пройти медицинскую комиссию. Чтобы не затягивать процедуру, парламент запросил копию медицинской карты заявительницы у медицинской службы Комиссии. Оценив состояние здоровья заявительницы на основе предоставленной информации, Парламент отозвал свое предложение о работе на том основании, что она не может работать ни в одном из учреждений ЕС. Заявительница подала жалобу на решение парламента на основании ст. 90 (2) Положений о персонале, которую парламент отклонил. Тогда заявительница решила обратиться в Суд. В исковом заявлении она утверждала, что ее медицинское досье, собранное Комиссией, должно было использоваться только в отношении ее найма Комиссией. По мнению истицы, парламент нарушил право на уважение частной жизни и правила, касающиеся защиты персональных данных, в частности относительно распространения медицинских данных и передачи медицинской карты, а также неправомерности вынесенного медицинским работником парламента решения. Она аргументировала это тем, что:

во-первых, медицинский работник вынес свое заключение на основании документов Комиссии;

во-вторых, эти документы должны были храниться в архивах Комиссии в соответствии с Руководством по процедурам медицинской службы не более шести месяцев и более того, поскольку заявительница не заняла должность в Комиссии, медицинские данные, полученные в ходе осмотра, не должны были быть внесены в медицинскую карту;

в-третьих, ст. 6, 7 Регламента № 45/2001 запрещают передачу медицинских данных из Комиссии в парламент. Медицинские данные, хранящиеся в архивах Комиссии, были собраны исключительно с целью принятия заявительницы на работу в Комиссию, а значит, они не могут быть использованы в других целях и обработаны другой организацией;

в-четвертых, задача медицинского работника парламента состоит в том, чтобы провести независимое медицинское обследование перед приемом на работу, а не расследовать историю болезни заявителя.

По мнению парламента, данное решение не нарушает правила о защите персональных данных, так как ст. 7 Регламента № 45/2001 предусматривает, что передача личных данных между учреждениями возможна, если они необходимы для законного выполнения задач, которые входят в компетенцию получателя. Рассматриваемый перевод был сделан для того, чтобы дать возможность парламенту выполнить одну из своих задач — проверку физической подготовленности кандидата перед устройством на работу. Кроме того, такая передача данных была оправдана заботой о том, чтобы избежать ненужных медицинских осмотров и дать администрации возможность получить полную информацию.

Рассмотрев доводы двух сторон, Суд постановил, что право на уважение частной жизни, закрепленное в ст. 8 ЕКПЧ и вытекающее из общих конституционных традиций государств-членов, является одним из основных прав, охраняемых правопорядком ЕС. В частности, оно включает в себя право человека хранить в тайне состояние своего здоровья. Передача третьему лицу, в том числе другому учреждению, персональных данных, относящихся к состоянию здоровья человека, собранных учреждением, представляет собой вмешательство в частную жизнь соответствующего лица независимо от того, каким образом получена информация. Регламент № 45/2001 действительно предусматривает осуществление межведомственных трансфертов, однако ст. 7 носит весьма общий характер. Кроме того, в ст. 6 говорится, что персональные данные обрабатываются только для целей, для которых они были собраны. Цель сбора Комиссией данных заключалась в определении пригодности заявителя для выполнения обязанностей на посту Комиссии. Использование их для определения ее пригодности к должности в парламенте означало бы изменение цели. Каждое учреждение является независимым работодателем и автономно в управлении своим персоналом. Изменение цели не предусмотрено ни в одном правовом тексте.

Суд отметил, что право на конфиденциальность медицинских данных охраняется законодательством ЕС не только для защиты частной жизни больных, но и для сохранения их доверия к медицинскому органу и медицинским услугам в целом. Ввиду чрезвычайно интимного и чувствительного характера медицинских данных возможность передачи или передача такой информации третьей стороне, даже если эта сторона является другим учреждением или органом

ЕС, без согласия соответствующего лица запрещены. Регламент № 45/2001 предусматривает в связи с этим в ст. 10 (1), что обработка медицинских данных, в принципе, запрещена с учетом ограничений согласно ст. 10 (2).

Кроме того, парламент ни в коем случае не мог утверждать, что заявительница намеренно отказалась сообщить ему, что она работала в Комиссии или что она уже прошла медицинское обследование в другом учреждении. Из пунктов 29, 31 решения о непригодности очевидно, что администрация и заявительница договорились о том, что последняя должна направить в парламент в январе 2009 г. требуемый пакет документов. Таким образом, заявительница могла предоставить парламенту эту информацию до того, как она приступила к исполнению своих обязанностей, или по случаю медицинского осмотра, на который она была приглашена и который должен был состояться 7 января 2009 г.

Таким образом, Суд пришел к выводу, что, во-первых, заявительница не дала согласия на передачу своих данных. Во-вторых, перевод не был «необходим для целей соблюдения конкретных прав и обязанностей нанимателя в области трудового права» в соответствии со ст. 10 (2) (b). Обязанность парламента контролировать пригодность к службе могла бы быть достигнута менее интрузивными средствами. Суд ЕС присудил аннулировать решение парламента и выплатить заявительнице компенсацию в размере 5 тыс. евро материальный ущерб 20 тыс. — за моральный ущерб.

Дело T-343/13 — CN v Parliament от 3 декабря 2015 г.[1] также связано с неправомерным распространением медицинских сведений. CN, бывший сотрудник Совета, находящийся на пенсии, требовал компенсации за материальный и нематериальный ущерб, понесенный в результате публикации отрывка из петиции, поданной заявителем, на официальном сайте Европейского парламента, доступ к которому также могут получить пользователи, находящиеся за пределами этого учреждения.

Этот отрывок содержал элементы персональных данных, включая информацию относительно состояния здоровья заявителя и того факта, что в его семье есть инвалид. В частности, публикация содержала имя заявителя и указание на то, что он страдал от опасного для жизни заболевания и что его сын имел тяжелую форму умственной и физической инвалидности.

---

[1] Arrêt du Tribunal de la Fonction Publique de L'union Européenne (première chambre). URL: https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:62014FJ0026&from=EN

Эта информация стала широкодоступной, поскольку доступ к отрывку из петиции, опубликованной парламентом, можно было получить введя имя заявителя в поисковой системе Google. Несмотря на запросы CN парламент удалил публикацию указанных медицинских данных только после того, как заявитель обратился за помощью к адвокату.

В качестве аргументов о том, что Европейский парламент действовал незаконно, заявитель утверждал, что были нарушены:

– ст. 8 (право на уважением частной и семейной жизни) Европейской конвенции о защите прав человека и основных свобод 1950 г.;

– ст. 8 (защита данных личного характера) Хартии Европейского союза об основных правах 2000 г.;

– ст. 22 (неприкосновенность частной жизни) Конвенции о правах инвалидов, принятой 13 декабря 2006 г. и ратифицированной ЕС 23 декабря 2010 г.;

– Регламент № 45/2001 Европейского парламента и Совета ЕС от 18 декабря 2000 г. о защите отдельных лиц в отношении обработки персональных данных учреждениями и институтами Сообщества и о свободном перемещении таких данных.

По утверждению Европейского парламента, публикация данных была законна, поскольку ранее заявитель высказывал свое согласие на обработку персональных данных, а по смыслу положений Регламента № 45/2001 возможность отзыва согласия не предусматривается. Он был должным образом проинформирован и не воспользовался имеющимся у него вариантом для запроса анонимной или конфиденциальной обработки его петиции. Несмотря на это парламент все же удалил информацию по просьбе CN, что представляло собой, с точки зрения Европейского парламента, некий «акт любезности».

В отношении вопроса защиты персональных данных Суд ЕС отметил, что положения ст. 8 Хартии ЕС об основных правах развиваются в Регламенте № 45/2001. Было также указано, что выражение «данные, касающиеся здоровья» должно иметь широкое толкование, с тем чтобы включать информацию, касающуюся всех аспектов как физического, так и психического здоровья человека. Однако это понятие не может быть расширено до такой степени, чтобы включать положения, которые не приводят к раскрытию каких-либо данных, касающихся здоровья или медицинских показаний человека.

Суд ЕС подробно в своем постановлении коснулся и вопроса распространения данных в Интернете, подчеркнув, что парламент провел серию операций по обработке персональных данных и что распространение таких данных, в том числе в Интернете, подпадает

под это понятие. Суд ЕС провел разграничение между обработанными Европейским парламентом данными, рассмотрев отдельно аспекты, связанные с персональными данными заявителя (включая информацию о его карьере) и с чувствительными личными данными и касающиеся здоровья заявителя и его сына.

В том, что касается персональных данных, Суд ЕС обозначил, что согласно ст. 10 Регламента № 45/2001 обработка персональных данных, раскрывающих сведения о здоровье, запрещена, но не тогда, когда было получено прямое согласие субъекта таких данных. Согласие при этом понимается как «любое свободно представленное конкретное и информированное указание на его или ее пожелания, с помощью которого субъект данных обозначает свое согласие на обработку касающихся его или ее данных». Таким образом, главные признаки, которые должны быть присущи подобному согласию, это конкретность, информированность (необходима достаточность сведений), прямовыраженность.

Заявитель такое согласие выразил, и его нельзя было отозвать согласно Регламенту № 45/2001, что было подтверждено Судом ЕС. Было также установлено, что парламент не совершил достаточно серьезного нарушения правового регулирования, распространяя персональные данные в Интернете.

Касательно личных медицинских данных Суд ЕС отметил, что, несмотря на то, что не приводилось каких-либо доказательств, подтверждающих возможность заявителя выступать в качестве законного представителя своего сына, и что данное CN явное согласие не может оправдать обработку этих данных парламентом, заявитель не может ссылаться на противоправность в результате предполагаемого нарушения прав третьей стороны, а именно его сына.

Суд ЕС посчитал, что заявитель не мог ссылаться на право на удаление данных, о которых идет речь, на основании Регламента № 45/2001, поскольку указанный акт не предполагает этого в случае наличия согласия субъекта медицинских данных, а в рассматриваемой ситуации оно явно присутствовало, как и было упомянуто ранее.

Парламент не обязан был удалять данные незамедлительно, поскольку их публикация была законна, и то, что, по словам заявителя, это заняло у Европейского парламента больше времени, чем предусмотрено Регламентом № 45/2001 в случае нарушения правовых положений, содержащихся в нем, не является основанием для признания парламента виновным.

Последним, что подчеркнул Суд ЕС перед объявлением об отклонении иска заявителя, являлась отсылка к основополагающим пра-

вам, гарантированным ЕКПЧ и составляющим общие принципы права ЕС, несмотря на то, что он не является участником этой Конвенции (ст. 6 Договора о ЕС). В отношении попытки заявителя апеллировать к нарушению ст. 8 ЕКПЧ Суд ЕС обозначил, что CN лишь ссылался на три решения ЕСПЧ, которые, по его мнению, показывают, что право на уважение частной жизни включает в себя его право хранить в тайне состояние своего здоровья. Соответственно, на решение по делу это существенно не повлияло.

В решении по данному делу сомнения вызывает апеллирование Суда к запрету на отзыв согласия, особенно учитывая тот факт, что Суд посчитал нужным сослаться на стандарты ЕКПЧ. В статье 5 Конвенции Овьедо СЕ[1], напрямую связанной с ЕКПЧ, сказано, что «лицо в любой момент может беспрепятственно отозвать свое согласие». Более того, в ст. 8 («Защита данных личного характера») Хартии ЕС об основных правах указывается, что лица имеют право на устранение ошибок в собранных в отношении них данных. Отметим, что заявитель был лишен такой возможности, так как у него отсутствовало разрешение на предварительное ознакомление с данными.

Таким образом, по нашему мнению, Суд принял позицию, согласно которой субъект данных несет повышенную личную ответственность за сохранность личной медицинской информации, если речь идет о его участи в публичных прошениях или петициях. Это достаточно интересный аспект, так как в большинстве случаев при разглашении медицинских данных с учетом их особой важности Суд принимает сторону заявителя, стараясь максимально обезопасить положение ущемленного лица.

Дело Суда ЕС F-84/12 — CN v Council of the European Union[2] от 16 сентября 2013 г. касалось заявления об отмене решения об отказе заявителю, бывшему служащему ЕС, в прямом доступе к окончательному отчету о выводах Комитета по инвалидности в отношении него и в доступе к диагнозу третьего врача этого Комитета. Следует отметить, что решение по данному делу было вынесено Трибуналом по делам гражданской службы, который был упразднен в 2016 г.

---

1 Конвенция о защите прав человека и человеческого достоинства в связи с применением достижений биологии и медицины: Конвенция о правах человека и биомедицине (ETS № 164) (заключена в г. Овьедо 4 апреля 1997 г.) // СПС «КонсультантПлюс».

2 Arrêt du Tribunal de la Fonction Publique de L'union Européenne (deuxième chambre). URL: http://curia.europa.eu/juris/document/document.jsf?text=&docid=141523&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=2271429

Трибунал отклонил жалобу, пояснив, что Регламент № 45/2001 о защите отдельных лиц в отношении обработки персональных данных учреждениями и институтами Сообщества и о свободном перемещении таких данных должен толковаться в соответствии со ст. 41 Хартии ЕС об основных правах, которая признает право каждого лица иметь доступ к своим данным. Хотя Регламент № 45/2001 не содержит положения, разрешающего институту отказывать заинтересованному лицу в доступе к его медицинским данным, он устанавливает средства доступа к персональным данным, включая медицинские, а также обязательства институтов ЕС по защите физических лиц. Суд приходит к выводу, что на основании ст. 20 (1) Регламента № 45/2001 институт ЕС вправе отказать лицу в прямом доступе к окончательному отчету Комитета по инвалидности: институт может счесть необходимым защитить заинтересованное должностное лицо и согласовать такую защиту с требованиями медицинской конфиденциальности. Таким образом, институт может принять решение, в соответствии с которым заинтересованному должностному лицу будет предоставлен доступ к данным отчета через медицинского эксперта, который предоставит объяснения, необходимые для понимания медицинского заключения, послужившего основаниям для решения, объявившего его инвалидом.

В статье 41 (2) (b) Хартии ЕС об основных правах признается право каждого лица на доступ к своим файлам, но при этом предусматривается, что такой доступ должен предоставляться при соблюдении среди прочего и законных интересов конфиденциальности и профессиональной тайны. Таким образом, это положение не требует предоставления должностным лицам прямого доступа к своим медицинским файлам при любых обстоятельствах, а, напротив, разрешает косвенный доступ, если это оправданно законными интересами конфиденциальности и профессиональной тайны.

Соответственно ст. 26a Положений о персонале, поскольку она признает, что должностные лица имеют право ознакомиться со своими медицинскими документами, и указывает, что такой доступ должен осуществляться в соответствии с договоренностями, установленными институтами, по мнению Суда ЕС, не может рассматриваться как противоречащая ст. 41 (2) (b) Хартии.

То же самое относится и к внутренней Директиве Совета № 2/2004, касающейся доступа должностных лиц и других сотрудников к их медицинской карте. В ней после упоминания того, что должностные лица имеют самые самое широкое право на доступ к своим медицинским картам, определяются условия и практические меры для такого доступа. Также в данном документе предусматрива-

ется, что с медицинской картой необходимо ознакомиться в помещении медицинского отдела Совета в присутствии лица, назначенного этим отделом.

Тем не менее, когда должностное лицо запрашивает доступ к медицинскому заключению, которое содержит данные психологического или психиатрического характера, оно может получить такой доступ только через назначенного им врача. Непрямой доступ такого рода через назначенного должностным лицом медицинского эксперта является средством согласования, как того требует ст. 41 (2) (b) Хартии, права должностного лица на доступ к имеющимся у него медицинским документам с требованиям конфиденциальности медицинской информации, которая предоставляет возможность каждому врачу самостоятельно решать, необходимо ли ему сообщать лицу, которого он лечит или обследует, о природе болезней, от которых лицо может страдать, или же нет.

Нормы Положений о персонале, касающиеся жалоб, позволяют должностным лицам оспаривать законность решения, принятого по завершении процедуры по установлению инвалидности, и в ходе такого оспаривания ссылаться на любое нарушение в предыдущих документах, тесно связанных с этим решением, например на окончательный отчет Комитета по инвалидности, причем даже не зная содержания решения.

Тем не менее, на наш взгляд, прямой доступ к медицинским персональным данным является основополагающим правом, а заявитель в данном деле был его лишен. Это является нарушением ст. 8 Хартии, которая так же применима к заявителю, поскольку он являлся не только должностным лицом, но и субъектом защиты прав, установленных Хартией для всех лиц независимо от рода их деятельности. Более того, к данной ситуации также применима ч. 2 ст. 10 Конвенции Овьедо: «Каждый человек имеет право ознакомиться с любой собранной информацией о своем здоровье». Часть 3 ст. 10 в то же время накладывает определенные ограничения: «В исключительных случаях — только по закону и только в интересах пациента — осуществление прав, изложенных в параграфе 2, может быть ограничено». На наш взгляд, в данном деле не было основания для таких ограничений.

Таким образом, решения Суда ЕС выявили проблемные места правового регулирования защиты персональных данных. В связи с этим в мае 2016 г. был принят новый Регламент (ЕС) 2016/679 Европейского парламента и Совета ЕС о защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных, а также об отмене Директивы 95/46/ЕС. Регламент

предоставляет гражданам больше прав, касающихся информированности об использовании их персональных данных, и устанавливает более четкие обязанности в отношении лиц и организаций, использующих персональные данные. Новшеством регламента является дифференцированный подход к определению медицинских, генетических и биометрических данных пациентов, которые рассматриваются теперь как особая категория «конфиденциальных данных». Они включают в себя все персональные данные, которые по своей природе особенно чувствительны в отношении основных прав и свобод и заслуживают особой защиты, поскольку контекст их обработки может создавать значительные риски.

Директива вступила в силу год назад, и до настоящего времени ЕС не вынес ни одного решения на ее основании. Однако можно утверждать, что такой основательный подход к разграничению категорий персональных медицинских данных станет еще одним шагом на пути их эффективной защиты, что может служить образцом для реформы законодательства Российской Федерации.

Глава 10
ЕВРОПЕЙСКИЕ СТАНДАРТЫ ЗАЩИТЫ ДАННЫХ. СРАВНИТЕЛЬНОЕ ИССЛЕДОВАНИЕ СУДЕБНОЙ ПРАКТИКИ

В 2019 году человечество отмечает 30-летие Интернета, в связи с чем уместно упомянуть о беспокойстве Тимоти Джона Бернерс-Ли — одного из разработчиков технологий Всемирной паутины, которое он выразил по поводу концентрации власти на нескольких доминирующих платформах. Ранее он назвал потерю контроля над личными данными главной угрозой современному Интернету[1]. Эти предупреждения в настоящее время особенно актуальны, несмотря на совершенствование законодательства и судебной практики (на международном и национальном уровнях), особенно в последнее время.

В области защиты данных в 2006 г. приняты Федеральный закон «Об информации, информационных технологиях и о защите информации» и ряд других законодательных актов: «О персональных данных», «Об обеспечении доступа к информации о деятельности судов Российской Федерации», «О защите детей от информации, причиняющей вред их здоровью и развитию». Эволюции изучения цифровизации права и усилению требований в области защиты данных посвящен ряд постановлений Правительства РФ.

Следует подчеркнуть, что на эффективность персонального правового регулирования и судебную практику повлияли и продолжают оказывать прогрессивное воздействие соответствующие директивы ЕС, Конвенции Совета Европы, а также практика Суда справедливости Европейского Союза (далее — Суд ЕС) и Европейского Суда по правам человека (далее — Суд). Это объяснимо, если задаться вопросом, кто более ответственен за защиту частной жизни — законодатель или суды. Следует отметить, что защита данных непосредственно связана с разумными ожиданиями как личности, так и общества относительно надежной защиты личной жизни. Соответствующие компании регулярно сталкиваются со сложными проблемами, среди которых наиболее острая: что образует частную информацию и в какой мере закон защищает ее.

---

[1] См.: Tim Berners-Lee, The Web Can Be Weaponised — and We Can`t Count on Big Tech to stop it. Gardian (March 12, 2018).

Вместе с тем общепризнано значение защиты общества от терроризма, что непосредственно часто связано с доступом правоохранительных органов и различных служб к большому объему информации персонального характера. Законодателю непросто успевать за технологическими изменениями. Необходимо постоянно анализировать инновации, их влияние на защиту данных. Принятые законы могут не отвечать новому состоянию информационной технологии, судьи в повседневной работе часто встречаются с вызовами цифровой эпохи, им регулярно приходится находить решения для достижения баланса между защитой частной жизни и общественной безопасностью, используя знания не только в области права. Это требует знания обширной практики двух европейских судов, которые вот уже на протяжении нескольких десятилетий формулируют позиции по сложным вопросам.

Так, Совет Европы, принявший 17–18 мая 2018 г. Модернизированную конвенцию о защите лиц в отношении обработки личных данных (Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data), дал определение понятию «личные данные» — это любая информация, касающаяся идентифицированного или идентифицируемой личности (предмет данных). В конвенции дано также определение понятия «обработка данных» — любая операция или комплекс работ, выполненных с использованием личных данных, таких как сбор, хранение, сохранение, изменение, раскрытие информации, принятие мер по обеспечению ее доступности, удаление или уничтожение, выполнение логических или арифметических операций на таких данных. Конвенция определила также другие важные понятия, одновременно провозгласив создание Комитета Конвенции. ЕС принял Общий регламент по защите данных (The European Union`s General Data Protection Regulation (GDPR) от 25 мая 2018 г.), который требует от всех контролеров данных и процессов, обрабатывающих личную информацию резидентов ЕС, «осуществления соответствующих технических и организационных мер... для обеспечения постоянной конфиденциальности, целостности, доступности и отказоустойчивости систем и служб обработки или штрафов до 20 млн евро или 4% годового общего оборота (самый допустимый)». В статье 8 Хартии ЕС об основных правах (от 7 декабря 2000 г.) предусмотрена защита данных личного характера. В частности, указывается, что каждый человек имеет право на защиту относящихся к нему данных личного характера; обработка данных должна производится без манипуляций, в четко определенных целях, с согласия заинтересованного лица либо при наличии других правомерных оснований, предусмотренных законом.

Каждый человек имеет право на получение доступа к собранным в отношении него данным и право на устранение в них ошибок. Соблюдение этих правил подлежит контролю со стороны независимого органа. Хартия закрепила важные права и требования, приняв во внимание практику Суда ЕС и ЕСПЧ.

Европейская конвенция о защите прав человека и основных свобод (далее — Конвенция) принималась в послевоенные годы, когда еще не было права на защиту данных. Однако с течением времени Суд, следуя доктрине «живого организма» (living instrument), обязан был путем интерпретации норм Конвенции ответить на вызовы времени. Статья 8 о праве на уважение частной и семейной жизни служит основной нормой, которая применяется в делах, связанных с вопросами защиты данных. Возможно применение и ст. 13, так как она обеспечивает право каждого на эффективное средство правовой защиты в случае предполагаемого нарушения Конвенции: каждый, кто считает, что нарушено его право на защиту персональных данных, имеет право на средство правовой защиты в национальной правовой системе. Суд в постановлении P.G. and J.H. v. the United Kingdom от 25 января 2001 г. (§ 56–59) подчеркнул, что личная жизнь является широким термином, не поддающимся исчерпывающему определению. Так, возможно наличие элементов, касающихся личной жизни человека и отражающих процессы вне его жилища или частных помещений. Люди иногда сознательно или преднамеренно вовлекаются в деятельность, которая регистрируется или может быть опубликована либо представлена в публичной форме. Разумные ожидания человека в отношении конфиденциальности могут быть существенным, хотя и не обязательно убедительным фактором. Суд признает принципы, лежащие в основе защиты данных в соответствии с Конвенцией, в частности право на неприкосновенность частной жизни, подчеркивая, что сбор личных данных, таких как стенограмма телефонных переговоров, фотографии, больничные записи и тканевые материалы, также подпадают под действие права на неприкосновенность частной жизни. Суд определил также, что должно быть законное основание для обработки персональных данных, что обработчики должны проявлять осторожность при передаче персональных данных третьим лицам и, где это возможно, персональные данные должны быть удалены, когда они больше не соответствуют цели, для которой были собраны. В деле Köpke v. Germany Суд к названным принципам добавил, что государства — участники Конвенции обязаны установить адекватные правила защиты данных в их национальном законодательстве (5 октября 2010 г., no 420/07).

Для полноты понимания практики Суда следует остановиться на методе, который он часто использует при рассмотрении таких дел. Во-первых, следует определить, имело ли место вмешательство в право, защищаемое п. 1 ст. 8 Конвенции; во-вторых, с учетом требований п. 2 данной статьи установить, было ли вмешательство оправдано обстоятельствами дела. Суд использует обычно три критерия: вмешательство должно быть предусмотрено законом, преследовать предусмотренную Конвенцией цель и быть необходимым в демократическом обществе.

В своей практике Суд исходит из того, что защита персональных данных распространяется на различные формы коммуникации, будь то обычная переписка, телефонные переговоры, переписка по электронной почте, любые сообщения через Интернет, информация, полученная при наблюдении с помощью глобальной системы навигации GPS, электронные письма с рабочего места и информация, полученная при использовании Интернета на рабочем месте, отпечатки пальцев и ДНК, видеозаписи, на которых есть изображения человека. Таким образом, Суд вносит свой вклад в защиту прав человека в цифровую эпоху.

§ 1. Сбор личных данных

В деле Uzun v. Germany заявитель подозревался в причастности к бомбовым атакам со стороны левого экстремистского движения. Он, в частности, жаловался, что осуществляемая слежка посредством GPS и использование полученных данных в ходе уголовного разбирательства против него нарушили его право на уважение частной жизни.

Суд не нашел нарушения ст. 8 Конвенции. Наблюдение при помощи GPS, обработка и использование полученных таким образом данных нарушают право заявителя на защиту личной жизни. Однако, по мнению Суда, все это преследовало законные цели защиты национальной безопасности, общественного порядка и прав потерпевших, предупреждения преступления и было пропорционально: GPS-наблюдение было назначено только после того, как менее строгие методы расследования оказались недостаточными, осуществлялись относительно короткий период (около трех месяцев) и оказали влияние на ход расследования только тогда, когда заявитель ехал в машине своего сообщника. Учитывая, что расследование касалось очень тяжких преступлений, наблюдение за заявителем посредством GPS было признано необходимым в демократическом обществе (постановление от 2 сентября 2010 г.).

Как следует из постановления Суда по делу Ben Faiza v. France относительно мер наблюдения против заявителя в уголовном преследовании о его причастности к преступлениям незаконного оборота наркотиков, в частности из утверждений заявителя, что эти меры (установка устройства геолокации на его транспортном средстве и постановление суда, выданное оператору мобильной связи для получения записи о его входящих и исходящих вызовах, а также для фиксации сотовой вышки с его телефонов, что позволяет впоследствии отслеживать его перемещение) представляют собой вмешательство в право на уважение его частной жизни.

Суд посчитал, что допущено нарушение ст. 8 Конвенции относительно геолокации в реальном времени 3 июня 2010 г., установив, что в указанном отношении французское право (ни статутное право, ни судебная практика) в соответствующее время не предусматривали с достаточной ясностью, в какой степени и каким образом власти имели право использовать свои дискреционные полномочия. Заявитель поэтому не обладал той минимальной защитой, которая соответствовала бы верховенству права в демократическом обществе. По мнению Суда, Франция в последующем законодательно определила правовой механизм использования геолокации, усилив право на уважение частной жизни (Закон от 28 марта 2014 г.). Однако Суд не установил нарушения ст. 8 Конвенции относительно судебного предписания мобильному оператору, поскольку оно было принято в соответствии с законом и направлено на определение истины в контексте уголовного разбирательства о ввозе наркотиков организованной преступной группой, преступном сговоре и отмывании денег, преследуя законные цели предотвращения беспорядков или преступлений и защиты общественного здоровья (постановление от 8 февраля 2018 г.).

В деле L.H. v. Latvia заявитель предполагал, что сбор его личных медицинских данных государственным агентством — Инспекцией контроля качества медицинской помощи и работоспособности — без его согласия нарушило право на уважение частной жизни. В этом постановлении Суд напомнил о важности защиты медицинских данных и, установив нарушение ст. 8 Конвенции, обратил внимание на то, что примененное право не предусматривало с достаточной ясностью объем усмотрения, предоставленного компетентным органам, а также способ его осуществления. Суд отметил, что право Латвии не ограничивает сферу личных данных, которые могли бы быть собраны указанным агентством. Были собраны медицинские данные о заявителе, относящиеся к семилетнему периоду, причем без разбора и предварительной оценки того, могут ли они иметь потенциально решающее значение и важность для достижения какой-либо цели,

которая могла быть достигнута в результате данного расследования (постановление от 29 апреля 2014 г.).

§ 2. Перехват сообщений, прослушивание телефонных разговоров и тайное наблюдение

Наиболее часто цитируемым и одним из ранее рассмотренных дел соответствующей тематики является Klass and Others v. Germany. Пятеро юристов обжаловали законодательство Германии, позволяющее властям контролировать их переписку и телефонную связь, не обязывая впоследствии информировать их о принимаемых против них мерах. Суд не обнаружил нарушения ст. 8 Конвенции, посчитав, что законодатель оправданно рассматривает вмешательство в осуществление права, гарантированного п. 1 ст. 8 Конвенции, необходимым в демократическом обществе в интересах национальной безопасности и предотвращения беспорядков или преступлений (п. 2 ст. 8 Конвенции). Суд подчеркнул, что полномочия тайного наблюдения за гражданами, характерного для полицейского государства, допускаются в соответствии с Конвенцией только при крайней необходимости для защиты демократических институтов, отметив, что демократическим обществам в настоящее время угрожают изощренные формы шпионажа и терроризма, в результате чего государство должно быть способным эффективно противостоять таким угрозам, осуществлять тайное наблюдение за подрывными элементами, действующими в пределах его юрисдикции. Суд посчитал, что существование соответствующего законодательства с предоставлением полномочий секретного наблюдения за почтой, сообщениями и телекоммуникациями в исключительных условиях было необходимо в интересах национальной безопасности и для предотвращения беспорядков или преступлений (постановление от 6 сентября 1978 г.).

Ключевой концепцией в наблюдении за коммуникацией является различие между содержанием сообщения, с одной стороны, и данными, относящимися к этому сообщению, — с другой (данные связи, или метаданные). Самый простой пример — письмо, отправленное по почте. Само письмо — это содержание, тогда как данные связи — это буквально информация, которая содержится на конверте, то есть адрес, на который оно было отправлено, почтовый штемпель с указанием времени и даты, когда оно было доставлено в службу почтовой связи, и, если он был указан, адрес отправителя[1].

---

1 Eric Metcalfe. Communications surveillance in a digital age. Melanges En L`Honneur / De Essays in honour of Dean Spielmann 2015. The Netherlands. P. 390.

В деле Malone v. the United Kingdom заявитель жаловался не только на то, что полиция прослушивала его телефонные разговоры, но и на то, что почтамт тайно соединил его телефон с устройством, которое автоматически регистрировало все номера, которые он набирал на своем телефоне, время набора и длительность звонка. Данная информация передавалась полиции. Суд отметил, что использование почтамтом названного устройства в целом было законным для целей предоставления телекоммуникационных услуг и отличается от скрытого перехвата полицией телефонных звонков. Однако Суд одновременно подчеркнул, что наличие права у почтового отделения записывать информацию об использовании заявителем телефона в своих целях не означает, что самой информации не должна быть обеспечена защита по ст. 8 Конвенции (постановление от 2 августа 1984 г., § 84).

Решение Суда по делу Malone означало переход прецедентного права о наблюдении за коммуникациями на новую ступень развития, указав на необходимость защиты конфиденциальности информации относительно общения лица как неотъемлемого элемента самого сообщения. Такая позиция Суда выгодно отличалась от узкого подхода, принятого за пять лет до него Верховным Судом США в деле Smith v. Maryland (442 US 735 (1979). В то же время Суд установил, что коммуникационным данным требуется меньшая защита, чем содержанию сообщений, на том основании, что информация о сообщении лица не так чувствительна, как то, что лицо на самом деле говорит и пишет.

В деле Wisse v. France (постановление от 22 декабря 2005 г.) оба заявителя были арестованы по подозрению в совершении вооруженного грабежа и помещены в места досудебного задержания. По ордеру, выданному следственным судьей, записывались телефонные разговоры между ними и их родственниками в комнате посещения тюрьмы. Заявителями были предприняты безуспешные попытки признания не имеющими законной силы записей бесед, при этом они ссылались на нарушение их права на личную и семейную жизнь. Суд установил нарушение ст. 8 Конвенции, указав, что закон не определяет с достаточной ясностью, как и в какой степени власти могут вмешиваться в частную жизнь задержанных, а также объем и способ осуществления своих полномочий в данной сфере. Следовательно, заявители не пользовались тем минимальным объемом защиты, который соответствует принципу верховенства права в демократическом обществе.

Согласно R.E. v. the United Kingdom (постановление от 27 октября 2015 г.) заявитель был арестован и задержан в Северной Ирландии в

трех случаях в связи с убийством офицера полиции. Он обжаловал режим скрытого наблюдения во время консультаций между задержанными и их адвокатами, а также между уязвимыми задержанными и «соответствующими взрослыми». Дело было рассмотрено с точки зрения принципов, развитых Судом в области перехвата телефонных разговоров адвоката и клиента, требующих строгих гарантий. Суд определил, что эти принципы следует применять к случаям скрытого наблюдения за консультациями юриста и клиента в полицейском участке. Установив нарушение ст. 8 Конвенции относительно упомянутого наблюдения, Суд отметил, что руководящие принципы по организации безопасной обработки, хранения и уничтожения материалов, полученных в результате такого скрытого наблюдения, были введены с 22 июня 2010 г. Однако на момент содержания заявителя под стражей эти принципы еще не вступили в силу и действующее национальное право не предоставляло достаточных гарантий защиты описанных консультацией заявителя и адвоката, полученных путем скрытого наблюдения. В то же время Суд не обнаружил нарушения по такому же наблюдению за консультациями задержанных и «соответствующих взрослых», поскольку на них не распространялись правовые привилегии, и поэтому задержанный не может рассчитывать на конфиденциальность как при юридических консультациях.

Постановление по делу Roman Zakharov v. Russia от 4 декабря 2015 г. касалось системы секретного перехвата сообщений сотовой телефонной связи. Заявитель предполагал, что российские операторы мобильной связи на основании действующих норм могли установить оборудование, позволяющее правоохранительным органам проводить оперативно-разыскные мероприятия в отсутствии достаточных гарантий, разрешающих осуществлять общий перехват сообщений.

Суд пришел к выводу о нарушении ст. 8 Конвенции, поскольку правовые нормы, регулирующие перехват сообщений, не предусматривали адекватных и эффективных гарантий против произвола и риска злоупотреблений, которые были присущи системе тайного наблюдения, предоставляя, в частности, возможности спецслужбам и полиции иметь прямой доступ с использованием технических средств к мобильной телефонной связи. Были отмечены следующие недостатки в правовом отношении: обстоятельства, при которых органы власти имели право прибегнуть к секретным мерам наблюдения; определение длительности таких мер, оснований, при которых они подлежали прекращению; установление процедуры для разрешения проведения перехвата, а также хранения и уничтожения по-

лученных таким образом данных, надзора за выполнением тайного наблюдения. Эффективность средств правовой защиты, доступных для оспаривания перехвата сообщений, была снижена тем, что они были доступны только лицам, которые могли представить доказательства, получение которых было невозможно при отсутствии какой-либо системы уведомлений или доступа к информации о перехвате. Таким образом, Суд особое внимание для формирования прецедента уделил хорошо разработанному им критерию «качество закона».

В деле Benedict v. Slovenia (постановление от 24 апреля 2018 г.) речь идет о неспособности полиции Словении получить судебное распоряжение о доступе к информации о подписчике, связанной с динамичным IP-адресом, зарегистрированным швейцарскими правоохранительными органами во время мониторинга пользователей определенной сети обмена файлами. Это привело к тому, что заявитель был идентифицирован после того, как он распространял файлы по сети, в том числе детскую порнографию.

Установив нарушение ст. 8 Конвенции (право на уважение частной жизни), Суд подчеркнул, что правовое положение, используемое полицией для получения информации о подписчике, связанной с динамичным IP-адресом, не соответствовало общепринятому стандарту «в соответствии с законом». Положение было недостаточно ясным, практически не обеспечивало защиту от произвольного вмешательства, не было гарантий против злоупотребления и независимого надзора за задействованными полицейскими силами.

§ 3. Мониторинг использования компьютера работниками

Дело Barbulescu v. Romania (постановление от 5 сентября 2017 г.) касается решения частной компании уволить работника после проверки его электронных сообщений, к содержанию которых она получила доступ. Заявитель указывал в жалобе, что решение работодателя было основано на нарушении его частной жизни и что национальные суды не защитили его право на уважение его личной жизни и корреспонденции.

Суд пришел к выводу о нарушении ст. 8 Конвенции, посчитав, что власти не защитили должным образом права заявителя по этой статье. Они 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 сте-

пени вторжения в его личную жизнь и корреспонденцию. По мнению Суда, национальные суды не обратили внимания, во-первых, на конкретные причины, оправдывающие осуществление мониторинга; во-вторых, на то, мог ли работодатель использовать меру, повлекшую за собой меньшее по характеру вмешательство; в-третьих, на наличие возможности получить доступ к сообщениям без ведома заявителя.

Постановление Libert v. France от 22 февраля 2018 г. касается увольнения работника французской национальной железнодорожной компании (SNCF) после изъятия его рабочего компьютера, в котором были обнаружены порнографические файлы и поддельные сертификаты, составленные для третьих лиц. Заявитель утверждал, что работодатель открыл его личные файлы, хранящиеся на жестком диске его рабочего компьютера. Суд не нашел нарушения ст. 8 Конвенции, подчеркнув, что в данном деле французские власти действовали в рамках закона (margin of appreciation). Он отметил, что файлы просматривались работодателем с законной целью защиты прав работодателей, которые вправе требовать, чтобы их сотрудники использовали компьютеры, предоставленные в их распоряжение, в соответствии с их договорными обязательствами и применяемыми правилами.

По мнению Суда, французское право содержит механизм защиты конфиденциальности, который, хотя и позволяет открывать профессиональные файлы, однако предусматривает ограничения, касающиеся файлов, идентифицированных как личные. Такие файлы возможно открыть в присутствии работника. Национальные суды решили, что указанный механизм не помешал бы работодателю открыть и эти файлы, поскольку они были должным образом определены как частные. Наконец, Суд посчитал, что местные суды должным образом оценили предположение заявителя о нарушении его прав и в их решениях достаточно оснований.

§ 4. Образцы голоса

Дело P.G. and J.H. v. the United Kingdom (постановление от 25 сентября 2001 г.) касается скрытых подслушивающих устройств в резиденции В. и использования этих устройств в полицейском участке. Так, голоса заявителей в участке полиции записывались после их ареста по подозрению в совершении грабежа. Суд посчитал, что осуществленное названными действиями вмешательство не было предусмотрено законом и нарушило ст. 8 Конвенции. Он подчеркнул, в частности, что в соответствующее время не существовало правовых норм, регулирующих использование тайных прослушивающих устройств полицией в ее же помещениях. Нарушение было

установлено в том числе по факту применения подслушивающего оборудования в квартире, но не в отношении полученной информации в результате использовании телефона.

§ 5. Видеонаблюдение

В деле Antovic and Mirkovic v. Montenegro (постановление от 28 ноября 2017 г.) Суд рассматривал жалобу двух профессоров университета на вмешательство в их частную жизнь путем установления видеонаблюдения в местах их преподавания. Они утверждали, что не осуществлялся эффективный контроль над собранной информацией и само наблюдение велось незаконно. Национальные суды отказали в иске о компенсации на том основании, что вторжение в личную жизнь не установлено, а видеонаблюдение велось только в аудиториях, которые являются публичным пространством. Суд признал, что видеонаблюдение осуществлялось незаконно и нарушило право на частую жизнь. Во-первых, было отвергнуто утверждение правительства о неприемлемости, повторившее по существу позицию национальных судов о публичном пространстве. Как отметил Суд, частная жизнь может включать также профессиональную деятельность, что соответствует требованиям ст. 8 Конвенции. Во-вторых, по мнению Суда, использование камеры наблюдения образует вмешательство в право на неприкосновенность частной жизни и названные действия властей нарушили положения национального права. Последнее никогда не было предметом рассмотрения местных судов, отвергающих саму идею вмешательства в частную жизнь.

§ 6. Хранение и использование личных данных

Как следует из постановления S. and Marper v. the United Kingdom от 4 декабря 2008 г. (§ 103), защита личных данных — фундаментально важный вопрос об уважении права человека на частную и семейную жизнь по ст. 8 Конвенции. Национальное право должно гарантировать предотвращение любой возможности использования личных данных, если это противоречит требованиям Конвенции. Потребность в таких гарантиях возрастает, когда речь идет о защите личных данных, подвергающихся автоматической обработке, особенно когда они используются в полицейских целях. Национальное законодательство должно, в частности, обеспечивать, чтобы такие данные были релевантными и нечрезмерными по отношению к целям, для которых они хранятся. Оно должно также гарантировать, что эти данные хранятся в том виде, который позволит идентифицировать субъектов

данных, причем исключительно для целей их хранения. Необходимо также обеспечить хранящимся личным данным эффективную защиту от злоупотребления и неправильного обращения.

§ 7. В контексте уголовной юстиции

В деле Perry v. the United Kingdom (постановление от 17 июля 2003 г.) заявитель был арестован в связи с серией вооруженных ограблений водителей мини-такси и освобожден в ожидании опознания. После того как он не смог присутствовать на нескольких процедурах, полиция попросила разрешения на его скрытую видеозапись для целей опознания и использовала ее против него. Суд установил нарушение ст. 8 Конвенции, отметив, что заявитель не знал об использовании снятых кадров в полицейском участке в ходе процедуры опознания, а также в качестве доказательства, наносящего ущерб его защите в ходе судебного разбирательства. Данная мера, предпринятая полицией, вышла за пределы обычного использования такого типа камеры и представляла собой вмешательство в право заявителя на уважение его частной жизни. Рассматриваемое вмешательство не соответствовало закону, поскольку полиция не следовала процедурам, описанным в законе: ими не было получено согласие заявителя или он не был информирован о том, что будет проводиться съемка, ему не были разъяснены его права.

В деле Khelili v. Switzerland (постановление от 18 октября 2011 г.) заявительница жаловалась на то, что с момента обнаружения ее визитных карточек во время полицейской проверки в 1993 г. полиция Женевы установила на этих карточках следующую запись: «Милая симпатичная женщина более тридцати желала бы встретиться с мужчиной, чтобы выпить или время от времени выходить. № тел. ...». Заявительница предполагала, что после этого полиция внесла ее имя в списки проституток, заподозрив в деятельности, которой она не планировала заниматься. Она утверждала, что хранение ложных данных о ее личной жизни нарушило ее право на уважение частной жизни. Суд пришел к выводу о нарушении ст. 8 Конвенции на том основании, что хранение в полиции документов с предположительно ложными данными о частной жизни нарушило ее право и что сохранение слова «проститутка» в течение многих лет не было не только оправданным, но и необходимым в демократическом обществе. Данное слово, как полагает Суд, может нанести ущерб репутации заявительницы и сделать ее повседневную жизнь проблематичной, учитывая, что указанные в списках полиции данные могут быть переданы властям. Изложенное особенно важно в связи с тем, что

персональные данные в настоящее время подлежат автоматической обработке, а это значительно облегчает не только доступ к ним, но и их распространение.

Согласно делу M.K. v. France (постановление от 18 апреля 2013 г.) в 2004—2005 гг. заявитель дважды находился под следствием по обвинению в краже книг. Он был оправдан по первому обвинению, по второму дело было прекращено. В обоих случаях были взяты отпечатки его пальцев и внесены в базу данных. Его просьба была удовлетворена лишь в связи с первым случаем, по второму же отклонена, включая апелляционную жалобу. Заявитель утверждал, что хранение его данных в компьютеризированной базе отпечатков пальцев нарушает его право по ст. 8 Конвенции. Суд посчитал, что его права нарушены, установив при этом: хранение данных представляет собой непропорциональное вмешательство в право заявителя на защиту частной жизни, и в этом нет необходимости в демократическом обществе. По мнению Суда, государство вышло за пределы усмотрения в таком вопросе, как система хранения отпечатков пальцев лиц, подозреваемых в правонарушении, но не осужденных, как это и было в деле заявителя, не установив справедливый баланс между конкурирующими публичными и частными интересами.

В постановлении по делу Brunet v. France от 18 сентября 2014 г. отмечалось, что заявитель в своей жалобе подчеркивал, что вмешательство в частную жизнь стало результатом внесения его имени в полицейскую базу данных (система обработки зарегистрированных правонарушений — STIC), содержащих информацию из отчетов о расследовании с указанием лиц, причастных к делу, потерпевших, и после прекращения уголовного дела против него. Суд посчитал, что государство в нарушение ст. 8 Конвенции вышло за пределы усмотрения: хранение может быть рассмотрено в качестве непропорционального нарушения права заявителя на частную жизнь и не было необходимым в демократическом обществе; заявитель не имел реальной возможности добиться удаления из базы данных информации относительно себя, длительность хранения которой в течение 20 лет может быть воспринята как хранение если не на неопределенный срок, то по крайней мере в качестве нормы.

Дело Aycaquer v. France (постановление от 22 июня 2017 г.) касается нарушения права на уважение частной жизни на основании распоряжения о предоставлении биологического образца для включения в национальную компьютеризированную базу данных ДНК (FNAEG) и того факта, что отказ лица выполнить этот приказ привел к уголовному осуждению. Суд пришел к выводу о нарушении ст. 8 Конвенции, посчитав, что 16 сентября 2010 г. Конституционный Совет вынес решение о соответствии положений FNAEG Конститу-

ции Французской Республики, включая «определение срока хранения таких персональных данных в зависимости от цели хранения файла, характера и серьезности правонарушения, о котором идет речь». Суд отметил, что до настоящего времени не было предпринято никаких надлежащих действий в отношении названной оговорки и что до сих пор нет положений, позволяющих дифференцировать срок хранения в зависимости от характера и тяжести совершенного преступления. Он также указал, что хранение профилей ДНК в общенациональном банке генетических данных не обеспечивает субъектам данных достаточную их защиту с учетом его продолжительности, тем более, что они не могут быть удалены. Именно в связи с этими обстоятельствами указанные правила не способствуют поддержанию баланса между публичными и частными интересами.

§ 8. В контексте информации о состоянии здоровья

В деле Chave née Jullien v. France (решение Европейской Комиссии по правам человека от 9 июля 1991 г.) речь идет о хранении в психиатрической больнице информации о принудительном размещении заявителя, незаконность которого была признана французскими судами. Заявительница рассматривала сохранение записи с информацией о ее содержании в психиатрическом учреждении как вмешательство в ее частную жизнь и требовала удаления этой информации. Комиссия признала жалобу неприемлемой, поскольку наличие указанной записи служит не только законным интересам гарантирования эффективной работы государственной медицинской службы, но и защите прав самих пациентов, особенно при принудительном помещеним в психиатрические учреждения. В данном деле рассматриваемая информация находилась под защитой соответствующих правил конфиденциальности. Эти документы не могут быть приравнены к иным записям, и к ним нет публичного доступа, за исключением исчерпывающего перечня лиц вне института. С учетом изложенного Комиссия признала вмешательство пропорциональным преследуемой законной цели — защите здоровья.

§ 9. В процессах, связанных с социальным страхованием

Согласно постановлению Суда по делу Vukota-Bojic v. Switzerland от 18 октября 2016 г. заявительница была вовлечена в дорожно-транспортное происшествие и впоследствии обратилась за пенсией по инвалидности. После разногласий со своим страховщиком о размере пенсии по инвалидности и судебных рассмотрений страховой агент

потребовал, чтобы она прошла новое медицинское обследование для установления дополнительных доказательств о состоянии ее здоровья. Когда она отказалась, страховщик нанял частных следователей для проведения за ней тайного наблюдения. Ими были получены доказательства, которые были использованы в последующем судебном разбирательстве, завершившемся сокращением размера пособия заявительницы. Она утверждала в жалобе, что наблюдение противоречило праву на уважение частной жизни и не должно было быть принятым в судебном разбирательстве. Суд согласился с позицией заявительницы в том, что действия страховщика влекли за собой ответственность государства в соответствии с Конвенцией, поскольку страховая компания — ответчик — в соответствии с законодательством Швейцарии осуществляет публичную власть. Он также посчитал, что проведение тайного наблюдения является вмешательством в частную жизнь заявителя, если даже оно проводилось в общественных местах, поскольку следователи регулярно собирали и хранили данные и использовали их в конкретных целях. Кроме того, наблюдение не было предусмотрено законом: в положениях швейцарского права не определено четко, когда и как долго наблюдение может проводиться, каким образом следует хранить данные и получать доступ к ним.

§ 10. Хранение в секретных реестрах

Дело Leander v. Sweden (постановление от 23 марта 1987 г.) касалось использования секретного досье полиции при найме заявителя в качестве столяра. Он временно работал в военно-морском музее в г. Карлскроне рядом с запретной зоной и долгое время жаловался на хранение данных, связанных с его профсоюзной деятельностью, что, как он полагал, привело к его отстранению от работы. По мнению заявителя, ничто в личном или политическом отношении не может рассматриваться как дающее основание для его регистрации в отделе безопасности как лица, представляющего «угрозу безопасности».

Суд пришел к выводу о не нарушении требований ст. 8 Конвенции, отметив, в частности, что хранение секретного реестра и выдача информации относительно частной жизни лица подпадает под действие ст. 8 Конвенции. В демократическом обществе, по мнению Суда, существование разведывательных служб и хранение данных может быть законным и преобладать над интересами граждан при условии, что оно преследует законные цели: предупреждение беспорядков или преступлений либо защита национальной безопасности. В данном деле Суд установил, что гарантии, содержащиеся в системе личного контроля в Швеции, соответствуют требованиям ст. 8 Кон-

венции и правительство Швеции имело право руководствоваться принципом преобладания интересов национальной безопасности над личными интересами заявителя.

§ 11. Раскрытие персональных данных

Дело Z. v. Finland (постановление от 25 февраля 1997 г.) касается раскрытия статуса заявительницы как ВИЧ-положительной в уголовном разбирательстве против ее мужа. Суд установил нарушение ст. 8 Конвенции, поскольку раскрытие личности заявительницы и факта заражения ВИЧ в тексте постановления суда апелляционной инстанции, доступного прессе, не было подтверждено какими-либо убедительными причинами и публикация соответствующей информации повлекла за собой нарушение права заявительницы на уважение ее личной и семейной жизни. Суд подчеркнул, в частности, что конфиденциальность данных о здоровье является жизненно важным принципом в правовых системах всех договаривающихся государств и важна не только с точки зрения уважения неприкосновенности частной жизни пациента, но и в части сохранения его (или ее) доверия к представителям медицинской профессии и в целом системе здравоохранения. Национальное право должно предусматривать надлежащие меры предосторожности, чтобы предотвратить любую утечку или разглашение личных данных о здоровье, что может противоречить ст. 8 Конвенции.

Постановление Суда по делу Peck v. the United Kingdom от 28 января 2003 г. имеет отношение к вопросу о раскрытии СМИ видеоматериалов, снятых на улице с помощью камеры видеонаблюдения, установленной местным советом, показывающей, как заявитель перерезал себе вены на запястьях. Суд определил, что опубликование отснятого муниципальным советом материала не сопровождалось наличием достаточных гарантий и представляло собой непропорциональное и неоправданное вмешательство в личную жизнь заявителя в нарушение ст. 8 Конвенции. Не было никаких оснований, оправдывающих опубликование местным советом кадров из видеоматериала без согласия заявителя или маскировки его личности либо без уверенности в том, что при передаче СМИ они сделают это. Цель предупреждения преступности и контекст раскрытия информации требовали особого внимания и осторожности в этом деле. В то же время Суд пришел к выводу о нарушении ст. 13 Конвенции в сочетании со ст. 8, так как заявитель по существу не имел эффективных средств правовой защиты в связи с нарушением права на частную жизнь.

Рассмотренное Судом дело Sõro v. Estonia (постановление от 3 сентября 2015 г.) касается жалобы относительно опубликованной в 2004 г. в государственной газете Эстонии информации о работе заявителя в КГБ в качестве водителя. Суд посчитал это нарушением ст. 8 Конвенции, поскольку данная мера не была пропорциональна преследуемой цели. По мнению Суда, согласно национальному законодательству информация относительно работников бывших специальных служб, включая водителей, была опубликована безотносительно конкретной функции, которую они выполняли. Более того, в то время как Закон о раскрытии информации вступил в силу через три с половиной года после провозглашения независимости, публикация информации о бывших работниках спецслужб растянулась на годы. Рассматриваемая информация в отношении заявителя была опубликована в 2004 г. и без всякой оценки того, представляет ли заявитель какую-либо угрозу. Наконец, хотя Закон о раскрытии информации не налагал никаких ограничений на работу, заявитель согласно его утверждениям был высмеян его коллегами и был вынужден уволиться. Суд отметил, что достигнутый результат тем не менее свидетельствует о том, насколько серьезным оказалось вмешательство в право заявителя на уважение его частной жизни.

§ 12. Доступ к личным данным

В деле Gaskin v. the United Kingdom от 7 июля 1989 г. заявитель, взятый в детстве под опеку, по достижении совершеннолетия желал узнать о своем прошлом, чтобы преодолеть свои личные проблемы. Суд установил нарушение требований ст. 8 Конвенции, поскольку примененные процедуры не обеспечили уважения частной и семейной жизни заявителя. Было отмечено, что лица, находящиеся в положении заявителя, имели защищаемый Конвенцией жизненный интерес в получении необходимой информации, чтобы понять, как прошло их раннее детство. Вместе с тем следует иметь в виду, что конфиденциальность публичных записей важна для получения объективной и достоверной информации и может быть необходима для защиты третьих лиц. В последнем аспекте британская система, которая предусматривает доступ к документам в зависимости от наличия согласия заявителя, в принципе может считаться отвечающей обязательствам по ст. 8 с учетом пределов усмотрения государства. По мнению Суда, однако, в указанной системе интересы лица, стремящегося получить доступ к записям, относящимся к его личной и семейной жизни, должны быть обеспечены, если сделавшее их лицо недоступно или отказывается ненадлежащим образом дать такое

согласие. Указанная система соответствует принципу пропорциональности, если предусматривает, что независимый орган в конечном счете решает, может ли быть предоставлен доступ в случаях, когда внесший запись не отвечает или отказывает в согласии. В рассматриваемом деле в распоряжении заявителя не имелась такая процедура.

Согласно постановлению Roche v. the United Kingdom от 19 октября 2005 г. заявитель был уволен из армии в конце 1960-х гг. В 1980-х годах у него участилось поывшение кровяного давления, позже к гипертонии присоединились бронхит и бронхиальная астма. Он был зарегистрирован в качестве инвалида и утверждал, что его проблемы со здоровьем — результат его участия в испытаниях горчичного и нервно-паралитического газа, проведенных британскими вооруженными силами (Porton Down Barracks, England) в 1960-х гг. Заявитель указывал, что он не имел доступа ко всей соответствующей информации, которая позволила бы ему оценить любой риск, которому он подвергался во время своего участия в этих испытаниях. Суд посчитал, что допущено нарушение ст. 8 Конвенции, а именно: Соединенное Королевство не выполнило своего позитивного обязательства обеспечить эффективную и доступную процедуру, позволяющую заявителю иметь доступ ко всей соответствующей информации, чтобы оценить любой риск, которому он подвергался во время своего участия в испытаниях. Любое находящееся в положении заявителя лицо, которое последовательно добивалось такого доступа независимо от каких-либо судебных разбирательств, не должно требовать их проведения для получения информации. Важно добавить, что в области информационных услуг и здравоохранения исследования инициировались только спустя почти 10 лет после того, как заявитель начал поиск документов, подав затем жалобу в Суд.

Дело Magyar Helsinki Bizottság v. Hungary (постановление от 8 ноября 2016 г.) показательно с точки зрения права на получение информации. Оно касается отказа властей предоставить неправительственной организации (далее — НПО) информацию, касающейся по долгу службы адвоката, на том основании, что такая информация классифицируется в качестве персональных данных, не подлежащих раскрытию по венгерскому законодательству. Заявитель-НПО утверждала, что суды Венгрии, отказав в передаче информации, нарушили ее право на доступ к ней. Суд посчитал, что право заявителя было нарушено на основании ст. 10 Конвенции (свобода выражения мнения). Он отметил, что информация, запрошенная заявителем, была необходима для завершения исследования о функционировании системы защиты, проводимой им в качестве молодежной правозащитной организации с целью содействия обсуждению вопро-

са, представляющего значительный общественный интерес. По мнению Суда, отказывая заявителю в доступе к запрашиваемой информации, национальные власти препятствовали реализации НПО ее права на свободу получения и передачи информации, нарушая таким образом саму суть их прав по ст. 10 Конвенции. Суд далее отметил, что право частной жизни защитников не было бы затронуто негативно, если бы запрос заявителя-НПО о предоставлении информации был удовлетворен, поскольку, хотя по общему признанию запрос информации касался личных данных, он не связан с данными не для всеобщего ознакомления. В постановлении также отмечается, что венгерское право, как его интерпретировали национальные суды, исключает значительную оценку права заявителя на свободу выражения мнения. Любые ограничения в отношении предполагаемой публикации, которая должна была способствовать обсуждению вопросов, представляющих общий интерес, следовало бы подвергать тщательному анализу. Наконец, аргументы венгерского правительства нельзя признать достаточными, показывающими, даже несмотря на существующую дискрецию, что обжалуемое вмешательство было «необходимым» в демократическом обществе. Не было также разумной пропорциональности между обжалуемой мерой (отказ предоставить имена ex officio адвокатов и случаев, когда они были назначены в качестве защитников в определенных юрисдикциях) и преследуемой законной целью (защита прав других лиц).

§ 13. Удаление или уничтожение личных данных

Постановление по делу Rotaru v. Romania от 4 мая 2000 г. касается утверждений заявителя о том, что невозможно было опровергнуть неверную информацию, хранящуюся в файле румынской разведывательной службы (RIS). Он был осужден к одному году лишения свободы в 1948 г. за критику коммунистического режима. Суд пришел к выводу о нарушении ст. 8 Конвенции на том основании, что хранение и использование разведслужбой информации о личной жизни заявителя не соответствовало закону. Он также отметил, что публичная информация, относящаяся к сфере частной жизни, может систематически собираться и храниться в файлах, принадлежащих органам власти. Это касается информации, относящейся к прошлому человека. В национальном праве нет положений, определяющих, какой вид информации может быть зарегистрирован, категории людей, в отношении которых могут быть приняты такие меры наблюдения, процедуры сбора и хранения информации, обстоятельства, в которых подобные меры могут быть приняты, или процедуры,

которым необходимо следовать. Соответствующий национальный закон не устанавливает ограничений по сроку давности информации или сроку ее хранения. Наконец, не было четкого, подробного положения, касающегося лиц, уполномоченных просматривать файлы, характера самих файлов, процедур и использования полученной таким образом информации.

Суд посчитал, что румынское законодательство не указывает с достаточной ясностью объем и способ применения предоставленного органам государственной власти соответствующего усмотрения. В данном деле Суд определил также нарушение ст. 13 Конвенции, поскольку заявитель не имел возможности оспорить хранение данных или опровергнуть правдивость рассматриваемой информации.

§ 14. Свобода выражения мнения и электронная коммерция

Delfi AS v. Estonia — первое дело (постановление от 16 июня 2015 г.), в котором Суд должен был проверить жалобу об ответственности за комментарии пользователей на новостном интернет-портале. Национальные суды отклонили аргумент портала о том, что в соответствии с Директивой ЕС 2000/31/ЕС об электронной коммерции его роль в качестве поставщика услуг информационного общества или хост-системы хранения была чисто технической, пассивной и нейтральной. Было установлено, что портал осуществляет контроль над публикацией комментариев. Суд посчитал, что требования ст. 10 Конвенции (о свободе выражения мнения) не были нарушены, поскольку решение эстонского суда об ответственности компании-заявителя было оправданным и соразмерными ограничению свободы выражения мнения на портале. Большая палата подчеркнула, в частности, что национальные суды должны решать вопросы толкования и применения внутреннего права. Он, таким образом, не затрагивал проблему в соответствии с законодательством ЕС и ограничился вопросом о том, было ли предсказуемым применение Верховным Судом национального права к ситуации заявителя-компании.

Однако анализ был бы неполным без отдельных важных решений Суда ЕС. К ним относится дело Google Spain SL, Google Inc. v. Agencia Espanola de Protection de Dafos and Mario Costela Gonzales (постановление от 13 мая 2014 г.). Указанное дело имеет много общего с рассмотренным Большой палатой ЕСПЧ делом Delfi As v. Estonia. Факты дела Google Spain дела следующие: в 2010 г. Mario Costela Conzales обратился с жалобой в испанское агентство по защите данных (AE PD) на издателя ежедневной газеты с большим тиражом в Испании, а также против Google Испании и Google Inc. Он оспари-

вал правомерность того, что, когда пользователь Интернета вводил свое имя в поисковик группы Google (поиск Google), в списке результатов отображались ссылки на две страницы газеты La Vanguardia за январь и март 1998 г. Эти страницы содержали объявления об аукционе по недвижимости, организованном после присоединения к процедуре взыскания долгов по социальному обеспечению, причитающихся с г-на Costela Gonzalez. Заявитель требовал, во-первых, от La Vanguardia удалить либо изменить рассматриваемые страницы (чтобы больше не появлялись относящиеся к нему персональные данные) или использовать определенные инструменты, предоставляемые поисковыми системами, для защиты данных. Во-вторых, он просил, чтобы Google Spain или Google Inc. удалили или скрыли относящиеся к нему личные данные, чтобы они больше не появлялись в результатах поиска и в ссылках на La Vanguardia. В этом контексте заявитель утверждал, что разбирательство по делу было полностью завершено и упоминание о нем в настоящее время совершенно не имеет значения (парадокс, но заявитель после этого решения будет постоянно упоминаться как поборник «права быть забытым»).

Агентство по защите данных отклонило жалобу против La Vanguardia, полагая, что данная информация была опубликована правомерно. Вместе с тем жалоба в отношении Google Spain и Google Inc. была удовлетворена. Агентство просило две компании предпринять необходимые меры для изъятия данных из их индекса и сделать доступ к ним невозможным в будущем. Google Spain и Google Inc. в свою очередь обратились с двумя исками в Национальный Верховный Суд Испании об отмене решения агентства. Именно в таком контексте и направил испанский суд ряд вопросов в Суд ЕС.

В своем решении Большая палата Суда ЕС пришла к выводу, что даже если физически сервер компании, обрабатывающей данные, находится за пределами Европы, правила ЕС применяются к операторам поисковых систем, если у них есть филиал или дочерняя компания в государстве-члене, которая способствует продаже рекламного пространства, предлагаемого поисковой системой. Последние являются контролерами персональных данных. Google, таким образом, должна выполнять свои обязанности в соответствии с европейским законодательством при обработке личных данных, сославшись на поисковую систему. Действует закон ЕС о защите данных, а также «право быть забытым».

Таким образом, Суд ЕС считает, что при определенных обстоятельствах человек имеет право обратиться с требованием, чтобы в поисковых системах были удалены ссылки с личной информацией о нем, и это относится к случаям, когда информация является неточ-

ной, неадекватной, несоответствующей для целей обработки данных. По мнению Суда ЕС, в рассматриваемом деле вмешательство в права лица не может быть оправдано просто экономической заинтересованностью поисковой системы. Суд ЕС четко разъяснил, что «право быть забытым» не является абсолютным, а должно коррелировать с другими фундаментальными правами — правом на свободу выражения и свободу средств массовой информации.

После дела Google Spain Суд ЕС, похоже, взял на себя ведущую роль в определении права на цифровую конфиденциальность в Европе. Следуя этому решению, рассматриваемые судьями Суда ЕС дела обусловили значительное укрепление этой свободы в конституционно-правовом смысле, установив примат этого права над другими законными правами и интересами.

Следует заметить, что еще до рассмотрения дела Google Spain Большая палата Суда ЕС вынесла постановление по делу Digital Rights Ireland Ltd (C-293/12) от 8 апреля 2014 г. В этом деле Суд ЕС подчеркнул, что он широко интерпретирует право на неприкосновенность частной жизни при рассмотрении Директивы о сохранении данных. Он отметил, что эта директива была введена для гармонизации национального законодательства, регулирующего массовое хранение метаданных из цифрового трафика, для предотвращения серьезных преступлений. Согласно директиве такие данные могут храниться не менее шести месяцев и не более двух лет. Суд подчеркнул, что вмешательство указанных положений в права, предусмотренные ст. 7 и 8 Хартии ЕС об основных правах, было бы особенно серьезным, поскольку «оно может вызвать в умах заинтересованных лиц ощущения, что их частная жизнь является предметом постоянного наблюдения» (§ 37). Судьи оценили, было ли вмешательство оправданным в свете ст. 52 Хартии, допускающей ограничение свобод при условии соблюдения сути этих свобод, отвечающей целям общих интересов и пропорциональности преследуемой цели. В связи с первым аспектом Суд аргументировал, что это не нанесло ущерба сути этого права, поскольку ограничивалось использованием данных и не рассматривало содержание сообщений. Более того, такой сбор данных предназначен для предотвращения и борьбы с преступностью и, по мнению Суда, было оправданно по причинам общественной безопасности. Однако в вопросе пропорциональности недоставало элементов. Во-первых, правила директивы кажутся общими и содержат пробелы, когда речь идет о людях, на которых влияет сбор данных, охватывающий «все европейское население» (§ 56) и «всех лиц и все средства электронной связи, а также все данные о трафике без каких-либо различий, ограничений или исключений, сделанных

в целях борьбы с серьезными преступлениями» (§ 57). Во-вторых, директива «не устанавливает какой-либо объективный критерий, с помощью которого можно определить пределы доступа компетентных национальных органов к данным и их использования в целях предотвращения, выявления или уголовного преследования за совершенные преступления, принимая во внимание степень и серьезность вмешательства в основные права, закрепленные в ст. 7, 8 Хартии, которые можно рассматривать в качестве серьезных оснований, оправдывающих вмешательство» (§ 60). В связи с данным решением исследователи отмечали, что оно позволило европейским гражданам добиваться отмены национальных правил хранения данных в местных судах, поскольку это нарушало «право на защиту данных, передаваемых через Интернет»[1]. После этого решения Суда ЕС многие национальные правовые системы эффективно провозглашали отдельные правила неконституционными, поддержав таким образом возросшую важность этого права в Европе[2].

Важным в этом ряду представляется дело Maximillian Schrems v. Data Protection Comissioner (постановление Суда ЕС от 6 октября 2015 г.). Суд ЕС лишил законной силы так называемое соглашение между Европейской комиссией и Соединенными Штатами Америки о «Безопасной гавани» (Safe Harbor), передаче данных между двумя сторонами Атлантики. Maximillian Schrems — австрийский юрист, который сначала обращался с жалобой к властям Ирландии и затем в Суд ЕС, чтобы передача его личных данных, полученных через Facebook, от ирландского филиала этой компании ее калифорнийскому родителю была объявлена незаконной. Трансграничный трафик цифровых данных уже давно является фундаментальными инструментом в торговых отношениях между Европой и Америкой. В целях реализации Директивы 95/46/ЕС, разрешающей передачу данных из ЕС в компании США, которые ратифицировали соглашение о «безопасной гавани» (принятие принципов защиты конфиденциальности, предусмотренных в европейском праве)[3]. Суд ЕС в названном постановлении признал это решение недействительным, указав, что оно «не может помешать лицам, чьи личные данные были

1 Federico Fabbrini. The European Court of Justice Ruling on the Data Retention Case and its Lessons for Privacy and Surveilllance in the US (2015) 28 Harv. Hum. Rts. J. 88.

2 См.: Niklas Vainio, Samuli Miettinen. Telecommunications data retention after Digital Rights Ireland: legislative and judicial reactions in the Member States. 2015. Int J Law Info Tech 23 (3), 290.

3 Di Luca Pietro Vanoni. Balancing privacy and national security in the global digital era: a comparative perspective of EU and US constitutional systems in Forum Quaderni Constituzionali — Paper, 14 giugno 2017. P. 7.

или могут быть переданы в третью страну, подать в национальные надзорные органы иск... о защите прав и свобод в отношении обработки данных» (§ 53). Такой подход усиливает власть национальных органов, которые должны быть способны независимо оценить, соответствует ли директиве передача личных данных в страну за пределы ЕС. Суд ЕС признал также недействительным решение Комиссии, поскольку правило, «позволяющее государственным органам на обобщенной основе иметь доступ к содержанию электронных сообщений», ставит под угрозу «суть основного права на уважение частной жизни» (§ 94), когда он не предусматривает «какой-либо возможности для лица прибегать к средствам правовой защиты для получения доступа к относящимся к нему личным данным или для исправления или удаления таких данных» (§ 95).

Большая Палата Суда ЕС, рассмотрев объединенные дела Tele2 Sverige and Watson, вынесла постановление от 21 декабря 2016 г., сделав акцент на защиту неприкосновенности частной жизни, полагая, что национальное право, устанавливающее общее и неизбирательное обязательство поставщиков услуг электронной связи хранить данные клиентов и предоставлять органам власти общий доступ к таким данным, несовместимо с законодательством ЕС.

В постановлении Большой палаты Суда ЕС по делу Unabhängiges Landeszentrum für Datenschutz Schleswig — Holstein v. Wirtshafsakademie Schleswig GmbH (постановление от 5 июня 2018 г.) подчеркивается, что владелец страницы Facebook должен рассматриваться в качестве совместного контролера вместе с Facebook и, таким образом, также отвечать за обработку персональных данных посетителей фан-страницы Facebook под защитой данных ЕС. В то время как приведенный вывод Суда ЕС основан на прежних правилах защиты данных ЕС, которые были заменены 25 мая 2018 г. на Общий регламент по защите данных (GDPR), они так же важны в контексте новой правовой базы, поскольку термины и концепции в этой области остались прежними. Решение Суда ЕС подтверждает, что в нормативном регулировании защиты данных не должно быть пробелов, а основные права человека подлежат обязательной защите.

Таким образом, представленные судебные решения служат усилению гарантий прав и свобод человека посредством эффективной защиты персональных данных, отвечая одновременно на вызовы времени путем поддержания надежного баланса между необходимостью защиты национальной безопасности и общественного порядка и соблюдением цифровой конфиденциальности.

ЗАКЛЮЧЕНИЕ

Проведенное исследование судебной практики показало, что большое количество вопросов в сфере обработки личных данных пользователей сети «Интернет» содержат дела последних пяти лет, особенно — последних двух-трех лет, что актуализирует определение нового порядка обработки персональных данных, а также реализацию соответствующих прав и их защиты посредством обновленных механизмов. Согласно выводам, сделанным авторами настоящего комментария, также показывают, что многие подходы в области защиты личных данных, остававшиеся долгое время универсальными, не могут быть реализованы в условиях стремительного развития цифровых технологий. Законодательные решения отстают от развивающихся правоотношений. В таких условиях необходимо повышение роли взаимосвязи законодательного и правоприменительного процессов, вовлечение правовой доктрины через правоинтерпретационную деятельность судов. Как продемонстрированно на примерах дел в области развития технологий Big Data, стороны судебного разбирательства зачастую привлекают зарубежные судебные доктрины для обоснования своей позиции по делу, которые анализируются судом с разных сторон. Полагаем, подобная практика является ответом на стремительное развитие цифровых технологий, когда суд с учетом множества обстоятельств дела должен верно распорядиться предоставляемой ему процессуальным законодательством дискрецией по вопросам оценки доказательств, квалификации правоотношений сторон, определения баланса частных и публичных интересов и т.д.

Следует отметить, что все большее значение приобретает доведение до субъектов персональных данных условий обработки таких данных, особенно в сети «Интернет». Предоставление простого согласия на обработку персональных данных без заполнения необходимых форм на интернет-странице может означать, что лицо не осознает последствий предоставления своих данных для последующей обработки путем включения их в различные базы данных. Суды также определили, что использование алгоритмов обработки личной переписки собственниками соответствующих ресурсов обмена сообщениями недопустимо.

Кроме того, сведения, полученные путем извлечения переписки из социальных сетей, мессенджеров, электронной почты, не вызывают доверия в связи с невозможностью их достоверного соотнесения

с автором сообщений. Для подтверждения их доказательственного значения, даже при условии удостоверения таких документов нотариусом, требуется совокупность иных косвенных доказательств.

Особого внимания требуют проблемы идентификации пользователей в сети «Интернет». Судебная практика по разным категориям дел демонстрирует, что использование электронной подписи для целей доставки юридически значимых сообщений положительно себя не зарекомендовало. В основном в гражданском обороте используется электронная почта, при этом она не всегда признается надлежащим средством доставки сообщений. Большое количество судебных разбирательств, связанных с использованием электронной подписи (как простой, так и усиленной), демонстрирует, что она зачастую используется неправомерно. Получение такой подписи в аккредитованном удостоверяющем центре не обеспечивает необходимого уровня доверия контрагентов к подписанным таким образом документам. Для гражданского оборота целесообразен упрощенный способ идентификации, когда предоставление и отзыв полномочий на доставку юридически значимых сообщений либо на совершение сделок могут быть совершены в короткий срок без посещения удостоверяющих центров, например путем выдачи электронной доверенности с ее привязкой к номеру телефона или иным средствам идентификации. Уход от электронной подписи как тенденция развития гражданского оборота может быть также приемлем при исключении самого понятия электронной цифровой подписи из ГК РФ в связи с внедрением категории цифровых прав.

Исследование практики использования личной переписки и иной персональной информации демонстрирует, что правоохранительные органы могут осуществлять сбор и извлечение необходимых для целей расследования личных данных без последующего предоставления стороне защиты разъяснения порядка совершенных с такими данными процессуальных действий на основании законодательства о государственной тайне. В связи с этим сведения из электронной переписки используются при обосновании принимаемых судом решений в основном по уголовным делам. Стороны цивилистического судебного процесса должны доказать достоверность и допустимость предоставленных доказательств, раскрыть порядок их получения и обработки.

В рамках исследования тенденций развития европейского законодательства и практики его применения можно отметить тенденцию усиления защиты персональных данных граждан в их взаимоотношениях с частными компаниями, занимающимися обработкой таких данных, равно как и с государством. При этом Суд ЕС, ЕСПЧ исхо-

дят из необходимости защиты человеческого достоинства, недопустимости неограниченного и бессистемного сбора информации, доведения ее до общественности без возможности последующего удаления по просьбе заинтересованного лица. Многие проблемы, как видится, указанным международным судам еще только предстоит рассмотреть, разработав соответствующие подходы защиты личных данных граждан, с учетом их возрастающей значимости и доступности.

Научное издание

ЗАЩИТА ДАННЫХ

научно-практический
комментарий
к судебной практике

Ответственные редакторы
доктор юридических наук, профессор
В.В. Лазарев,
доктор юридических наук
Х.И. Гаджиев

Ответственные секретари
Ю.Э. Ибрагимова, А.И. Сидоренко

Подписано в печать 20.12.2019.
Формат 60×90/16. Бумага офсетная. Гарнитура Newton.
Печать офсетная. Усл. печ. л. 11,0. Усл. изд. л. 9,8.
Тираж 500 экз. (1-й завод 1–60 экз.). Заказ № .

Институт законодательства и сравнительного правоведения
при Правительстве Российской Федерации