НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ «ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»

Доклад НИУ ВШЭ

«РЕГУЛИРОВАНИЕ ДАННЫХ В РОССИЙСКОЙ ФЕДЕРАЦИИ: ТЕКУЩЕЕ СОСТОЯНИЕ, ПРОБЛЕМЫ, ПЕРСПЕКТИВЫ»

Руководители авторского коллектива:**М.В.Якушев, А.А.Ефремов**

Издательский дом
Высшей школы экономики
Москва, 2021

Данные как основа цифровой экономики и как объект правового регулирования

1. *Цифровая трансформация* определена в качестве одной из национальных целей развития Российской Федерации на период до 2030 г. (в соответствии с указом Президента РФ от 21.07.2020 N 474). В 2020 г. в Конституции РФ появилась норма, предусматривающая отнесение к предметам ведения РФ обеспечение безопасности личности, общества и государства при обороте цифровых данных. Стратегия развития информационного общества в Российской Федерации на 2017 – 2030 годы[1] предусматривает необходимость «обеспечить баланс между своевременным внедрением современных технологий обработки данных и защитой прав граждан, включая право на личную и семейную тайну».

2. Вместе с тем, имеет место *снижение позиций России в международных рейтингах*, связанных с развитием цифровых технологий и цифровой трансформации. Так, в 2020 г. снизилось с 32 до 36 место России в рейтинге электронного правительства ООН (EGDI), а в Глобальном инновационном индексе (GlobalInnovationIndex) по показателю «качества регулирования позиция» России снизилась с 96 места в 2018 г. до 105 – в 2020 г.

3. Указанные обстоятельства свидетельствуют об актуальности изучения и *совершенствования правового регулирования оборота данных* в России. Институтом права цифровой среды НИУ ВШЭ в 2020 году проведены комплексные исследования в области правовых аспектов данных, включая *общетеоретические* вопросы, а также более конкретные вопросы оборота *общедоступных данных* и современного состояния регулирования данных при соблюдении *тайны связи.* Результаты указанных исследований представлены в настоящем докладе.

Понятие «данных» в правовой теории. Текущее состояние правового регулирования данных в Российской Федерации

4. Несмотря на то, что информация в человеческом обществе существует с момента его зарождения, а его эволюция немыслима без использования информации, как таковая информация долгое время (за отдельными исключениями) не являлась объектом правоотношений. Правовое регулирование стало осуществляться в отношении лишь тех объектов, которые имели реальную экономическую ценность. В «постиндустриальном», «информационном» обществе, для которого характерно определенное экономическое благополучие человечества, приобретают особое значение не только экономические права и свободы, но и нематериальные блага, направленные на свободное и полное развитие личности.

[1] Утверждена указом Президента РФ от 09.05.2017 N 203

5. Правовой институт *данных* тесно связан с понятием *информации*, выделение которой в качестве отдельного объекта правоотношений было обусловлено как социально-экономическим развитием, так и собственно эволюцией юридической теории. Информация – одна из правовых категорий, относительно определения которой нет единой точки зрения. Действующее федеральное законодательство[2] определяет информацию как «(…) сведения (сообщения, данные) независимо от формы их представления». Таким образом, в настоящее время ставится *знак равенства между* такими понятиями, как «информация», «сведения», «сообщения», «данные». Такая позиция является неточной и устаревшей.

6. Следует отметить, что в нормативных правовых актах до последнего времени в основном использовался термин «информация», однако применительно к определенным правовым институтам используется именно термин «данные» (*персональные данные, базы данных, большие данные, открытые данные*, и т.п.). При этом замена термина «данные» на равнозначный согласно законодательному определению термин «информация» приводит к качественному изменению смысла регулируемых категорий: например, «*открытые данные*» и «*открытая информация*» имеют существенно различное содержание и объёмы понятий.

7.Ситуация с используемой терминологией изменилась с развитием нормотворчества в рамках перехода к цифровой экономике. Термин «информация» практически вышел из употребления и почти повсеместно был заменен «данными», которые рассматриваются как «ключевой актив цифровой экономики».В определении *цифровой экономики*, приведенном в Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы,[3] цифровая экономика рассматривается как «хозяйственная деятельность, в которой *ключевым фактором производства являются данные в цифровом виде*, обработка больших объемов и использование результатов анализа которых (…) позволяют существенно повысить эффективность различных видов производства (…)».

8.Таким образом, следует законодательно отграничить правовую категорию «данных» от включающей её сейчас категории «информации». Что касается юридической науки, то она с легкостью перешла с термина «информация» на термин «данные» без каких-либо уточнений и оговорок. Лишь в единичных публикациях ставится вопрос о необходимости разграничения терминов «информация» и «данные», использование которых как синонимов создает проблемы

[2] Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации" // СЗ РФ, 31.07.2006, N 31 (1 ч.), ст. 3448; далее – «ФЗ об информации».
[3] Утверждена Указом Президента РФ от 9 мая 2017 г. № 203.

в правоприменительной практике. В этой связи[4] следует зафиксировать, что понятие данных, вне анализа юридических нюансов его содержания, успешно используется в специальной литературе в соответствии с определением Международной организацией по стандартизации, согласно которому «данные – это представление информации (фактов, концепций или инструкций) в виде, пригодном для передачи, связи или обработки как человеком, так и автоматическими средствами»[5].

9.После внесения в 2020-м году в Конституцию Российской Федерации изменений, в ней присутствуют *и* информация, *и* данные. При этом, если в отношении информации по-прежнему сохраняются права свободно искать, получать, передавать, производить и распространять информацию любым законным способом, то применительно к данным речь уже идет об их *обороте*. Но «оборот данных» еще не означает *исключительно экономический* оборот, возможен и *неэкономический оборот* данных, например, получение, обработка и предоставление данных в государственных информационных системах. Включение в Конституцию упоминания об обороте *цифровых данных* ставит вопросы о специфическом правовом режиме именно цифровых данных, о свободном или ограниченном обороте определенных категорий данных (либо о запрете таковых), о лицах, обладающих правами на различные действия с этими данными, об основаниях их возникновения и прекращения.

10.Новой для правовой науки является и категория *управление данными*, поскольку до принятия нормативных правовых актов по развитию цифровой экономики такое словосочетание практически не использовалось. К сожалению, как подробно проанализировано в проведённом в рамках данной проектной работы исследовании, разработка и принятие Концепции создания и функционирования национальной системы управления данными[6] происходило без учёта действующей нормативной базы и привлечения экспертов в соответствующей предметной области. В результате указанная Концепция на практике применяться не может, сроки исполнения «дорожной карты» по её реализации, рассчитанной до 2021 года, полностью сорваны[7].

11.Необходимость существенной модернизации нормативного массива информационного права, обусловленного формированием цифровой экономики, сомнений не вызывает. Целесообразно выделить два основных направления правового регулирования

---

[4] Напр., Савельев А.И. Гражданско-правовые аспекты регулирования оборота данных в условиях попыток формирования цифровой экономики // Вестник гражданского права. 2020. N 1. С. 60 - 92.

[5]ДокументISO/IEC/IEEE 24765:2010(en); по-английски: *representation of facts, concepts, or instructions in a manner suitable for communication, interpretation, or processing by humans or by automatic means.*

[6] Утверждена распоряжением Правительства РФ от 03.06.2019 № 1189-р.

[7] См. Постановление Правительства РФ от 24.11.2022 № 1911.

данных: (1) *корректировку действующего законодательства* в целях его соответствия новым реалиям (применительно к различным категориям данных речь идет о персональных данных, иных охраняемых законом видов информации, идентификации и аутентификации, электронном документообороте и пр.) и (2) разработку*новых законодательных и подзаконных актов*, в том числе в случае появления новых объектов правоотношений (применительно к данным речь может идти и «больших данных», обезличенных данных, открытых данных, *цифровом профиле* и т.п).Возможно также (3) *сохранение действующего регулирования* без внесения каких-либо изменений, с учётом возможностей *саморегулирования* и *применения правовых норм по аналогии*. Следует помнить, что на разных этапах развития экономических отношений наблюдаются разное соотношение государственного регулирования, дерегулирования и допустимости саморегулирования в тех или иных сферах, что зависит от целого ряда причин. Отказ от правового регулирования может быть обусловлен различными факторами, в частности, применительно к общественным отношениям, которые государство *не считает нужным* регулировать, или *неэффективно регулировать* правом, или *невозможно регулировать* правом. К правовым институтам, связанным с категорией данных, это относится в полной степени.

12.Действующее российское законодательство в сфере данных характеризуется фрагментарностью, внутренней несогласованностью в регулировании информационных отношений, отсутствием должной координации разработки новых правовых актов и внесения изменений в уже существующих. Помимо уже упоминавшегося «базового» ФЗ об информации, отдельные аспекты использования данных, как разновидности правовой категории информации, регулируются в кодексах (Гражданском, Уголовном, Налоговом, Кодексе об административных правонарушениях), двух федеральных законах о доступе к информации[8], и нескольких десятках иных федеральных законов.

13.Детальное регулирование *персональных данных* содержится в Федеральном законе «О персональных данных»[9]. В нем персональные данные определяются как «*любая информация,* относящая к прямо или косвенно определённому или определяемому физическому лицу» – то есть и здесь данные определяются как информация. Положения российского законодательства, регулирующие отношения в сфере предоставления доступа к открытым данным, открытыми данными называют *форму представления информации*, размещаемой в интернете в

[8]Федеральный закон от 09.02.2009 N 8-ФЗ "Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления" // СЗ РФ, 16.02.2009, N 7, ст. 776., Федеральный закон от 22.12.2008 N 262-ФЗ "Об обеспечении доступа к информации о деятельности судов в Российской Федерации" // СЗ РФ, 29.12.2008, N 52 (ч. 1), ст. 6217.

[9] Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных" // СЗ РФ, 31.07.2006, N 31 (1 ч.), ст. 3451; далее – «ФЗ о персональных данных».

установленном законом формате[10]. Законодательство о тайнах (о коммерческой, государственной, врачебной и иных видах тайны) определяет информацию, составляющую ту или иную тайну, через категорию *сведений.*

14.Таким образом, единообразный подход к пониманию различий между категориями «информация», «данные», «сведения», «сообщения» *не соблюдается*. Понятия «информация» и «данные» чаще всего определяются одно через другое, в результате чего анализ содержания указанных понятий в законодательстве представляет собой безрезультатный замкнутый круг. Такая ситуация не может считаться допустимой, поскольку излишняя синонимичность может вредить юридической технике и, как следствие, влиять на качество правового регулирования[11].

15.На доктринальном уровне признаётся, что данные становятся информацией только тогда, когда они *помещены в определенный контекст и воспринимаются человеком*. При этом возможен и представляется более продуктивным подход, при котором данные (как информация, представленная в форме, пригодной для последующей обработки) могут рассматриваться в правовом смысле по аналогии с извлечёнными полезными ископаемыми и представлять собой «сырьё» для последующей обработки и изготовления продуктов, имеющих потребительскую ценность и востребованных на рынке конечных потребителей. В этом случае информация, представляющая собой предмет преимущественно публично-правовых отношений, будет являться почти полной аналогией природным ресурсам (полезным ископаемым) до их извлечения и введения в гражданский оборот последующей переработкой (обработкой).

16.Появление категории данных как «*сырья*» для информационных продуктов связано с процессами развития цифровых технологий, в том числе технологий обработки «больших данных», искусственного интеллекта, интернета вещей. Развитие таких технологий привело к своеобразному исключению человека из процесса сбора и обработки информации, сделав сам фактор человеческого восприятия указанных сведений на определенных этапах их обработки *не значимым*.

17.В эпоху «больших данных» и машинного обучения возможности по преобразованию данных в *полезную* информацию многократно увеличились, что увеличило актуальность правового регулирования отношений в сфере оборота данных. Объектом охраны в отношении данных является не конкретная смысловая единица (либо совокупность таких смысловых единиц), а *массивы данных*, представленные, как правило, в цифровом виде и обрабатываемые в

[10] Ч. 4 ст. 7 ФЗ об информации.

[11]Суслопаров А.В. Соответствие норм Уголовного кодекса России принципу единства и определенности терминологии на примере терминов "информация", "сведения", "данные" // Законы России: опыт, анализ, практика. 2017. N 11. С. 94 - 98.

компьютерных информационных системах – при том, что традиционный объект регулирования совокупности данных (*базы данных*) относится к интеллектуальной собственности и охраняет не контент (собственно данные), а структуру баз данных по аналогии с литературными произведениями.

18.Определение понятия *набора данных* содержится в Национальной стратегии развития искусственного интеллекта на период до 2030 года[12], в соответствии с которой под ним понимается «совокупность данных, *прошедших предварительную подготовку (обработку)* в соответствии с требованиями законодательства Российской Федерации об информации (..) и необходимых для разработки программного обеспечения на основе искусственного интеллекта». Данное определение носит достаточно узкий характер, в том числе с точки зрения указанной в нем цели – разработки программного обеспечения.

19.Правовой режим данных должен быть дифференцированным в зависимости от потребностей регулирования и соответствующих приоритетов государственной политики. В условиях цифровой экономики (и появления соответствующей категории в Конституции РФ) важно выделить сферу правового регулирования оборота *цифровых данных*, то есть *данных, представленных в электронной форме и обрабатываемых в информационных системах*. Возможно также выделение категорий *обработанных – необработанны*х данных (что позволит более аккуратно регулировать так называемые *сырые данные*, однозначно регламентируя обязанности обладателя информации по приведению данных в вид, пригодный к применению) и категории «неперсональных» данных, подобно тому, как это уже сделано в Европейском Союзе.

20.Отдельного внимания заслуживает проблематика *общедоступных данных*, потенциал использования которых очень значителен – такие данные могут использоваться для повышения эффективности работы государственных органов и обеспечения прозрачности их деятельности для общества, для повторного использования в экономике и создания новых продуктов. В то же время тесно связанные между собой право на неприкосновенность частной жизни и защиту персональных данных по своей правовой природе концептуально противоположны «полной правовой и технической открытости»[13], которой характеризуются общедоступные данные, доступ к которым *не ограничен* в соответствии с нормами международного права, внутригосударственного законодательства или принятыми их обладателем организационными и (или) техническими мерами по ограничению такого доступа.

[12]УтвержденаУказомПрезидентаРФот 10.10.2019 N 490.

[13] Dalla Corte L. (2018) The European Right to Data Protection in Relation to Open Data. In: van Loenen B., Vancauwenberghe G., Crompvoets J. (eds) Open Data Exposed. Information Technology and Law Series, vol 30. T.M.C. Asser Press, The Hague.

21.Следует, однако, учитывать, что в федеральном законах имеются нормы, относящиеся к разным категориям данных (информации):

- *общедоступная информация* (ст. 7 ФЗ об информации);

- *общедоступные персональные данные* и общедоступные источники персональных данных (п. 10 ч. 1 ст. 6, ст. 8, п. 2 ч. 2 ст. 10, п. 3 ч. 4 ст. 18 ФЗ о персональных данных);

- *открытые данные* (ч. 4, 5 ст. 7 ФЗ об информации), в том числе *общедоступная информация о деятельности государственных органов и органов местного самоуправления в форме открытых данных* (ч. 2.1 ст. 7 Федерального закона от 09.02.2009 N 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»);

- *обнародованные базы данных* (п. 2 ст. 1260, ст. 1333-1336 ГК РФ).

22.Общая дефиниция, определяющая общедоступные данные (ст. 7 ФЗ об информации) через критерий фактического *отсутствия ограничений доступа* к такой информации, устанавливая тем самым презумпцию общедоступности любой информации, размещенной в «открытом доступе», представляется соответствующей целям регулирования. В то же время, нужно иметь в виду, что «ограничение доступа» представляет собой довольно широкое понятие, которое потенциально может охватывать разнообразные *юридические, организационные и технические ограничения*. Это, в свою очередь, может приводить к пограничным ситуациям, вызывающим трудности на практике. Например, это касается размещения информации в рамках сервисов, доступ к которым предоставляется любому лицу, но при условии прохождения им предварительной регистрации и (или) внесения платы.

23.Федеральный закон о персональных данных разделяет понятия персональных данных, *сделанных общедоступными субъектом* персональных данных, и *общедоступных источников* персональных данных. Обработка общедоступных персональных данных не обеспечена дополнительными гарантиями, например, требованием о необходимости соответствия последующей обработки данных разумным ожиданиям субъекта. Так, в случае размещения субъектом своих персональных данных на интернет-ресурсе, субъект зачастую не рассчитывает, что его данные будут извлечены и воспроизведены на другом интернет-ресурсе. При отсутствии прямого закрепления в законе, необходимость соблюдения интересов субъекта находит отражение в разъяснениях уполномоченного органа по защите прав субъектов персональных данных. В частности, соответствующие разъяснения даны в отношении данных соискателей,

разместивших свое резюме в открытом доступе[14].Вместе с тем разъяснения Роскомнадзора сами по себе носят рекомендательный характер, а вышеприведенное разъяснение было дано регулятором применительно к конкретному случаю, и однозначного закрепления данная позиция на практике не получила.

24.В ФЗ о персональных данных однозначно не закреплено соотношение понятий «общедоступные источники персональных данных» (ст. 8) и «персональные данные, сделанные общедоступными субъектом персональных данных» (п. 10 ч. 1 ст. 6). В то же время имеются основания полагать, что с юридической точки зрения персональные данные, сделанные общедоступными, не сводятся к данным, включенным в общедоступные источники. Так, в законе явно разделяются понятия общедоступных данных и данных из общедоступного источника, что побуждает вообще считать ненужным термин «общедоступный источник персональных данных» и заменить его на термин «*справочный источник персональных данных*» как более адекватно отражающий суть указанного явления.

25.Применительно к понятию «*открытые данные*» уместно уточнить, что, несмотря на отмеченную в научной литературе важность данного института[15] и наличие большого числа относящихся к открытым данным нормативных правовых актов разного уровня, до настоящего времени сохраняется разрыв между функциональной открытостью ведомств (доступностью собираемых и генерируемых данных) и их информационной открытостью.[16]Ключевой проблемой обеспечения доступности открытых данных о деятельности органов государственной власти и местного самоуправления является *неэффективный механизм контроля за обеспечением такого доступа*.

26. Отдельным аспектом регулирования данных является их охрана в случае передачи их по сетям электросвязи (соблюдение *тайны связи*, гарантированной ст.23 Конституции Российской Федерации). Такая охрана традиционно рассматривается как составная часть системы основных прав и свобод человека, его правового статуса. В то же время в действующем законодательстве (в частности, в Федеральном законе «О связи»[17]) понятие «тайна связи» не раскрывается, равно как не имеется и однозначного представления, на какой круг субъектов должны распространяться соответствующие конституционные требования. Поскольку в

[14]Абз. 12 п. 5 разъяснений Роскомнадзора «Вопросы, касающиеся обработки персональных данных работников, соискателей на замещение вакантных должностей, а также лиц, находящихся в кадровом резерве» // СПС КонсультантПлюс.

[15] Савельев Д.А. О создании и перспективах использования корпуса текстов российских правовых актов как набора открытых данных // Право. Журнал Высшей школы экономики. 2018. № 1. С. 26-44.

[16] Оценка открытости государственных информационных систем в России. Аналитический доклад. - М., 2020. - С. 109-112.

[17] Федеральный закон «О связи» от 07.07.2003 г. № 126- ФЗ // СПС КонсультантПлюс; далее – «ФЗ о связи»

условиях цифровой экономики соблюдение режима конфиденциальности тех или иных видов данных требует однозначного понимания, какими методами и в каком объёме должна обеспечиваться их конфиденциальность, имеющиеся пробелы в правовом регулировании должны быть устранены. В частности, речь идёт об определении прав и обязанностей операторов связи и иных лиц, обязанных соблюдать тайну связи; о круге лиц, в отношении которых тайна связи должна соблюдаться; а также о правильной и единообразной квалификации сведений, составляющих тайну связи.

27.Большинство авторов, предпринимающих попытку дать определение понятия «тайна связи»[18], делают акцент на «личном» характере соответствующих сведений, а также на том, что институт тайны связи имеет своей целью защиту интересов граждан. На этом основании нередко делается вывод о том, что тайна связи не распространяется на коммуникации с участием юридических лиц, а также на переписку и переговоры делового (профессионального) характера. В современных условиях такие выводы должны рассматриваться как ошибочные. Несмотря на то, что правовой институт тайны связи исторически тесно связан с обеспечением права на неприкосновенность частной жизни, в действительности тайна связи имеет *самостоятельную сферу* правовой охраны. В частности, в Конституции Российской Федерации право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений отделено от права на неприкосновенность личной жизни. Законодательство об информации[19] также не разделяет субъектов, чья тайна связи подлежит защите, используя универсальный подход об охране тайны связи любых субъектов (физических, юридических лиц и публично-правовых субъектов).

28.Право на тайну связи является самостоятельным правом, имеющим собственное содержание, структуру, субъектно-объектный состав, механизмы и гарантии его реализации. Право на неприкосновенность частной жизни защищает информацию, определяемую *по содержательному* признаку, то есть информацию, которая характеризует обстоятельства, относящиеся к личности физического лица (например, *персональныеданные*, которые являются таковыми только в том случае, если они могут быть соотнесены с идентифицированным или идентифицируемым лицом). В свою очередь, тайна связи охватывает данные, которые определяются не по содержательному, а *по формальному* критерию: соответствующие данные

[18] Апанасенко С.С., Гладких Е.Л. Тайна телефонных переговоров в уголовном праве России. Ростовский научный журнал. Выпуск № 1. Январь 2019. С. 278 – 293; Рязанов Н.Ю. Эволюция права на тайну связи // Право и государство: теория и практика. 2015. № 8(128). С. 111 – 115.

[19] См., например, Федеральный закон «Об информации, информационных технологиях и о защите информации» № 149-ФЗ, далее – «ФЗ об информации»), также Федеральный закон «О связи» № 126-ФЗ.

должны иметь форму сообщений, которые находятся в состоянии передачи или уже были переданы по каналам связи. Данная логика в некоторой степени нарушается, когда речь заходит об охране тайной связи *метаданных* – информации, которая характеризует сообщения, но не раскрывает их содержание (например, информации об адресатах сообщений, времени их направления и т.д.). Однако такая информация охраняется тайной связи только в том случае, если она относится к упомянутым выше сообщениям, а сообщения, в свою очередь, все равно определяются по формальному критерию. Соответственно, формальный характер критерия, с использованием которого происходит выделение сведений, составляющих тайну связи, косвенно охватывает не только сами сообщения, но и их метаданные.

29. Описанное выше разделение наглядно иллюстрирует российское законодательство о связи, которое проводит различие между *сведениями об абоненте* и сведениями, *составляющими тайну связи*, о которых говорится в статьях 53 и 63 ФЗ о связи соответственно. Нормативные положения, посвященные охране сведений об абоненте, во многом дублируют положения законодательства о персональных данных, требуя от оператора связи обеспечить конфиденциальность сведений, позволяющих идентифицировать абонента или иным образом относящихся к нему. В свою очередь, нормы о тайне связи в принципе не содержат какой-либо привязки к характеру передаваемых сведений: ознакомление с корреспонденцией не допускается независимо от того, позволяет она идентифицировать абонента или нет.

30.С учетом вышеизложенного тайна связи может быть охарактеризована как режим конфиденциальности, который применяется к любым сведениям, передаваемым или переданным в составе переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, а также к информации о таких сообщениях. В рамках такого подхода можно констатировать, что тайна связи защищает не только частную переписку, но и *коммуникации, связанные с профессиональной деятельностью*. Неслучайно значительное место в отечественной и зарубежной судебной практике занимают споры, связанные с соблюдением права на тайну корреспонденции в отношении рабочих коммуникаций. Также в настоящее время отсутствуют основания для исключения из сферы правовой охраны сообщений, передаваемых юридическими лицами или иными корпоративными структурами. Такой подход характерен как для отечественного правопорядка, так и для зарубежных юрисдикций.

31.При оценке содержания тайны связи доминирует широкий подход, согласно которому тайной связи охватывается не только содержание осуществляемых коммуникаций, но и сам факт таких коммуникаций и связанные с ними сведения, которые получили в законодательстве

наименование «информация о соединениях» [20]. Вместе с тем такой подход подвергается критике со стороны отдельных ученых ввиду расширительного толкования тайны связи и необоснованного распространения режима тайны связи на сведения о соединениях[21]. Также в науке ставится под сомнение целесообразность отнесения технических идентификаторов абонентского оборудования к тайне связи, основывая свою позицию на существенно меньшей ценности такой информации для абонента в сравнении с содержанием коммуникаций[22].

32.ФЗ об информациив статье 9 закрепляет, что условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение устанавливаются федеральными законами. В 2014 г. он был дополнен рядом статей, регулирующих деятельность организаторов распространения информации в сети «Интернет». Согласно ст. 10.1 ФЗ об информации под организатором распространения информации в Интернете понимается лицо, осуществляющее деятельность по обеспечению функционирования информационных систем и (или) программ для электронных вычислительных машин, которые предназначены и (или) используются для приема, передачи, доставки и (или) обработки электронных сообщений пользователей Интернета. При этом законодатель выделил специальную категорию организаторов распространения информации – организаторов сервиса обмена мгновенными сообщениями, квалифицирующим признаком которой является использование для обмена электронными сообщениями исключительно между пользователями этих информационных систем и (или) программ для электронных вычислительных машин, при котором отправитель электронного сообщения определяет получателя или получателей электронного сообщения, не предусматриваются размещение пользователями Интернета общедоступной информации в сети «Интернет» и передача электронных сообщений неопределенному кругу лиц. Таким образом, под определение организатора сервиса обмена мгновенными сообщениями попали социальные сети, мессенджеры. Сервисы электронной почты не имеют указанного признака и поэтому относятся к «обычным» организаторам распространения информации в интернете. Данное разграничение организаторов распространения информации в сети «Интернет» важно отметить, поскольку для

[20] Терещенко Л.К. Отдельные вопросы, возникающие в судебной практике при применении норм о тайне связи // Комментарий судебной практики / отв. ред. К.Б. Ярошенко. М.: Институт законодательства и сравнительного правоведения при Правительстве РФ, ИНФРА-М, 2016. Вып. 21. С. 145 – 153.

[21]Чечетин А. Ограничение тайны связи // Законность. 2005. № 7. С. 40; Богдановский А. Может ли ошибаться Конституционный суд? // Законность. 2006. № 8. С. 34.

[22]Рего А.В., Мацкевич А.Ю. Проблема доступа антимонопольных органов к тайне связи // Российское конкурентное право и экономика. 2019. № 3. С. 18.

организатора сервиса это влечет разный объем обязанностей.

33.Вместе с тем, в законодательстве России не содержится формализованного определения тайны связи либо критериев, которые позволили бы определить ее границы. Это, в свою очередь, приводит к различному толкованию содержания тайны связи и разночтениям при отнесении тех или иных сведений к такой тайне. Дополнительная сложность возникает ввиду того, что одни и те же данные могут подпадать под различные правовые режимы. Так, сведения о личной жизни лица могут охраняться как личная и семейная тайна. В то же время, такие сведения, передаваемые в сообщении по каналам электросвязи, становятся тайной связи.

34.В контексте перспективного регулирования следует обратить внимание на возможность обработки сведений, составляющих тайну связи, как в форме, доступной для интерпретации человеком, так и *в машиночитаемой* форме. Представляется, что обработка сведений, составляющих тайну связи, исключительно в машиночитаемом формате без участия человека сопряжено с меньшими рисками для конфиденциальности абонентов (пользователей), что должно быть учтено в нормативном регулировании.

35.Определённое развитие регулирование данных наблюдается в *подзаконных* нормативных правовых актах, таких как Указ Президента РФ «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы»[23], где установлено, что главным способом обеспечения эффективности цифровой экономики становится внедрение технологии обработки данных, что позволит уменьшить затраты при производстве товаров и оказании услуг; Постановление Правительства РФ № 573 (2013 г.)[24] № 583, закрепляющее правила квалификации информации, размещаемой государственными органами в форме открытых данных, в качестве общедоступной; Постановление Правительства РФ от № 676 (2015 г.) [25], определяющее требования к порядку создания и эксплуатации государственных информационных систем и содержащихся в их базах данных информации. Значительное число подзаконных актов регламентирует порядок работы с персональными данными и устанавливает различные требования в сфере информационной безопасности.

36.Важным представляется недавно принятый Федеральный закон «О едином федеральном информационном регистре, содержащем сведения о населении Российской

[23] Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы»

[24] Постановление Правительства РФ от 10.07.2013 № 583 «Об обеспечении доступа к общедоступной информации о деятельности государственных органов и органов местного самоуправления в информационно-телекоммуникационной сети «Интернет» в форме открытых данных».

[25] Постановление Правительства РФ от 06.07.2015 № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации».

Федерации»[26], предусматривающий, в частности, регулирование на уровне Правительства РФ порядка формирования записей федерального регистра сведений о населении и внесения в них изменений.

37.Регулирование данных на уровне *субъектов РФ* в большинстве случаев носит фрагментарный характер, и в основном относится к вопросам создания региональных информационных систем. Как правило, региональные законодатели делегируют право регламентации региональных информационных систем исполнительным органам государственной власти субъектов РФ[27]. Однако особого внимания заслуживают законодательные акты г. Москвы, в силу своего многообразия, актуальности (принятия в условиях коронавирусной инфекции 2020 года) и уникальности – аналогичных норм не существует в подавляющем большинстве иных субъектов РФ. Именно на уровне города Москвы предусматривается и значительный массив регулирования, обозначенный специальным федеральным законом, который регламентирует условия проведения эксперимента по установлению правового режима, связанного с разработкой и внедрением технологий искусственного интеллекта[28].

38.Отдельные вопросы регулирования данных находят отражение *также в судебной практике*. Хотя по делам, связанным с регулированием данных (и информации в целом), она также не является однозначной с точки зрения единообразного трактования данных и заполнения пробелов в законодательном регулировании. Например, Конституционным судом было решено, что под распространением религиозной литературы и материалов религиозного назначения в рамках миссионерской деятельности следует понимать не только вручение данных материалов конкретным лицам, но и обеспечение свободного доступа к этой литературе и материалам неопределенного круга лиц[29]. Был также сделан вывод, что общедоступные данные – это те данные, которые можно использовать без разрешения их обладателя.

---

[26]Федеральный закон от 08.06.2020 N 168-ФЗ "О едином федеральном информационном регистре, содержащем сведения о населении Российской Федерации" // СЗ РФ, 15.06.2020, N 24, ст. 3742.

[27] См., например, Областной закон Ленинградской области от 18.07.2016 № 60-оз (ред. от 15.04.2019) «О государственных информационных системах Ленинградской области» (принят 29.06.2016), Закон Санкт-Петербурга от 07.07.2009 № 371-70 (ред. от 29.11.2013) «О государственных информационных системах Санкт-Петербурга».

[28] Федеральный закон от 24.04.2020 № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации - городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных».

[29] Определение Конституционного Суда РФ от 07.12.2017 N 2793-О "Об отказе в принятии к рассмотрению жалобы религиозной организации "Религиозная христианская организация "Армия спасения" в городе Владивостоке" на нарушение конституционных прав и свобод пунктом 3 статьи 17 Федерального закона "О свободе совести и о

39. Знаковой для регулирования отношений в области тайны связи была попытка Конституционного Суда Российской Федерации в 2003 г.[30] дать определение содержанию тайны связи, отсутствующему в действующем законодательстве: «Право каждого на тайну телефонных переговоров по своему конституционно-правовому смыслу предполагает комплекс действий по защите информации, получаемой по каналам телефонной связи, независимо от времени поступления, степени полноты и содержания сведений, фиксируемых на отдельных этапах ее осуществления. В силу этого информацией, составляющей охраняемую Конституцией Российской Федерации и действующими на территории Российской Федерации законами тайну телефонных переговоров, считаются любые сведения, передаваемые, сохраняемые и устанавливаемые с помощью телефонной аппаратуры, включая данные о входящих и исходящих сигналах соединения телефонных аппаратов конкретных пользователей связи; для доступа к указанным сведениям органам, осуществляющим оперативно-розыскную деятельность, необходимо получение судебного решения. Иное означало бы несоблюдение требования статьи 23 (часть 2) Конституции Российской Федерации о возможности ограничения права на тайну телефонных переговоров только на основании судебного решения».

40.Данное разъяснение корреспондирует закрепленной в п. 3 ст. 55 Конституции РФ норме, согласно которой права и свободы человека и гражданина могут быть ограничены федеральным законом только в той мере, в какой это необходимо для целей защиты конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. Следует отметить, что Конституционный суд Российской Федерации в Определении анализировал Федеральный закон от 16.02.1995 № 15-ФЗ «О связи»[31] (далее – ФЗ о связи 1995 г.), который утратил силу с 01 января 2004 года. Его заменил действующий ФЗ о связи, содержащий в себе схожие, но не полностью аналогичные нормы ФЗ о связи 1995 г. В то время как ст. 32 ФЗ о связи 1995 г. (комментируемая КС РФ) содержала в себе достаточно лаконичную формулировку, согласно которой «прослушивание телефонных переговоров, ознакомление с сообщениями электросвязи, задержка, осмотр и выемка почтовых отправлений и документальной корреспонденции, получение сведений о них, а также иные ограничения тайны связи допускаются только на основании судебного решения», действующий ФЗ о связи подходит к данному вопросу

религиозных объединениях" и частью 3 статьи 5.26 Кодекса Российской Федерации об административных правонарушениях"

[30] Определение Конституционного Суда РФ от 02.10.2003 № 345-О «Об отказе в принятии к рассмотрению запроса Советского районного суда города Липецка о проверке конституционности части четвертой статьи 32 Федерального закона от 16 февраля 1995 года «О связи».

[31] Федеральный закон от 16.02.1995 № 15-ФЗ «О связи» // СПС «КонсультантПлюс».

несколько иначе, проводя достаточно четкое разграничение между правом на свободу как таковым в ст. 63 и случаях ее ограничения в виде возложения на операторов связи обязанности в определенных случаях предоставлять информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, текстовых сообщений, изображений, звуков, видео- или иных сообщений пользователей услугами связи.

41.Можно сделать вывод, что Конституционный суд РФ дает расширительное по сравнению с действующим законодательством толкование понятию тайны связи, поскольку, согласно его разъяснениям, получение любой информации, связанной с оказанием услуг связи, поставлено в зависимость от наличия судебной санкции. Действующий ФЗ о связи, к тому же, «получение сведений об услугах связи» не относит к охраняемой Конституцией РФ тайне связи.

42.Таким образом, нормативный массив российского законодательства об информации, обороте данных, общедоступных данных и тайне связи нуждается в достаточно *срочном обновлении*. Это связано с необходимостью как приведения его в соответствие с текстом внесённых изменений в российскую Конституцию, так и ликвидации правовой неопределённости в регулировании возникающих общественных отношений, связанных с новейшими (цифровыми) технологиями. Одним из выходов могла бы стать кодификация всего комплекса «информационных» законодательных актов, однако все попытки создания *Информационного кодекса* до настоящего момента были безуспешными. Возможна разработка не Кодекса, а *Основ информационного законодательства*, которые включали бы базовые положения, понятийный аппарат и принципы регулирования в сфере информации и оборота данных.

Понятие «данных» в зарубежных юрисдикциях

43.Безусловный интерес для определения приоритетных направлений развития российского законотворчества в сфере данных (и, в честности, цифровых данных) представляет *зарубежный опыт*. Следует, однако, отметить, что ни на уровне международно-правовых актов, ни в зарубежных правовых системах (как, собственно, и в российских законах до 2020 года) понятие «*цифровые данные*» не используется вообще, а в конвенциональных документах, составляющих основу международного информационного права, не используется и понятие «данные», определяя как базовое понятие только «*сообщение*» или «*сообщение электросвязи*». В то же время в актах Международной организации по стандартизации (ISO)[32] и

[32] ISO/IEC 2382:2015 Information technology — Vocabulary. URL: https://www.iso.org/standard/63598.html

межгосударственных стандартах[33] содержится определение данных, ставшее де-факто общепринятым: «*предоставление информации в формальном виде, пригодном для передачи, интерпретации или обработки людьми или компьютерами*».

44.Самостоятельное международно-правовое регулирование имеет институт *персональных данных*, который в значительной степени основан на нормах Конвенции Совета Европы о защите прав физических лиц при автоматизированной обработке персональных данных[34] (на принципах которой основан и российский ФЗ о персональных данных). Важнейшим документом Европейского Союза, устанавливающим принципы работы с персональными данными, является вступивший в 2018 году в силу Общий регламент защиты данных (GDPR)[35], который распространяется на все организации, которые осуществляют свою деятельность в ЕС, а также на те организации, которые не присутствуют на его территории, но их деятельность по обработке направлена на лиц, находящихся на территории Евросоюза. В целом для всех компаний и организаций, которые занимаются обработкой персональных данных, установлено два принципа, определяющих подходы к системному проектированию:

- *проектируемая* конфиденциальность (*protectionbydesign)* на начальном этапе работы с персональными данными компания должна установить такой уровень технических и организационных мер, который бы не позволил нарушить принципы защиты данных;

- конфиденциальность *по умолчанию* (*protectionbydefault*) – подразумевается, что компании обеспечивают такой уровень защиты, который делает невозможным доступ к персональным данным третьих лиц.

45.Ещё одним документом, регулирующим данные в ЕС, является Регламент по регулированию свободного потока данных[36], предметом регулирования которого являются любые данные, которые не отнесены к персональным (*non-personal - dataotherthanpersonaldata).* Такие данные не подпадают под определение персональных данных согласно GDPR, также с помощью таких данных невозможно идентифицировать физическое лицо. Основной идеей принятия документа является создание новых правил и принципов, отменяющих препятствия

---

[33] ГОСТ 33707-2016 (ISO/IEC 2382:2015) Информационные технологии (ИТ). Словарь. URL: http://docs.cntd.ru/document/1200139532

[34] Convention 108 + Convention for the protection of individuals with regard to the processing of personal data. - URL: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1)

[35]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation); далее – «GDPR».

[36] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1807

развития цифровой экономики. Так, по общему правилу, согласно Регламенту: запрещается осуществлять локализацию неперсональных данных; государственные органы могут иметь доступ к неперсональной информации для осуществления функций контроля и надзора; провайдерам рекомендуется создавать кодексы саморегулирования, основанные на лучших практиках для поставщиков облачных услуг и облегчения смены таких поставщиков. Однако это не означает, что неперсональные данные перемещаются абсолютно свободно и неконтролируемо, поскольку требования к локализации таких данных могут быть установлены как на уровне национального законодательства государства-члена, так и на законодательном уровне Европейского Союза. Такие требования могут быть вызваны соображениями безопасности, а сами ограничения по локализации могут быть определены как через требование осуществлять хранение данных только в пределах определенного государства, так и через требование к оборудованию, предназначенному для обработки неперсональных данных (например, обязанность применения только сертифицированного оборудования определенного государства-члена). Неперсональные данные, в свою очередь, можно классифицировать по происхождению следующим образом:

- данные, по которым *нельзя идентифицировать личность* (например, данные о погодных условиях, генерируемые датчиками, установленными на ветряных турбинах);
- данные, которые являлись ранее персональными данными, но впоследствии были обезличены (*анонимизированы*).

46.Важным принципом работы с данными в Евросоюзе является*интероперабельность*. Отдельный Регламент устанавливает интероперабельность данных в информационных системах разных государств-членов ЕС[37]. Основной целью регламентации процесса интероперабельностиданных является создание «цифрового правительства», то есть возможности *получения электронных услуг разного вида*. Директива по регулированию свободного потока данных под *открытыми данными* понимает данные открытого формата, которые могут использоваться свободно, повторно и совместно любым человеком для любых целей.

47.Законодательство стран – членов Европейского Союза (а также вышедшей из него Великобритании) в области информации и данных основывается на актах прямого действия

[37]Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0817).

европейского законодательства. В них, как правило, действуют законы о защите персональных данных, полностью соответствующие GDPR, либо имеющие отсылки к этому регламенту. При этом собственно данные и персональные данные рассматриваются как две самостоятельные категории, каждая из которых обладает определённой совокупностью признаков. Например, в соответствии со статьей 3 Закона Великобритании «О защите данных» данные представляют собой «информацию, которая обрабатывается и записывается с помощью автоматизированного оборудования и является частью соответствующей системы или же записью, находящейся в распоряжении государственного органа». В свою очередь персональные данные являются «любыми данными, относящимися к живому человеку, на основании которых этот человек может быть идентифицирован». Персональные данные также представляют собой информацию, которая включает в себя любое выражение мнения об индивидуальных особенностях человека или его личности, и которая находится в распоряжении *контролера данных* (аналог в российском законодательстве – «*оператор персональных данных*») или может поступать ему для обработки.

48.Информационное законодательство стран англосаксонской правовой традиции основывается на *законах о свободе информации*, закрепивших принцип обеспечения доступа к информации, накапливаемой и хранимой в государственных информационных системах соответствующих стран. Так, в США принятый в 1966 году Закон о свободе информации[38] устанавливает презумпцию, что вся информация, находящаяся в ведении государственных органов и департаментов, должна быть доступна гражданам США. В Законе нет определения понятий «информация» или «данные», однако существует перечень тех сведений, которые должны быть доступны населению. Вся информация, которая может быть запрошена, рассматривается как записи (*records*). Однако переход к концепции доступности информации, содержащей акты государственных органов власти, не отменяет ограничения доступа к определённой категории информации. К такой информации относят:

- конфиденциальную информацию, где речь идёт о закрытой информации персонала государственных органов, данных об их личной жизни,

- результаты деятельности правоохранительных органов, например, расследования по вопросам национальной безопасности.

49.Ещё одним актом, регулирующим деятельность по информационному обмену в США, является Закон о конфиденциальности,[39] который ставит своей целью обеспечение баланса

[38]The Freedom of Information Act (FOIA) URL: https://www.justice.gov/oip/freedom-information-act-5-usc-552
[39] https://www.justice.gov/opcl/privacy-act-1974

интересов между государственными нуждами в сборе информации и праве граждан на защиту своих персональных данных. Терминологически акт оперирует такими понятиями как *запись (record),* которая включает в себя любое сообщение либо набор информации о человеке (*aboutanindividual*), включая информацию о его образовании, финансовых операциях, медицинскую историю и другое. Данный перечень является открытым. Из таких записей формируется *система записей* (*system of records*), которая представляет собой группу записей, находящихся в ведении какого-либо государственного органа и из которой информация может быть извлечена по тем или иным критериям. В противовес записям, которые являются *идентификаторами*, то есть по сути персональными данными, существует категория статистическойзаписи (*statisticalrecord*), которая представляет собой информацию, используемую для статистических исследований. Статистические записи, как установлено в комментариях к закону, представляют собой категорию данных, по которым нельзя сделать вывод о предпочтениях или привилегиях конкретного лица, то есть идентифицировать. В Законе понятия «информации» (*information*) и «данные» (*data*) используются достаточно несистемно, при этом термин «данные» чаще используется в смысле как синоним письменных записей*(record*).

50.Аналогичным образом в Великобритании Закон о свободе информации 2000 года[40] регулирует порядок запрос информации у государственных органов, дает определение термину «набора данных» (*datasets*) («набор информации, хранящийся в электронной̆ форме»). Такой набор данных может представлять собой информацию, собранную и переданную для государственных целей, в том числе для принятия решений, либо набор фактических данных, не адаптированных, не агрегированных, то есть «*сырых* данных», в том числе нестатистических. Информация в таком «наборе данных» данных подлежит использованию определённым лицом для целей иных, чем те, что установлены в документе (*re-use*). При этом авторские права на набор данных принадлежат государственным органам, а для многократного использования данных государственный орган должен иметь лицензию на использование данных повторно. В основе Закона лежит также порядок взаимодействия с информацией, находящейся в ведении государственных органов власти, то есть данных, которые являются зафиксированной информацией, находящейся в ведении государственных органов власти и не подпадающих под категории персональных данных. Общедоступной записью (*publicrecord*) считают запись,

[40] Freedom of information Act 2000 URL: http://www.legislation.gov.uk/ukpga/2000/36/pdfs/ukpga_20000036_en.pdf)

сделанную государственным органом. Первоначально этот термин появился в английском законодательстве в 1958 году и означал запись актов гражданского состояния.

51.Таким образом, особенностью актов информационного законодательства многих зарубежных стран (США, Германия, Великобритания и др.) является регламентация такой правовой категории как *запись*. Фактически именно «записи» являются «минимальными единицами» регулирования информационных объектов, введёнными в национальное законодательство[41]. В Российской Федерации аналогичные правовые категории в федеральном законодательстве не легитимизированы, хотя также широко используются – запись актов гражданского состояния, запись в судовом (бортовом) журнале, запись в реестре акционеров и т.п.

52.Что касается стран так называемого *Ближнего зарубежья* (таких, как Казахстан и Беларусь), то их законодательные акты в сфере оборота информации и защиты данных в основном копируют принципы регулирования, установленные в российском законодательстве.

53.Отдельные вопросы регулирования данных рассматриваются в документах различных интеграционных объединений с участием Российской Федерации. Так, Положение о модели данных Евразийского экономического союза[42] содержит определения «*модель данных*» (представление юридических фактов (обстоятельств, действий или событий), связей между ними и их состояний в виде графического и (или) словесного описания, пригодное для передачи, интерпретации и обработки формализованным образом) и «*объект модели данных*» (составная часть модели данных, определяющая описание предмета, субъекта, обстоятельства, действия или события и (или) их состояний, в отношении которых осуществляется моделирование). Однако практическое внедрение указанных категорий в законодательство стран ЕАЭС еще только предстоит.

54.Применительно к *общедоступным данным* проведенный сравнительно-правовой анализ международно-правового и внутригосударственного законодательного регулирования позволил сформулировать следующие выводы:

---

[41]Аналогией в российском праве (но не в федеральных законах) также «запись», например, *запись актов гражданского состояния, запись в судовом (бортовом) журнале, запись в реестре акционеров* или *запись в домовой книге*. Эти категории представляют собой внесенные в официальном порядке сведения, которые порождают правовые последствия для лиц, к которым такая запись относится. Несмотря на то, то именно записи порождают совокупность («базу данных» или «массив данных») юридически значимых сведений, необходимая для этого регламентация в Российской Федерации отсутствует.

[42]Утверждено решением Коллегии Евразийской экономической комиссии от 26.12.2017 № 190, URL: http://www.consultant.ru/document/cons_doc_LAW_287170/).

- единой общемировой модели правового регулирования общедоступных данных в настоящее время не существует, формирование такого регулирования тесно связано с особенностями национальных правовых систем и наличием в них специального законодательства о персональных данных, которое может быть как основано на европейской модели регулирования персональных данных (Совет Европы, ЕС), так и предусматривать национальные особенности;

- европейская модель правового регулирования данных ограничивает свободную обработку общедоступных данных целями, для которых указанные данные были сделаны общедоступными, и носит в значительной мере императивный характер, снижая возможности для диспозитивного регулирования на договорной основе между субъектами соответствующих отношений, (в отличие от США, где данные вопросы рассматриваются в рамках соответствующих соглашений между субъектами отношений по обработке данных);

- «азиатская» модель регулирования, в том числе опыт Сингапура, показывает возможности для обеспечения баланса интересов субъектов персональных данных и лиц, осуществляющих обработку таких данных, путем конкретизации на законодательном уровне видов персональных данных, которые являются «*общедоступными по умолчанию*», а также предусматривает возможности снижения требований по обеспечению мер безопасности при обработке общедоступных данных

- в целом опыт стран ЕС, Канады (информационные комиссары) и азиатских стран (Япония) свидетельствует о необходимости изменения статуса уполномоченного органа, в том числе в части *возможности осуществления им оперативного подзаконного нормативного правового регулирования в сфере персональных данных, в том числе общедоступных и открытых государственных данных*;

- принцип «открытости по умолчанию» на практике реализуется только в отношении государственных данных и иных данных, созданных на основе бюджетных средств.

55.Наконец, в отношении *тайны связи* базовым международно-правовым документом следует признать Декларацию прав и свобод человека[43], в статье 12 которой устанавливается, что «никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произвольным посягательствам на неприкосновенность его жилища, тайну его корреспонденции или на его честь и репутацию. Каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств». В развитие Декларации принимались

[43] Всеобщая декларация прав человека (принята Генеральной Ассамблеей ООН 10.12.1948) URL: http://www.consultant.ru/document/cons_doc_LAW_120805/

многочисленные конвенциональные документы универсального (глобального) и регионального характера. Например, в упоминавшейся выше Конвенции Совета Европы № 108 регламентирован вопрос о защищённости персональных данных как составляющей тайны связи.

56. Зарубежное законодательство, аналогично российскому, допускает ограничение тайны в отношении определённых ситуаций или видов данных. Так, в федеральном законодательстве США широко используется согласие пользователя услугами связи для раскрытия данных о его коммуникациях любому лицу, им указанному. Операторы связи вправе использовать информацию о коммуникациях пользователей для целей предотвращения мошенничества, обрабатывать геолокационные данные в ситуациях, сопряжённых с угрозой жизни и здоровью. Также операторы связи вправе использовать информацию о коммуникациях пользователей для целей оказания маркетинговых услуг с согласия пользователей. При этом в законах многих стран, а также в судебной практике, отмечается правомерность перехвата работодателем электронных сообщений работников, если работодатель предварительно уведомил работников и получил согласие на это.

57. Проведённое исследование регулирования тайны связи в различных юрисдикциях позволяет сделать вывод, что в целом наблюдается общий подход к пониманию правового института тайны связи, а различия в регулировании на уровне актов национального законодательства не носят принципиального характера.

Выводы и рекомендации: как должно меняться законодательство о данных (включая вопросы регулирования общедоступных данных и тайны связи) в условиях цифровой экономики

58.Развитие «экономики данных» существенно осложняется неадекватностью относящегося к ней регулирования. К наиболее характерным проблемам в этой связи можно, в частности, отнести:

- отсутствие учета особенностей каждого вида охраняемой законом информации, и, как следствие, однотипная методика администрирования такой информации;

- низкие темпы обновления законодательной базы, необходимой для прорывного развития цифровой экономики;

- чрезмерная сложность разрешительных процедур при использовании данных, полученных с помощью современных технических средств[44].

[44] например, кадастровая палата Росреестра не принимает к регистрации планы межевания участков, подготовленные по данным аэрофотосъемки. Этому препятствует утвержденная в 1980 году инструкция по

59.К сожалению, серьёзные теоретические разработки, на которые можно было бы опираться при разработке правового регулирования в сфере данных, пока еще отсутствуют (за редким исключением). Эффективное правовое регулирование данных невозможно обеспечить без создания обновленного *адекватного понятийного аппарата*, в первую очередь, необходимо разведение понятий «информация» и «данные». С учётом последних изменений в Конституции РФ направления развития законодательства должны носить как юридико-технический характер – в сторону унификации, гармонизации регулирования, устранения выявленных коллизий, так и содержательный – в сторону регулирования оборота цифровых данных с учётом законных интересов всех субъектов.

60.Законодательство должно обеспечивать *баланс интересов* граждан, бизнеса и государства при регулировании оборота данных, имея в виду первоочередным решение вопросов безопасности указанных субъектов при обороте *цифровых данных*. Категория баланса интересов является важной и в практике Конституционного Суда РФ, который использует ее в более чем 1000 постановлений и определений. В сфере информационных отношений это связано с оценкой конституционности законодательства о государственной тайне[45], банковской тайне,[46] и др. Общие подходы к определению баланса интересов в практике Конституционного Суда РФ аналогичны применяемым Европейским судом по правам человека. В частности, в Определении Конституционного Суда РФ от 14.12.2004 N 453-О указано, что «закрепление в законе *отступлений от банковской тайны*– исходя из конституционного принципа демократического правового государства, обязанности государства соблюдать и защищать права и свободы человека и гражданина как высшую ценность и обеспечивать их баланс в законодательстве и правоприменении, верховенства Конституции РФ и ее высшей юридической силы, свободы экономической деятельности и свободного предпринимательства –*не может быть произвольн*ым; такие отступления (в частности, предоставление банками, иными кредитными организациями и их служащими сведений о счетах и вкладах и операциях по счету, а также сведений о клиентах государственным органам и их должностным лицам) *должны*

аэрофотосъемке, где, в частности, предписано использование плёночных фотокамер и есть множество других ограничений, неактуальных для современных беспилотных устройств

[45]Постановление Конституционного Суда РФ от 07.06.2012 N 14-П по делу о проверке конституционности положений подпункта 1 статьи 15 Федерального закона "О порядке выезда из Российской Федерации и въезда в Российскую Федерацию" и статьи 24 Закона Российской Федерации "О государственной тайне" в связи с жалобой гражданина А.Н. Ильченко // Справочная правовая система «Консультант Плюс».)

[46]Определение Конституционного Суда РФ от 14.12.2004 N 453-О "Об отказе в принятии к рассмотрению жалобы открытого акционерного общества "Акционерный коммерческий банк "Энергобанк" на нарушение конституционных прав и свобод абзацем первым пункта 3 статьи 7 Закона Российской Федерации "О налоговых органах Российской Федерации", пунктом 2 статьи 86 и пунктом 1 статьи 135.1 Налогового кодекса Российской Федерации" // Справочная правовая система «Консультант Плюс».)

отвечать требованиям справедливости, быть адекватными, соразмерными и необходимыми для защиты конституционно значимых ценностей, в том числе частных и публичных прав и интересов граждан, не затрагивать существо соответствующих конституционных прав, т.е. не ограничивать пределы и применение основного содержания закрепляющих эти права конституционных положений, и могут быть оправданы лишь необходимостью обеспечения указанных в статье 55 (часть 3) Конституции РФ целей защиты основ конституционного строя Российской Федерации, нравственности, здоровья, прав и законных интересов других лиц и общественной безопасности»[47].

61.Инструментами обеспечения баланса интересов в рамках правового регулирования данных и их оборота выступают процедуры оценки регулирующего[48] и фактического воздействия и мониторинга правоприменения, в рамках которых возможно внедрение специализированной оценки воздействия правового регулирования на развитие цифровых технологий[4950], которая будет обеспечивать выявление и балансировку интересов всех субъектов отношений в рамках нормотворчества и последующей оценки (мониторинга) действующего правового регулирования.

62.В рамках правоприменения интересы личности, общества и государства и обеспечение их баланса может оцениваться в ходе мониторинга правоприменения, а также в рамках судебной практики. При этом целесообразно отразить следующие группы интересов:

- *интересы личности в сфере правового режима данных и их оборота* (наличие качественных и доступных цифровых сервисов на основе данных; обеспечение защиты персональных данных, сведений, составляющих различные виды тайн (личную, семейную, банковскую, налоговую, медицинскую и т.д.); защита от информационного воздействия, в том числе рекламы, созданной на основе анализа данных о поведении конкретного человека);

-*интересы бизнеса в сфере правового режима данных и их оборота* (извлечение прибыли за счет развития оборота данных, цифровых сервисов (продуктов), созданных на их основе; устранение правовых и организационных (административных) барьеров, связанных с обработкой данных; снижение издержек, связанных с исполнением установленных нормативными правовыми актами требований в сфере защиты данных; обеспечение защиты

[47]Постановление Конституционного Суда Российской Федерации от 14 мая 2003 года N 8-П по делу о проверке конституционности пункта 2 статьи 14 Федерального закона "О судебных приставах")

[48] Татаринова О.В. Институт оценки регулирующего воздействия как инструмент реализации баланса частного и публичного интереса (анализ правоприменительной практики) // Власть Закона. 2018. № 1 (33). С. 278-287.

[49] Ефремов А.А. Оценка воздействия правового регулирования на развитие информационных технологий: механизмы и методика // Закон. 2018. № 3. С. 45-56.

[50] Ефремов А.А. Оценка воздействия правового регулирования на развитие информационных технологий: зарубежный опыт и российские подходы к методике // Информационное право. – 2018. – № 4. – с. 29-32.

сведений, составляющих коммерческую тайну; обеспечение свободного доступа к открытым данным органов государственной власти и местного самоуправления);

- *интересы общества в сфере правового режима данных и их оборота* (обеспечение свободного доступа к открытым данных органов государственной власти и местного самоуправления; защита детей от информации, пропаганды и агитации, наносящих вред его здоровью, нравственному и духовному развитию, в том числе от ненадлежащей рекламы, пропаганды насилия и жестокости, порнографии, наркомании,токсикомании, антиобщественного поведения);

- *интересы государства в сфере правового режима данных и их оборота* (обеспечение информационной безопасности государства, в том числе защиты сведений, составляющих государственную тайну; развитие национального рынка данных и технологий обработки данных, их конкурентоспособности и экспортного потенциала; повышение привлекательности российской юрисдикции для развития рынка данных и технологий обработки данных).

63.Необходимо более четкое разграничение *различных категорий* данных с определением (корректировкой) особенностей их правового режима, а также различных *субъектов правоотношений*, связанных с оборотом данных. В частности, такое разграничение может основываться на критериях (а) кто является обладателем данных, (б) относятся ли данные к какому-либо охраняемому законом виду тайн, (в) если в составе данных персональные данные.

64.*Новые виды данных* характеризуются своим многообразием, вместе с тем пока отсутствует необходимость их всеобъемлющего и детального регулирования. При выработке возможных моделей необходимо в первую очередь придерживаться принципа *минимизации регулирования*. Так, применительно к правовой категории «*больших данных*» следует предельно аккуратно выбирать наиболее целесообразное регулирование деятельности лиц, участвующих в их обработке, включая определение их правового статуса (как «операторов больших данных»), прав и обязанностей, порядка обезличивания таких данных и соблюдения иных законных интересов лиц, чьи данные предполагается обрабатывать. Не исключено, что в кратко- и среднесрочной перспективе можно было бы ограничиться использованием механизмов саморегулирования и уже существующих в законодательстве требований по обезличиванию (анонимизации) персональных данных в установленных случаях.

65.Юридическое значение обезличивания персональных данных заключается в двух аспектах. Во-первых, обезличивание относится к мерам защиты персональных данных при их обработке. Во-вторых, обезличивание влияет на условия обработки персональных данных. Так,

обезличивание является условием обработки персональных данных без согласия субъекта в статистических или иных исследовательских целях (п. 9 ч. 1 ст. 6 ФЗ о персональных данных). Необходимо учитывать, что окончательно (*необратимо*) обезличенные данные, выведенные из-под регулирования, – это категория не статичная, она зависит от технологического контекста и других объективных условий. Представляется возможным разработать обязательные минимальные критерии обезличенных данных и базовую методику их обезличивания, без соблюдения которых данные не могут быть признаны обезличенными. Каждый оператор, намеревающийся обрабатывать обезличенные данные, должен использовать свои критерии и методику обезличивания (не ниже обязательных минимальных требований) с учетом конкретных рисков соотнесения этих данных с физическим лицом. Помимо этого, в законодательство необходимо ввести понятие *необратимого* обезличивания данных и приравнять необратимое обезличивание персональных данных к их уничтожению (с закономерным выведением необратимо обезличенных данных из-под требований законодательства о персональных данных).

66.Одной из тенденций развития правового регулирования в сфере *персональных данных* является признание права на *переносимость* персональных данных (*righttodataportability*), которое уже получило закрепление в GDRP[51]. Переносимость данных подразумевает возможность переносить и повторно использовать информацию из одних приложений и информационных систем в другие, тем самым способствовать свободному обмену данными и не допускать «запирания» (*lock-in*) информации в автономных, изолированных системах. Несмотря на очевидную пользу переносимости данных в контексте защиты прав субъектов персональных данных и обеспечения конкуренции на цифровых рынках, практическая реализация этого принципа связана со значительными сложностями организационного, технического характера и издержками операторов персональных данных.

67.В целом система защиты прав субъектов персональных данных в рамках адаптации к условиям цифровой экономики должна развиваться по следующим направлениям:

- изменение требований к согласию на обработку персональных данных в сторону большей гибкости моделей согласия для обеспечения баланса между автономией воли субъектов персональных данных и публичными интересами, интересами третьих лиц;

[51] Статья 20 GDPR устанавливает, что субъект персональных данных имеет право получать свои персональные данные, которые он направил оператору, в структурированном, широко используемом и машиночитаемом формате, а также имеет право беспрепятственно переносить эти данные от одного оператора к другому. При этом если существует соответствующая техническая возможность, перенесение персональных данных должно осуществляться напрямую от одного оператора к другому.

- увеличение роли организационно-технических средств защиты информации, развитие инструментов «мягкого» права и саморегулирования операторов по вопросам защиты персональных данных;

- оптимизация института юридической ответственности за нарушения в сфере персональных данных с целью усиления превентивной (профилактической) функции;

- обеспечение прозрачности и доверия граждан к алгоритмам обработки данных, защита интересов субъектов персональных данных от дискриминации в процессе принятия автоматизированных решений.

68.Среди появившихся сравнительно недавно объектов регулирования можно отметить отсутствующее в российском праве понятие *геолокационных данных*. Геолокация осуществляется в нескольких направлениях: позиционирование (фиксирование местонахождения объекта), геокодирование (присвоение географических координат определенным объектам на карте), геотеггинг (присоединение геоданных к метаданным фотографии или страницы сайта в интернете)[52]. Как и с «большими данными», основная проблематика геолокационных данных связана с их соотношением с законодательством о персональных данных. Так, косвенная идентификация предполагает возможность отнесения к персональным данным информации, которая сама по себе хотя и не указывает однозначно на имя конкретного лица, но содержит описание каких-либо его индивидуальных характеристик, позволяющих отграничить его от других субъектов, выделить из круга лиц, к которому он принадлежит, или по крайней мере сузить такой круг лиц. При наличии иных идентификаторов у оператора геолокационные данные должны признаваться носящими значительный идентифицирующий потенциал, а следовательно, попадающими под сферу действия законодательства о персональных данных.

69.Далее, необходимо упомянуть как новый объект права так называемый *цифровой след*, который можно определить как совокупность данных о «*действиях пользователя в цифровом пространстве*»[53]. Указанное понятие было предложено делить на две категории: «активный» и «пассивный». К первой относится информация, которую пользователь оставляет в социальных сетях и личных кабинетах на сайтах, включая портал госуслуг и банковские ресурсы. К ней относятся, например, Ф.И.О., дата рождения, контактная информация, место работы, личные фото и видео. Пассивный след — это данные, которые оставляются ненамеренно или вследствие

[52] Щербакова Е.В. Использования геолокационных данных в сфере электронной коммерции // E-commerce и взаимосвязанные области (правовое регулирование): Сборник статей / Рук. авт. кол. и отв. ред. д.ю.н. М.А. Рожкова. М.: Статут, 2019. С. 114-130.

[53]URL: https://pro.rbc.ru/demo/5d6d2d529a7947132a5e721)

работы соответствующего программного обеспечения, в частности, это данные, которые собирает операционная система устройства пользователя или поисковая программа, которыми пользуется человек. Представляется, что необходимость регулирования самого по себе «цифрового следа» пока преждевременна в силу наличия законодательства о персональных данных, регулирующих соответствующие отношения.

70.Особое экономическое значение имеет правовая регламентация условий включения данных в хозяйственный оборот, включая требования к порядку заключения и содержанию *гражданско-правовых сделок с данными*. В действующем гражданском законодательстве и «базовом» ФЗ об информации такая регламентация отсутствует, упоминаются лишь особенности договора о возмездном оказании (информационных) услуг и более подробно описываются лицензионные процедуры передачи правообладателем объектов интеллектуальной собственности. В то время как суть данных как объекта, имеющего потребительскую стоимость, не может лишь сводиться к форме организации их совокупности (баз данных), подлежащей охране по аналогии с литературными произведениями. Дополнительно следует рассмотреть допустимость включения данных (и иных информационных объектов) в гражданско-правовой оборот на основании договоров коммерческой концессии, а также уступки (цессии) прав обладателя информации по смыслу ст.2 ФЗ об информации.

71.При этом следует учитывать, что информация является объектом не только гражданско-правовых, но и *публично-правовых* отношений (не связанных напрямую с созданием добавленной стоимости), и не вся информация может являться предметом *свободного* оборота. Существует ряд ограничений, установленных для защиты прав человек (персональные данные передаются и обрабатываются только после наличия твёрдо выраженного и объективно данного согласия), запрещён оборот информационных продуктов, где содержится информация, ограниченная в доступе или несущая в себе негативные последствия распространения (информация антиобщественного характера).

72.В условиях цифровой экономики институт *государственных (муниципальных) информационных систем* должен развиваться в направлении интеграции с иными информационными системами, в которых обрабатываются данные, имеющие общественное значение. Для этих целей предлагается в дополнение к ГИС и МИС предусмотреть институт публичных информационных систем, которые будут объединять ГИС, МИС и иные общественно значимые информационные системы в единую экосистему, построенную на принципах интероперабельности и единых стандартах информационного взаимодействия. Данные, обрабатываемые в публичных информационных системах, должны соответствовать

требованиям полноты, точности, достоверности, актуальности и непротиворечивости, при этом любые отклонения от указанных требований должны иметь объективные основания и понятны пользователям данных, для чего на операторов/поставщиков данных должны быть возложены обязанности по обеспечению прозрачности сбора и обработки данных.

73.В отношении информации, на основании которой принимаются юридически значимые решения (оказываются государственные и муниципальные услуги), целесообразно закрепить статус так называемых *эталонных данных* (данных, имеющих преобладающее, первичное, эталонное значение) и возложить на операторов информационных систем, в которых обрабатываются «эталонные данные», обязанности по обеспечению полноты, точности, достоверности, актуальности таких данных и по мониторингу иных публичных информационных систем на предмет содержания в них аналогичных данных, выявлению противоречий и их устранению через каналы межоператорского взаимодействия. Закрепление правового режима «эталонных данных» является необходимым условием эффективной реализации реестровой модели оказания государственных и муниципальных услуг.

74.Резюмируя вышесказанное, первоочередные меры в сфере развития общих норм законодательства о данныхдолжны быть направлены на:

- унификацию и согласование юридической терминологии, используемой для регулирования информационных отношений в различных законодательных актах;

- устранение коллизий между различными правовыми режимами информации (между правовым режимом персональных данных и профессиональными тайнами, государственной тайной и информацией служебного характера и др.)

- усиление «цифровой» составляющей информационного законодательства, закрепление правового режима «цифровых данных», учёт особенностей обработки данных современными информационными технологиями («большие данные», машинное обучение) и защита законных интересов субъектов правоотношений при такой обработке (интересов личности при автоматизированной обработке данных, интересов общества и государства в части обеспечения информационной открытости, коммерческих интересов – в части защиты конфиденциальных сведений и охране интересов инвесторов в цифровую экономику);

- адаптацию традиционных правовых режимов информации к условиям цифровой среды (необходим пересмотр старой парадигмы оборота данных с учетом современных технологических реалий в части защиты информации, составляющей коммерческую, государственную тайну и др.).

75.Применительно к унификации терминологического аппарата, целесообразно в статье 2 ФЗ об информации исключить слово «данные», переформулировав определение понятия «информация» следующим образом: «*информация – сведения (сообщения) о ком-либо или о чём-либо, независимо от формы представления*».

76.Необходимо также (в ФЗ об информации) дать легальное определение понятию «записи», которое в наиболее точной редакции могло бы звучать как *юридически значимые сведения, внесённые (созданные, сохранённые) уполномоченным лицом в информационной системе или иным установленным законодательством образом*». Такое определение позволит однозначно понимать «запись» не только в электронной форме (в информационной системе), но и в иных форматах, таких как «запись актов гражданского состояния», «запись в судовом журнале», «запись в реестре акционеров» и т.п.

77.В свою очередь, рассмотрение записей в информационных системах позволит понимать таковые как *цифровые данные* без необходимости давать определение данным «вообще», поскольку сложилось общепринятое понимание данных как информации в виде, пригодном для передачи, связи или обработки как человеком, так и автоматическими средствами. При этом было бы разумным уточнить определение информационной системы как «*совокупность записей (цифровых данных), содержащихся в базах данных и обеспечивающих их обработку информационных технологий и технических средств*».

78.Применительно к совершенствованию регулирования общедоступных данных предложено «точечные изменения» ряда федеральных законов, направленные на уточнение порядка применения этой правовой категории данных. В частности, в ст.7 ФЗ об информации уместно дополнение о том, что в случае, если доступ к информации обусловлен необходимостью соблюдения определённых предварительных условий (в том числе, преодоления технических механизмов защиты данных, такая информация *не может* считаться общедоступной. В ФЗ о персональных данных следовало бы заменить понятие «общедоступный источник» (персональных данных) на «справочный источник. Требуется *усилить ответственность*уполномоченных организаций и должностных лиц за неразмещение общедоступной информации в форме открытых данных, недостоверность и (или) несвоевременность их размещения. Наконец, в гражданском законодательстве предлагается закрепить правило о том, что обработка материалов, содержащихся в общедоступных базах данных, и охраняемых как объекты авторских ли смежных прав, *допускается без разрешения правообладателя*, если такая обработка направлена на анализ текста и данных в цифровой форме в целях машинного обучения или с иной целью, предполагающей получение

производной информации о закономерностях, тенденциях и корреляциях, выражаемых в обрабатываемых данных. Это соответствует и практике, наблюдаемой в европейских юрисдикциях.

79. Более частные вопросы регулирования данных относятся к сфере тайны связи. Так, с учётом современного уровня развития информационных технологий предлагается:

- распространить (однозначно уточнить, что) правовой режим тайны связи на сообщения, передаваемые не только физическими, но и юридическими лицами и иными организациями.

- включать те или иные данные в категорию тайны связи в зависимости от критериев, которыми они характеризуются. Основным критерием предлагается считать факт наличия сообщения, (а) имеющего определённое содержание и (б) являющегося объектом коммуникации, информационного обмена. К данным, составляющим тайну связи, безусловно относится *содержание* («*контент*») сообщений электросвязи, независимо от технологий их передачи. Помимо содержания сообщений следует различать *сведения об абонентах* (правовая охрана которых во многом совпадает с режимом персональных данных), а также *сведения о соединениях* (включая, в частности, геоинформационные данные) с *различающимся* по сравнению с тайной связи правовым режимом;

- установить обязанность обеспечивать информацию, составляющую тайну связи, операторам сервисов электронной почты, а также компаниям, которые по факту оказывают услуги связи, однако не должны по законодательству иметь лицензию (по аналогии и с курьерскими службами доставки)

- распространить режим тайны связи на субъектов правоотношений, привлекаемых для целей оказания услуг связи, а также расширить перечень целей обработки сведений, составляющих тайну связи для оператора услуг связи;

- уточнить требования к работе с «Большими данными» в контексте соблюдения тайны связи. Режим персональных данных и тайна связи являются дополняющими, а не совпадающими, поэтому при работе с «Большими данными» операторам таких данных требуется вменить обязанность соблюдать требования к обработке не только персональных данных, но и тайны связи,

- установить правовую возможность предоставления согласия на машинный анализ сведений, составляющих тайну связи, в условиях обеспечения соблюдения прав человека. Для решения данного вопроса требуется нормативное закрепление функциональных и технических требований к средствам автоматической обработки сведений, составляющих тайну связи,

поскольку при машинной обработке одной из главных задач является обеспечение высоких стандартов защиты в условиях агрегирования больших массивов данных.

80.Представленные результаты научно-исследовательских работы Института права цифровой среды, обобщённые выводы и сформулированные предложения по корректировке законодательства в сфере регулирования данных, подтверждают, что в целом Российская Федерация имеет все шансы не только занимать лидирующие позиции в глобальной цифровой экономике в силу накопленного технологического потенциала, но и создать законодательные механизмы и гарантии для обеспечения дальнейшего устойчивого развития всех аспектов цифровизации хозяйственной и общественной жизни.