

Анализ и обобщение материалов правоприменительной практики в области обработки персональных данных

Эксперт: д.ю.н., доцент Архипов В.В.

В анализе судебной правоприменительной практики участвовал обучающийся I курса магистратуры Я.М. Салихов.

Аннотация

В рамках проведенного подхода был проведен анализ и обобщение материалов правоприменительной (судебной) практики в области обработки персональных данных за период с 2017 по 2022 г. В основу отчета положены репрезентативные судебные решения по ключевым направлениям практики, соответствующим трем основным аспектам персональных данных (права человека, цифровая экономика, информационная безопасность), из следующих областей: персональные данные и право на неприкосновенность частной жизни; правовой режим персональных данных, распространяемых посредством социальных медиа; использование персональных данных о судимости в коммерческих базах данных; использование биометрических персональных данных в различных областях деятельности, в том числе в области общественной безопасности; действие нормативных правовых актов в области персональных данных в пространстве и по кругу лиц; сопутствующие вопросы, связанные с особенностями отдельных условий обработки персональных данных. По результатам мониторинга отмечена тенденция к глубокому и детальному анализу проблем правового регулирования обработки персональных данных. Можно констатировать, что в правоприменительной практике стал устоявшимся подход, согласно которому обработка персональных данных на общедоступных интернет-ресурсах и в базах данных может осуществляться в общественно значимых целях, хотя в то же время требуется баланс между свободой доступа к информации и неприкосновенностью частной жизни – доступность и публичность данных еще сама по себе не означает, что они не относятся к частной жизни. Сложилась практика применения законодательства о персональных данных к иностранным лицам, осуществляющим деятельность на территории Российской Федерации через сеть Интернет, позже нашедшая отражение в законодательстве. В отношении обработки биометрических персональных данных сохраняется неопределенность в части определения моментов сбора персональных данных, установления личности и применения специального режима биометрических персональных данных.

1. Обоснование выбора темы мониторинга

Согласно ст. 2 Конституции Российской Федерации (далее – «Конституция»), человек, его права и свободы являются высшей ценностью, а признание, соблюдение и защита прав и свобод человека и гражданина – обязанность государства. Ст. 23 Конституции указывает, что каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени, при этом каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ст. 24 Конституции определяет, что сбор, хранение, использование и

распространение информации о частной жизни лица без его согласия не допускается. В то же время, как следует из ч. 4 ст. 29 Конституции, каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. При этом в соответствии с ч. 3 ст. 55 Конституции, права и свободы человека и гражданина могут быть ограничены федеральным законом, хотя и только в той мере, в какой это необходимо в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. Хотя в приведенных статьях термин «персональные данные» не используется прямо, в совокупности их положений отражается определенная концепция баланса конституционных ценностей, характерных для отношений по поводу обработки персональных данных, а также принципиальное значение персональных данных для современного социально-экономического контекста: персональные данные непосредственно связаны с различными правами человека, представляют собой ценный «актив» цифровой экономики и явление, имеющее отношение к информационной безопасности.

В сравнительно-правовом аспекте следует отметить, что российская модель защиты персональных данных исторически связана с Конвенцией СДСЕ № 108 о защите физических лиц при автоматизированной обработке персональных данных (Страсбург, 28.01.1981) (далее – «Конвенция № 108»). Конвенция № 108 была ратифицирована Федеральным законом от 19.12.2005 № 160-ФЗ с заявлениями и вступила в силу для Российской Федерации с 1 сентября 2013 года. Структура и общие положения Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – «Закон о персональных данных»), который в первой редакции действовал с 26.01.2007, в целом следуют логике Конвенции № 108, однако за последние годы в Закон о персональных данных было внесено более 25 изменений, большая часть из которых приходится на период с 2013 года – период, когда информационное законодательство Российской Федерации начало все больше отражать стремление к информационному суверенитету. Сохранив значительную часть общих принципов, на сегодня Закон о персональных данных содержит ряд отличий от своего европейского источника, которые существенным образом влияют на практику правоприменения. В то же время, основные доктринальные представления о роли и значении персональных данных не меняются: персональные данные представляют собой ценность, тесно связанную с неприкосновенностью частной жизни (хотя данные явления – все же разные правовые категории).¹ Персональные данные могут рассматриваться в контексте права на неприкосновенность частной жизни, которое еще в советской правовой доктрине могло быть отнесено к личным неимущественным правам.² Кроме того, в современной цифровой среде персональные данные могут рассматриваться и в другом аспекте – как явление, конституирующее публичную цифровую репрезентацию пользователя и, следовательно, сближающееся не столько с правом не на

¹ См. напр.: Дмитрик Н.А. Пределы правового регулирования в цифровую эпоху // Информационное общество. 2018. № 3. С. 47–58.

² Дмитрик Н.А. О правовой природе согласия на обработку персональных данных // Информационное право. 2018. № 5. С. 43.

неприкосновенность частной жизни, а с правом на неприкосновенность личности как таковой.³

В свою очередь, говорить о том, что персональные данные стали «новой нефтью» в цифровой экономике стало уже своего рода клише. В отечественной юридической литературе значение (и правовые проблемы) персональных данных в контексте использования технологий больших данных было исчерпывающе продемонстрировано А.И. Савельевым еще в 2015 г. в статье «Проблемы применения законодательства о персональных данных в эпоху “Больших данных” (Big Data)».⁴ Как отмечал автор, «обладание большими массивами информации в совокупности с необходимыми инструментами для ее сбора и обработки позволяет создавать товары и услуги в высокой доле добавленной стоимости, а также принимать эффективные управленческие решения».⁵ Технологии больших данных (с использованием инструментов обработки персональных данных) используются в банковском секторе, страховой деятельности, электронной коммерции, медицинской сфере и профилактики правонарушений.⁶ При этом автор уже тогда отметил правовые коллизии в данной области, а именно несовместимость технологий «больших данных» с принципом ограничения обработки персональных данных заранее определенными целями, концепцией информированного, конкретного и сознательного согласия (в тех случаях, когда такое согласие является условием обработки персональных данных) и то обстоятельство, что обезличивание персональных данных не гарантирует их анонимность.⁷ Представления и подходы в этой области развиваются,⁸ однако еще сложно говорить о принципиальном разрешении коллизий. В настоящее время ведутся исследования в области новых методов обезличивания персональных данных, рассматриваются предложения по изменению состава условий обработки персональных данных и т.д. Так или иначе, регулирование персональных данных и правоприменительная практика в данной области принципиально важна для развития электронной коммерции, а технологии больших данных рассматриваются в России как одна из «сквозных цифровых технологий».

Далее, в стратегических документах Российской Федерации особое значение уделяется целому ряду аспектов, которые тесно связаны с обработкой персональных данных. Доктрина информационной безопасности Российской Федерации (утверждена Указом Президента Российской Федерации от 05.12.2016 г. № 646) (далее – «Доктрина») ряд общих положений, непосредственно связанных с персональными данными. Например,

³ Статья эксперта, в которой обосновывается данный подход, принята к публикации в журнале «Закон» в 2022 г. Подход, в том числе, следует из ключевого положения современной медиафилософии, согласно которому виртуальная репрезентация пользователя (которая формально-юридически может быть понята как совокупность персональных данных в цифровой среде, являющаяся при этом публичной в значительной части ситуаций и несводимая к предмету неприкосновенности частной жизни) составляет часть его «тела» в философско-психологическом понимании. См.: Очеретяный К.А. Тело как медиа: опыт реконструкции. Диссертация на соискание ученой степени кандидата философских наук. Санкт-Петербургский государственный университет. Санкт-Петербург, 2015.

⁴ См.: Савельев А.И. Проблемы применения законодательства о персональных данных в эпоху «Больших данных» (Big Data) // Право. Журнал Высшей школы экономики. 2015. № 1. С. 43–66.

⁵ Там же. С. 45.

⁶ Там же. С. 47–52.

⁷ Там же. С. 52–61.

⁸ См. напр.: Савельев А.И. Направления регулирования Больших данных и защита неприкосновенности частной жизни в новых экономических реалиях // Закон. 2018. № 5. С. 122–144 и более поздние публикации, в т.ч. иных авторов.

согласно п. 8 Доктрины, обеспечение и защита конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информации, неприкосновенности частной жизни при использовании информационных технологий, относится к национальным интересам в информационной сфере. Среди прочего, согласно п. 14 Доктрины, угрозы в области обработки персональных данных рассматриваются в контексте возрастающих масштабов компьютерной преступности. В целом, вопросы безопасности находят отражение в Федеральном законе от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», отдельные нормы которого можно считать бланкетными, отсылающими и к законодательству о персональных данных. В п. 31 Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы определены действия, необходимые для защиты данных, среди которых можно отдельно отметить п. «г», которым предусмотрено обеспечение обработки данных на российских серверах при электронном взаимодействии лиц, находящихся на территории Российской Федерации, а также передача таких данных на территории Российской Федерации с использованием сетей связи российских операторов. В рассматриваемой области это положение находит прямое отражение в требовании, закрепленном ч. 5 ст. 18 Закона о персональных данных о «локализации» персональных данных.

Наконец, именно в рамках правоприменительной практики в области персональных данных (и, как раз, в связи с требованием о «локализации» персональных данных) за последние годы был поставлен принципиальный вопрос о применении требований российского законодательства к иностранным компаниям, действующим через сеть Интернет. Впоследствии эти подходы нашли отражение в положениях Федерального закона от 01.07.2021 № 236-ФЗ «О деятельности иностранных лиц в информационно-телекоммуникационной сети “Интернет” на территории Российской Федерации».

Данные три аспекта персональных данных (права человека, цифровая экономика, информационная безопасность) определяют три ключевых обобщенных носителя юридически значимых интереса в этой области – личность, бизнес и государство,⁹ – обуславливают непреходящую значимость проблематики персональных данных в современных условиях и задают вектор отбору репрезентативных решений в ходе мониторинга правоприменения.

2. Методы и ограничения исследования

Основным специальным методом исследования является формально-юридический (догматический) метод предполагающий, с одной стороны, принятие положений действующего позитивного права за аксиому, а с другой – постановку гипотез о правильном результате юридического толкования, которая подлежит подтверждению или опровержению. Главные задачи формально-юридического метода заключается в оценке правоприменительной практики, выявлению формальной неопределенности отдельных правовых норм, объяснение закономерностей развития правоприменительной практики и законодательства.

⁹ Данная точка зрения была ранее раскрыта в одной из предшествующих публикаций эксперта. См.: Архипов В.В. Проблема квалификации персональных данных как нематериальных благ в условиях цифровой экономики, или нет ничего более практичного, чем хорошая теория // Закон. 2018. № 2. С. 52–68.

Временные рамки исследования составляют 5 лет. Это обусловлено как инструментальными соображениями, так и тем обстоятельством, что именно данный период характеризуется увеличением количества правоприменительных решений в области обработки персональных данных.

Настоящий отчет при этом построен по принципу отражения наиболее значимых, по мнению эксперта, правоприменительных решений в области обработки персональных данных, прямо или косвенно соответствующих основным отмеченным ранее направлениям: непосредственная защита прав субъектов персональных данных, обработка персональных данных в цифровой экономике, информационная безопасность (включая вопрос о применении законодательства о персональных данных к зарубежным операторам персональных данных). Правоприменительным решениям по отдельным менее значимым вопросам комментарии даются по мере необходимости.

3. Анализ правоприменительной практики по основным направлениям

За исследуемый период к наиболее значимым правоприменительным решениям в области обработки персональных данных, по мнению эксперта, относятся указанные в соответствующих разделах далее.

3.1. Персональные данные и право на неприкосновенность частной жизни

Наиболее значимым правоприменительным актом в данном случае можно считать Постановление Конституционного Суда РФ от 25.05.2021 № 22-П «По делу о проверке конституционности пункта 8 части 1 статьи 6 Федерального закона “О персональных данных” в связи с жалобой общества с ограниченной ответственностью “МедРейтинг”». Данный акт завершил длительную историю судебного разбирательства, связанную с возможностью юридического лица, являющегося владельцем сайта в сети Интернет (при этом зарегистрированного как средство массовой информации), используемого среди прочего для распространения сведений о работниках медицинской организации и отзывов об их профессиональной деятельности.¹⁰ Значение данного спора, в том числе, обусловлено значимостью данного сервиса, а также тем, что и другие заметные цифровые ресурсы, как в области медицины, так и в области других областей профессиональной деятельности, построены по такому же принципу. В рассматриваемом деле жалоба была подана в контексте спора с физическим лицом, требовавшим удаления персональных данных с сайта заявителя.

По существу ООО «МедРейтинг» оспаривало конституционность п. 8 ч. 1 ст. 6 Закона о персональных данных, который устанавливает в качестве одного из возможных условий обработки персональных данных осуществление профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных. Положения данного пункта оспаривались в той части, в которой он, по мнению заявителя, позволяет суду на основе произвольно выбранных критериев оценивать соблюдение баланса между правом на неприкосновенность частной жизни и свободой распространения информации, запрещать

¹⁰ См.: Апелляционное определение Воронежского областного суда от 12.02.2019 г. по делу № 33–789; Апелляционное определение Воронежского областного суда от 30.05.2019 г. по делу № 33–3559; Апелляционное определение Воронежского областного суда от 12.03.2020 г. по делу № 33–1212; Апелляционное определение Воронежского областного суда от 05.08.2021 г. по делу № 33–4431/2021; Определение Воронежского областного суда от 22.07.2021 г. по делу № 33–4431/2021.

средствам массовой информации обрабатывать персональные данные медицинского работника, которые в силу закона стали общедоступными, и тем самым создавать препятствия для осуществления профессиональной деятельности журналиста и законной деятельности средств массовой информации.

Согласно резолютивной части рассматриваемого Постановления Конституционного Суда РФ, п. 8 ч. 1 ст. 6 Закона о персональных данных был признан не противоречащим Конституции Российской Федерации в той мере, в какой он по своему конституционно-правовому смыслу в системе действующего правового регулирования:

- допускает размещение на сайте в сети Интернет средством массовой информации, действующим в форме сетевого издания, персональных данных медицинского работника, ранее размещенных на основании федерального закона на официальном сайте соответствующей медицинской организации, вне зависимости от наличия на то его согласия;

- предусматривает обязанность редакции такого средства массовой информации не допускать наличия на своем сайте исходящих от третьих лиц оценок, не относящихся к профессиональной деятельности медицинского работника, а равно очевидно противоправных высказываний;

- предусматривает обязанность редакции такого средства массовой информации принимать меры по проверке сведений, предположительно содержащих не соответствующие действительности утверждения, порочащие честь, достоинство или деловую репутацию медицинского работника, на основании его обращения в разумные сроки, с целью их изменения либо удаления, а равно с целью опубликования в установленном законом порядке опровержения (ответа) на том же сайте, на время проверки приостанавливая доступ к соответствующему отзыву или делая пометку о его спорном характере;

- не исключает возможности на основании судебного решения, вынесенного по обращению медицинского работника, установить для такого средства массовой информации – если оно допускает систематическое злоупотребление правом при размещении персональных данных медицинского работника или систематически не предотвращает такого злоупотребления правом лицами, размещающими отзывы, – запрет на распространение персональных данных медицинского работника и (или) отзывов о его профессиональной деятельности, когда иные способы защиты не смогли (не могут) обеспечить защиту его прав.

Тем самым Конституционный Суд РФ устранил существенную формальную неопределенность, сопровождавшую п. 8 ч. 1 ст. 6 Закона о персональных данных долгое время и существенным образом повлиял на последующую практику.¹¹ Кроме того, в отечественной правоприменительной практике получил отражение тот значимый тезис, что фактически общедоступный характер информации сам по себе еще не означает, что данная информация не относится к предмету неприкосновенности частной жизни.

Тем не менее, объективно сохраняется относительная неопределенность в отношении того, считать или нет правовой режим сайта в сети Интернет в рассматриваемом

¹¹ См. напр.: Определение Четвертого кассационного суда общей юрисдикции от 25.11.2021 по делу № 88–20323/2021; Определение Четвертого кассационного суда общей юрисдикции от 08.06.2021 по делу № 88–13314/2021.

деле существенным фактом для иных рассматриваемых дел, относящихся к аналогичным, но не зарегистрированным в качестве средств массовой информации ресурсам. Актуальность данной проблемы подчеркивается судебными спорами, связанными с другими аналогичными, но не находящимся под таким правовым режимом, ресурсами.¹² По мнению эксперта, с учетом особенностей функционирования интернет-сервисов и их значения, такой правовой режим не является принципиальным для реализации в правоотношениях той логики, которая была заложена в резолютивной части приведенного судебного решения. Однако это означает необходимость проработки взвешенной, основанной на балансе интересов позиции, которая устраняла бы формальную неопределенность по применению рассматриваемого условия обработки персональных данных в отношении ресурсов, не зарегистрированных в качестве средств массовой информации.

3.2. Правовой режим персональных данных, распространяемых посредством социальных медиа

За рассматриваемый период данный вопрос был затронут в контексте широкой связи с известным спором между ООО «ВКонтакте» и ООО «Дабл», предмет которого лежит в плоскости интеллектуальных прав (как показывает анализ судебных актов,¹³ несмотря на очевидную связь с проблематикой обработки персональных данных в социальных медиа, данный вопрос по существу сторонами не затрагивается). Согласно фабуле дела в изложении соответствующего судебного акта, Акционерное общество «Национальное бюро кредитных историй» обратилось в Арбитражный суд города Москвы с заявлением о признании недействительным предписания Управления Роскомнадзора по Центральному федеральному округу об устранении выявленного нарушения в части необходимости включения в уведомление уполномоченного органа данных физических лиц (клиентов либо потенциальных клиентов финансовой организации) из открытых источников информации, передаваемых финансовой организации, полученных с использованием сервиса Double Data Social Link - web-ссылка, результат поиска о клиенте либо потенциальном клиенте, и сервиса Double Data Social Attributes - обработка профиля искомого физического лица в открытых источниках информации, а также в части указания на нарушение требований пункта 1 части 1 статьи 6 Федерального закона от 27 июля 2006 года N 152-ФЗ "О персональных данных" в виде отсутствия согласия на обработку содержащихся в открытых источниках (социальных сетях: ВКонтакте, Одноклассники, МойМир, Instagram, Twitter; интернет-порталов Авито и Авто.ру) персональных данных клиента либо потенциального клиента финансовой организации, в рамках оказания услуги на основании сервиса "big data".¹⁴

¹² См. напр.: Определение Третьего кассационного суда общей юрисдикции от 17.05.2021 г. № 88-8193/2021

¹³ См.: Решение Арбитражного суда г. Москвы от 12.10.2017 г. по делу № А40-18827/17-110-180; Постановление Девятого арбитражного апелляционного суда от 06.02.2018 г. по делу № А40-18827/17; Постановление Суда по интеллектуальным правам от 24.07.2018 г. по делу № А40-18827/2017; Решение Арбитражного суда г. Москвы от 22.03.2021 г. по делу № А40-18827/17-110-180; Постановление Девятого арбитражного апелляционного суда от 08.07.2021 г. по делу № А40-18827/17.

¹⁴ См.: Решение Арбитражного суда г. Москвы от 05.05.2017 г. по делу № А40-5250/17-155-51; Постановление Девятого арбитражного апелляционного суда от 27.07.2017 г. № 09АП-31744/2017 по делу № А40-5250/17; Постановление Арбитражного суда Московского округа от 09.11.2017 г. № Ф05-16382/2017 по

Согласно правовой позиции, отраженной в соответствующих судебных решениях, рассматриваемые данные нельзя считать общедоступными лишь потому, что они размещены в открытых источниках. Суд при этом сослался на положение ч. 1 ст. 8 Закона о персональных данных, согласно которому 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. Соответственно, заявитель должен был доказать наличие согласий субъектов персональных данных на обработку их персональных данных рассматриваемым способом.

Отметим, что применение концепции общедоступных источников персональных данных к социальным медиа выглядит ошибочным с точки зрения исторического толкования ст. 8 Закона о персональных данных. Однако и в этом случае тезис о возможности свободного использования фактически общедоступных данных нуждается в дополнительном обосновании в свете той позиции, которая была представлена в п. 3.1 настоящего отчета (использование данных, которые фактически являются общедоступными, также должно осуществляться на каком-либо законном основании, не предполагающем нарушение прав субъектов персональных данных). Кроме того, конкретно по этой категории дел, как можно заключить, поставлена точка в связи с изменениями, внесенными Федеральным законом от 30.12.2020 г. № 519-ФЗ, которым из Закона о персональных данных было исключено условие обработки, предусмотренное п. 10 ч. 1 ст. 6 (осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе) и введено новое условие «обработка персональных данных, разрешенных субъектом персональных данных для распространения, осуществляется с соблюдением запретов и условий, предусмотренных статьей 10.1 настоящего Федерального закона».

3.3. Использование персональных данных о судимости в коммерческих базах данных

Один из вопросов, который за исследуемый период нашел отражение в ограниченном виде (на уровне одного судебного спора), но который поднимает принципиальную проблему возможности создания информационных коммерческих баз данных на основе персональных данных, полученных из различных открытых источников, был на момент подготовки отчета рассмотрен Щербинским районным судом г. Москвы.¹⁵ Истец обратился в суд с иском к ответчикам, в том числе, о признании действий незаконными и наложении запрета на распространение персональных данных при том, что ответчики на коммерческой основе предлагали третьим лицам приобрести базу данных, содержащую персональные данные истца. Истец не давал согласия на распространение персональных данных.

Как следует из судебного решения, спорные персональные данные были связаны с судимостью истца по приговору одного из судов г. Москвы. Как следует из правовой

делу № А40-5250/2017; Определение Верховного Суда РФ от 29.01.2018 № 305-КГ17-21291 по делу № А40-5250/2017.

¹⁵ Решение Щербинского районного суда г. Москвы от 29.10.2021 г. по делу № 2-1328/21.

позиции, отраженной в рассматриваемом судебном решении, согласно ч. 3 статьи 10 Закона о персональных данных, обработка персональных данных о судимости может осуществляться лицами в случаях и в порядке, которые определяются в соответствии с федеральными законами. Однако федеральным законом, определяющим случаи и порядок осуществления любыми лицами обработки персональных данных о судимости, является, в том числе, и Закон о персональных данных. Согласно п. 11 ч. 1 ст. 6 Закона о персональных данных, обработка персональных данных допускается, когда осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом. Части 1 и 3 ст. 15 Федерального закона от 22.12.2008 № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации» (далее – «Закон об обеспечении доступа к информации о деятельности судов») устанавливает, что тексты приговоров размещаются не позднее одного месяца после дня их вступления в законную силу. При размещении в сети Интернет текстов судебных актов, принятых судами общей юрисдикции, в целях обеспечения безопасности участников судебного процесса и защиты государственной и иной охраняемой законом тайны из этих актов исключаются персональные данные, указанные в ч. 4 указанной статьи. Не подлежат исключению фамилии, имена и отчества осуждённого. Данные об уголовном деле в отношении истца и принятые в отношении него судебные решения по этому делу были опубликованы на сайтах Генеральной прокуратуры Российской Федерации и соответствующих судов.

В свете этого суд согласился с доводами ответчика, согласно которым судимость истца подлежала опубликованию и обязательному раскрытию в соответствии федеральным Законом об обеспечении доступа к информации о деятельности судов. При этом время, в течение которого эта информация (данные) должны быть опубликованными (раскрыты), не ограничено ни временем, в течение которого лицо, осуждённое за совершение преступления, считается судимым, ни каким-либо иным сроком. Соответственно, наличие информации на указанных ресурсах о судимости истца, полученной законным путем, права и законные интересы истца нарушать не может. Более того, как было установлено судом, целью использования базы данных является защита законных интересов третьих лиц и достижение общественно значимых целей, прежде всего противодействие легализации (отмыванию) доходов, полученных преступным путем и финансированию терроризма, а сам ресурс широко используется российскими органами государственной власти и кредитными организациями. В свете этого суд счел также возможным сослаться и на п. 7 ч. 1 ст. 6 Закона о персональных данных, по которому персональные данные могут обрабатываться для осуществления прав и законных интересов оператора или третьих лиц, либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных. Также судом был сделан сопутствующий вывод о том, что исходя из смысла ч. 1 ст. 18 Закона о персональных данных, получение персональных данных из открытых источников не подпадает под понятие «сбор персональных данных» (при котором обязательно обеспечивать их обработку с использованием баз данных, находящихся на территории персональных данных).

Данный правоприменительный акт на момент подготовки отчета оспаривается, однако в нем отражена правовая позиция, которая может, при определенных

обстоятельствах, способствовать разрешению неопределенности законодательства о персональных данных, как минимум, в двух аспектах: возможность обработки персональных данных, ставших фактически общедоступными, в общественно значимых целях (но отличных от случая с профессиональной деятельностью, рассмотренного ранее), и пределы и условия обработки персональных данных о судимости. Правовую позицию, представленную в рассмотренном решении в целом можно считать обоснованной, однако нельзя исключать и ее изменения в свете изменений, внесенных Федеральным законом от 30.12.2020 г. № 519–ФЗ, которым из Закона о персональных данных было исключено условие обработки, предусмотренное п. 10 ч. 1 ст. 6 (осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе) и введено новое условие «обработка персональных данных, разрешенных субъектом персональных данных для распространения, осуществляется с соблюдением запретов и условий, предусмотренных статьей 10.1 настоящего Федерального закона».

3.4. Использование биометрических персональных данных в различных областях деятельности

В настоящее время вопросам правовых моделей обработки биометрических персональных данных уделяется повышенное внимание в теории и на практике. С одной стороны, биометрические персональные данные используются в перспективных цифровых технологиях (преимущественно, в целях идентификации). С другой стороны, риски, связанные с утечкой или неправомерной обработкой биометрических персональных данных значительно выше, чем в случае с иными категориями персональных данных – как раз в силу степени точности идентификации субъекта, а также в связи с тем, что, как минимум, ряд биометрических персональных данных не может быть произвольно изменен субъектом, что снижает возможности защиты субъекта при различных нарушениях с точки зрения информационной безопасности. При этом объем нормативного регулирования обработки биометрических персональных данных по-прежнему достаточно ограничен и способствует неопределенности по многим вопросам.

3.4.1. Обработка биометрических персональных данных для целей, связанных с общественной безопасностью

Технологии, в которых применяется обработка биометрических персональных данных для целей, связанных с общественной безопасностью, преимущественно связаны с использованием систем искусственного интеллекта (нейросетей) при обработке материалов видеонаблюдения и являются предметом острых дискуссий не только в России, но и во всем мире. Для целей отчета ограничимся наиболее репрезентативными судебными делами, вскрывающими некоторые проблемы юридического характера.

Так, в одном из репрезентативных случаев¹⁶ заявитель указал, что при рассмотрении дела об административном правонарушении производился осмотр записей с камер видеонаблюдения, в конкретном определенном промежутке времени. При этом зафиксировано целенаправленное приближение фокуса камеры (увеличение изображения) в 32 раза с фиксацией на лице, что свидетельствует о применении технологии

¹⁶ См.: Кассационное определение Второго кассационного суда общей юрисдикции от 31.07.2020 г. №88а-17020/2020; Апелляционное определение Московского городского суда от 30.01.2020 по делу №33а-707/2020, 2а-577/2019.

распознавания лиц и противоречит ч. 1 ст. 11 Закона о персональных данных (необходимость письменного согласия). Также по мнению заявителя, такая обработка биометрических персональных данных нарушает тайну частной жизни. В этой связи жалоба была направлена на прекращение обработки биометрических ПД, без согласия заявителя, системой ГУ МВД. При этом суды отказали в удовлетворении требований указав, в частности, на то, что: действия ответчиков соответствуют законодательству, осуществляются в том числе в интересах безопасности самого заявителя и не нарушают прав и законных интересов заявителя; технология распознавания лиц сама по себе не запрещена; Департамент информационных технологий г. Москвы, будучи оператором ЕЦХД, имеет необходимые правовые основания для обработки информации; сотрудники ГУ МВД РФ по г. Москве используют систему для реализации служебных обязанностей; граждане не относятся к непосредственным объектам видеонаблюдения, сбор персональных данных не осуществляется, как не осуществляется и процедура идентификации личности (хотя происходит сопоставление данных с видеокамер с фотографией в распоряжении правоохранительных органов).

Известная на момент подготовки отчета судебная практика по данному вопросу демонстрирует отсутствие достаточного уровня формальной определенности, как минимум, по трем ключевым вопросам: отнесение соответствующих данных к персональным данным как таковым; определение факта и момента сбора персональных данных (при том, что понятие сбора персональных данных не определено на уровне Закона о персональных данных) и определение момента «установления личности» (понятие, с которым ч. 1 ст. 11 Закона о персональных данных связывает применение специального правового режима обработки биометрических персональных данных) на различных этапах функционирования технологических решений в области распознавания лиц и видеоаналитики в целом.

Исходя из общего определения персональных данных («любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу...»), видеоизображения и производная от них информация и идентификаторы (векторы) должны рассматриваться как персональные данные. В то же время, в отдельных случаях из судебной практики может следовать обратное, что создает объективную правовую неопределенность.

В части определения момента сбора важно то, что с данным моментом Закон о персональных данных связывает целый ряд обязанностей оператора (ст. 18 Закона о персональных данных). Существующая в области применения систем видеонаблюдения и распознавания лиц неопределенность связана с тем, что некоторые системы позиционируются как не направленные на наблюдение за физическими лицами (а направленные, например, на наблюдение за неодушевленными объектами и (или) территориями), но полученные из них видеоматериалы могут в дальнейшем использоваться для установления принадлежности данных к определенным физическим лицам на основании сравнения, например, векторов (технической информации, возникающей из обработки видеоизображений по ряду критериев, в том числе собственно биометрических параметров силуэта, лица и т.п.).

Наконец, определение момента идентификации (установления личности) принципиально важно для применения специального режима биометрических

персональных данных. Тот критерий, что персональные данные, характеризующие физиологические и биологические особенности человека, на основании которых можно установить его личность, фактически используются для установления личности субъекта персональных данных, в любом случае определяет применение специального режима биометрических персональных данных. Тем не менее, в законе или правоприменительной практике однозначно не определено, что именно следует считать «установлением личности». В имеющейся судебной практике, связанной со специфическим контекстом публичных интересов, высказана позиция, что сравнение различных производных данных (одни, в конечном счете, получены из систем видеонаблюдения, другие – от других государственных органов) не представляет собой процесс установления личности, однако данное утверждение не представляется универсальным для всех случаев, поскольку процесс сопоставления данных такого рода, с точки зрения здравого смысла и общих доктринальных подходов, и может быть интерпретирован как выражение процесса идентификации личности.

Более того, даже понимая и разделяя значимость особых государственных интересов в обеспечении безопасности посредством инструментов видеонаблюдения и видеоаналитики, можно поставить вопрос о возможной избыточности аргументации правоприменительных органов, стремящихся разрешить вопросы о моменте сбора и установления личности в рассматриваемых случаях, поскольку применение технологий распознавания лиц (в случае, если они применяются) в публичных целях может быть обосновано с отсылкой к ч. 2 ст. 11 Закона о персональных данных либо данный аспект может свидетельствовать о необходимости уточнения законодательных оснований в данной области. Иными словами, текущая судебная практика демонстрирует потенциал для развития законодательной базы в данной области.

3.4.2. Обработка биометрических персональных данных в иных обстоятельствах

В иных обстоятельствах правоприменительная практика также демонстрирует недостаточную степень единообразия в подходах к определению того, когда и при каких условиях определенные виды данных, обрабатываемые определенным образом, могут рассматриваться как биометрические персональные данные.

Так, по вопросу признания определенной информации биометрическими персональными данными можно привести следующие примеры, когда информация признавалась в качестве таковых:

- *фотографии на пропусках* (напр. Определение Верховного Суда РФ от 05.03.2018 №307-КГ18-101 по делу № А42-342/2017; Постановление Арбитражного суда Северо-Западного округа от 21.11.2017 №Ф07-11732/2017 по делу №А42-342/2017);
- *видеоизображения, получаемые с помощью видеокамеры в общей долевой собственности истца и ответчика* (напр. Определение Пятого кассационного суда общей юрисдикции от 28.09.2021 №88–7100/2021).
- *информация о здоровье наследодателя, содержащаяся в медицинской организации* (напр. Апелляционное определение Московского городского суда от 30.01.2019 по делу №33а-1238/2019).
- *сведения, содержащиеся в удостоверении моряка* (напр. Апелляционное определение Санкт-Петербургского городского суда от 07.07.2020 №33а-13473/2020 по делу №2а-769/2020).

- *ладони учащихся, рисунок вен рук, используемый для идентификации при оплате* (напр. Решение Лискинского районного суда Воронежской области от 09.07.2018 №12–35/2018).

В то же время можно привести и обратные примеры, когда информация не признавалась биометрическими персональными данными (помимо примера, ранее приведенного в п. 3.4.1 отчета):

- *видеоизображения на частных камерах видеонаблюдения при том, что земельный участок истцов не охватывается камерой, а качество съемки не позволяет достоверно идентифицировать полученные при съемке изображения с конкретными лицами* (напр. Апелляционное определение Верховного суда Республики Коми от 04.02.2019 по делу №33–640/2019).

- *видеоизображение, полученное посредством съемки на камеру мобильного телефона (по причине того, что видеозапись не содержит сведений, позволяющих идентифицировать физическое лицо как конкретного субъекта данных)* (напр. Постановление Четвертого кассационного суда общей юрисдикции от 16.10.2020 №16–894/2020).

- *видеозапись с камер наблюдения медицинской организации, продемонстрированная посетителю с целью помощи в установлении обстоятельств пропажи телефона посетителя* (напр. Определение Восьмого кассационного суда общей юрисдикции от 19.12.2019 №88–1005/2019).

- *информация, потенциально собираемая с камеры видеонаблюдения в доме при том, что она не направлена на квартиру истца и используется для охраны и безопасности владельца* (напр. Решение Кировского районного суда города Саратова от 01.06.2021 по делу №2–2354/2021).

- *информация с камер видеонаблюдения в государственном органе до передачи в целях идентификации* (напр. Апелляционное определение Нижегородского областного суда от 19.12.2018 по делу № 33а-15421/2018).

- *изображение спящего работника до того момента, как оно будет передано для установления личности* (напр. Решение Кинешемского городского суда Ивановской области от 27.05.2021 по делу №2–873/2021).

3.5. Действие нормативных правовых актов в области персональных данных в пространстве и по кругу лиц

В доктрине правового регулирования отношений в сети Интернет проблема определения юрисдикции (в широком смысле слова) традиционно рассматривается как «сквозная». Деятельности в Интернете в обычных условиях носит принципиально трансграничный характер, и обычным положением дел является предоставление каким-либо оператором персональных данных услуг, направленных на субъектов персональных данных, находящихся в другой юрисдикции, в том числе в Российской Федерации, без каких-либо форм традиционного прямого присутствия – например, филиала или представительства). Это порождает проблему, связанную с возможностью и пределами распространения национального законодательства на такого рода деятельность зарубежных компаний. Исторически в информационном праве одной из первых областей, в которых данная проблема стала актуальной (наряду с регулированием отношений по поводу рекламы), стала область персональных данных.

В российской правоприменительной практике за отчетный период (из предшествующих актов можно отметить Решение Таганского районного суда г. Москвы от 04.08.2016 г. по делу №2-3491/2016 и Апелляционное определение Московского городского суда от 10.11.2016 г. по делу № 33-38783/16, в которых соответствующая аргументация была уже кратко представлена в принципиальной форме) наиболее полное отражение данная проблема нашла в административном деле, в рамках которого рассматривался вопрос об ответственности иностранной интернет-компании по ст. 19.7 КоАП за отсутствие надлежащего ответа на запрос Роскомнадзора, сделанный на основании ст. 23 Закона о персональных данных¹⁷ и последующие дела, связанные с требованием об ответственности за нарушение требования о «локализации» персональных данных.¹⁸

Основными аргументами для применения положений российского законодательства к деятельности иностранного юридического лица в данном случае выступили следующие. Доступ к социальной сети свободный, не ограничен на территории России и в целом не ограничен по принципу гражданства. Акты, определяющие условия предоставления сервисов, размещенные на сайте, представлены на русском языке, из чего следует, что деятельности компании направлена на привлечение, в том числе, русскоязычного населения, основную долю которого составляют граждане Российской Федерации и проживающие на ее территории. В целом в таком контексте суд квалифицировал деятельность социальной сети как деятельность по сбору персональных данных граждан Российской Федерации посредством сети Интернет, в том числе с территории Российской Федерации.

Хотя по степени значимости данную позицию было невозможно проигнорировать при подготовке отчета, следует заметить, что такая позиция стала уже устоявшейся по многим другим вопросам и сейчас не подразумевает каких-либо специальных оснований для критического осмысления в связи с принятием Федерального закона от 01.07.2021 № 236-ФЗ «О деятельности иностранных лиц в информационно-телекоммуникационной сети “Интернет” на территории Российской Федерации», вполне определенно устанавливающего критерии, при которых деятельность зарубежных лиц может рассматриваться как осуществляемая на территории Российской Федерации.

3.6. Сопутствующие результаты мониторинга правоприменения в области персональных данных

Помимо рассмотренных репрезентативных дел по ключевым, с точки зрения значимости, направлениям за отчетный период можно также отметить правоприменительную практику по частным вопросам, в том числе связанным с условиями обработки персональных данных.

Можно отметить следующие позиции.

В части такого условия, как предоставленное субъектом согласие (п. 1 ч. 1 ст. 6 Закона о персональных данных): согласие на обработку персональных данных может быть

¹⁷ Постановление Мирowego судьи судебного участка № 422 Таганского района г. Москвы от 05.04.2019 г. по делу № 5–618/19.

¹⁸ См. напр.: Постановление Мирowego судьи судебного участка № 374 Таганского района г. Москвы от 13.02.202 г.; Решение Таганского районного суда г. Москвы от 16.03.2020 г.; Постановление Второго кассационного суда общей юрисдикции от 07.07.2020 г. по делу №16-3770/20.

выражено дистанционным способом посредством авторизации через СМС;¹⁹ требование о получении согласия как обязательное условие для предоставления услуг по медицинскому страхованию не нарушает права потребителя в случае, если иным образом профессиональная сторона не имеет возможности оказывать услуги по организационным причинам.²⁰

В части исполнения оператором требований, возложенных законом (п. 2 ч. 1 ст. 6 Закона о персональных данных): предоставление данных пользователя социальной сети полиции на основании соответствующего закону требования в связи оперативно-разыскной деятельностью является законным;²¹ требование о предоставлении персональных данных прокурором на основании законодательства соответствует данному основанию;²² оператор мобильной связи может хранить персональные данные абонентов и после отзыва согласия на основании требований законодательства о связи.²³

В части обработки персональных данных осуществляемой в связи с участием лица в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах (п. 3 ч. 1 ст. 6 Закона о персональных данных): обработка персональных данных ответчика по делу, связанному с задолженностью по кредитному договору, осуществляется на данном основании и не рассматривается как нарушение банковской тайны;²⁴ сбор доказательств посредством видеозаписи военкоматом для целей последующего предоставления в ходе судебного разбирательства может быть основан на данном условии и не подразумевает недопустимое доказательство;²⁵ передача персональных данных всей семьи, проживающей на определенной жилплощади управляющей компанией своему судебному представителю для целей защиты прав и законных интересов в суде осуществляется на основе данного условия обработки персональных данных.²⁶

Если обработка персональных данных необходима для исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве (п. 3.1 ч. 1 ст. 6 Закона о персональных данных): обработка персональных данных третьим лицом, осуществляющим взыскание долга, соответствует законодательству по этому основанию, даже если такое право было получено на стадии исполнительного производства;²⁷ передача персональным данным со стороны банка в адрес судебных приставов соответствует

¹⁹ Апелляционное определение Новосибирского областного суда от 12.10.2017 г. по делу № 33-9263/2017.

²⁰ Апелляционное определение Московского городского суда от 12.12.2018 г. по делу № 33-54212/2018.

²¹ Определение Третьего кассационного суда общей юрисдикции от 15.07.2020 г. по делу № 88-8222/2020; Определение Третьего кассационного суда общей юрисдикции от 01.06.2020 г. № 88-9326/2020.

²² Определение Восьмого кассационного суда общей юрисдикции от 31.01.2020 г. № 16-275/2020.

²³ Апелляционное определение Московского городского суда от 06.07.2020 г. по делу № 33-23715/2020.

²⁴ Апелляционное определение Санкт-Петербургского городского суда от 27.02.2020 № 33-648/2020 по делу № 2-1855/2019.

²⁵ Апелляционное определение Верховного суда Республики Мордовия от 24.04.2018 по делу № 33а-770/2018.

²⁶ Апелляционное определение Санкт-Петербургского городского суда от 29.05.2019 г. № 33-11444/2019 по делу № 2-5365/2018.

²⁷ Апелляционное определение Московского городского суда от 22.08.2018 по делу № 33-33329/2018.

данному основанию, однако банк обязан надлежащим образом идентифицировать должника во избежание нарушения прав третьих лиц.²⁸

В отношении оказания государственных или муниципальных услуг (п. 4 ч. 1 ст. 6 Закона о персональных данных): отказ в ежемесячной выплате за первого ребенка в отсутствие согласия на обработку персональных данных отца является незаконным, поскольку действует данное условие для обработки персональных данных;²⁹ данное условие для обработки персональных данных применимо в случаях прямого обращения в государственные органы, однако согласие на обработку персональных данных требуется в случае обращения за услугой через МФЦ;³⁰ центр оказания государственных услуг, принимающий платежи от домохозяйств в силу закона может обрабатывать персональные данные, полученные в ходе общего собрания жильцов, даже в отсутствие согласия на обработку персональных данных.³¹

В отношении обработки персональных данных на основании договора, стороной которого является субъект персональных данных (п. 5 ч. 1 ст. 6 Закона о персональных данных): персональные данные можно считать обрабатываемыми на данном основании даже в том случае, когда договор заключен посредством конклюдентных действий;³² если будет доказано, что оператор не сумел надлежащим образом идентифицировать сторону возможного кредитного договора, в результате чего он начал обрабатывать персональные данные другого лица, то оператор не может опираться на такое условие обработки;³³ изменение стороны в договоре не отменяет возможность опираться на сам договор как условие обработки персональных данных;³⁴ деятельность по возврату долга, порученная специализированной организации, может рассматриваться как деятельность, предполагающая обработку персональных данных по указанному основанию (наряду с законным интересом кредитора).³⁵

В связи с обработкой персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц, либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных (п. 7 ч. 1 ст. 6 Закона о персональных данных): обработка персональных данных в рамках деятельности по возврату долга, порученная специализированной организации, может осуществляться на данном основании;³⁶ владелец

²⁸ Апелляционное определение Новосибирского областного суда от 17.08.2017 по делу № 33-7782/2017.

²⁹ Определение Четвертого кассационного суда общей юрисдикции от 18.02.2020 по делу № 88-5815/2020.

³⁰ Определение Московского городского суда от 17.06.2019 № 4га-621/2019.

³¹ Апелляционное определение Московского городского суда от 30.11.2017 г. по делу № 33-40869/2017.

³² Апелляционное определение Нижегородского областного суда от 30.04.2019 г. по делу № 33-4851/2019.

³³ Апелляционное определение Оренбургского областного суда от 20.06.2017 г. по делу № 33-4320/2017.

³⁴ Апелляционное определение Свердловского областного суда от 21.08.2018 г. по делу № 33-14121/2018.

³⁵ Решение Санкт-Петербургского городского суда от 29.10.2019 г. № 7-1848/2019 по делу № 12-577/2019.

³⁶ Решение Санкт-Петербургского городского суда от 29.10.2019 г. № 7-1848/2019 по делу № 12-577/2019 (указанное ранее).

земельного участка в садоводстве не может потребовать предоставления реестра других владельцев на данном основании;³⁷ обработка персональных данных в ходе спам-звонков по телефону в целях взыскания долга с помощью услуг третьего лица не может быть основана на данном условии;³⁸ обработка персональных данных для целей защиты прав в рамках судебного процесса охватывается, в том числе, и данным основанием, а предоставление персональных данных суду не может рассматриваться как незаконная передача персональных данных.³⁹

В случае когда осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом (п. 11 ч. 1 ст. 6 Закона о персональных данных): запрос субъекта персональных данных об удалении его персональных данных из информационной системы, содержащей информацию о результатах избирательного процесса не может быть удовлетворен, поскольку у оператора имеется указанное законное основание для обработки персональных данных.⁴⁰

4. Заключение

Исследование показывает, что за период с 2017 по 2022 г. (март 2022 г.) количество правоприменительных решений в области персональных данных лишь увеличилось. Вероятно, во многом это следует связывать как с повышением юридической грамотности и осведомленности о защите персональных данных самих субъектов персональных данных, так и повышением общего уровня квалификации правоприменительных органов в изучаемой сфере.

Помимо частных вопросов толкования отдельных положений законодательства о персональных данных, за отчетный период правоприменительная практика Российской Федерации была обогащена правовыми позициями по вопросам пределов неприкосновенности частной жизни в цифровом пространстве, возможности использования третьими лицами фактически общедоступных персональных данных, включения отдельных категорий персональных данных в коммерческие базы данных, использования биометрических персональных данных в различных областях деятельности (включая общественную безопасность), применения российского законодательства к иностранным операторам персональных данных.

Отличительная черта данного периода анализа заключается в том, что ряд положений, ранее выработанных правоприменительной практикой, уже нашел свое отражение в новых законодательных актах (таких как Федеральный закон от 01.07.2021 № 236-ФЗ «О деятельности иностранных лиц в информационно-телекоммуникационной сети “Интернет” на территории Российской Федерации») или поправках в Закон о персональных данных (таких как поправки о персональных данных, разрешенных субъектом к распространению, введенные Федеральным законом от 30.12.2020 г. № 519-ФЗ).

³⁷ Апелляционное определение Московского областного суда от 03.06.2019 г. по делу № 33-17997/2019.

³⁸ Апелляционное определение Санкт-Петербургского городского суда от 26.03.2019 г. № 33-4314/2019 по делу № 2-4433/2018.

³⁹ Апелляционное определение Верховного суда Республики Башкортостан от 24.07.2019 г. по делу № 33-14414/2019.

⁴⁰ Апелляционное определение Свердловского областного суда от 22.12.2017 г. по делу № 33а-21308/2017.

Некоторые из выявленных проблем, связанные с отсутствием достаточной определенности или единообразия, по-прежнему остаются. Если принимать во внимание репрезентативные материалы, то речь идет о недостаточной определенности ряда вопросов, касающихся биометрических персональных данных (момент сбора биометрических персональных данных, понятие установления личности как критерий для применения специального правового режима и др.), а также о недостаточной определенности правового режима фактически общедоступных данных в связи с ограничительным толкованием данной категории на уровне правоприменительной практики и новых вопросов, которые возникают в связи с поправками, введенными Федеральным законом от 30.12.2020 г. № 519–ФЗ.

В то же время за сравнительно небольшой промежуток времени наметилась устойчивая тенденция к внимательному рассмотрению правовой проблематики персональных данных, что отличает современный период от периода начала действия Закона о персональных данных.

Список проанализированных судебных решений

1. Апелляционное определение Верховного суда Республики Башкортостан от 24.07.2019 г. по делу № 33-14414/2019.
2. Апелляционное определение Верховного суда Республики Коми от 04.02.2019 по делу №33–640/2019.
3. Апелляционное определение Верховного суда Республики Мордовия от 24.04.2018 по делу № 33а-770/2018.
4. Апелляционное определение Воронежского областного суда от 12.02.2019 г. по делу № 33–789.
5. Апелляционное определение Воронежского областного суда от 30.05.2019 г. по делу № 33–3559.
6. Апелляционное определение Воронежского областного суда от 12.03.2020 г. по делу № 33–1212.
7. Апелляционное определение Московского городского суда от 30.11.2017 г. по делу № 33-40869/2017.
8. Апелляционное определение Московского городского суда от 22.08.2018 по делу № 33-33329/2018.
9. Апелляционное определение Московского городского суда от 12.12.2018 г. по делу № 33-54212/2018.
10. Апелляционное определение Московского городского суда от 30.01.2019 по делу №33а-1238/2019.
11. Определение Московского городского суда от 17.06.2019 № 4га-621/2019.
12. Апелляционное определение Московского городского суда от 30.01.2020 по делу №33а-707/2020, 2а-577/2019.
13. Апелляционное определение Московского городского суда от 06.07.2020 г. по делу № 33-23715/2020.
14. Апелляционное определение Московского областного суда от 03.06.2019 г. по делу № 33-17997/2019.

15. Апелляционное определение Нижегородского областного суда от 19.12.2018 по делу № 33а-15421/2018.
16. Апелляционное определение Нижегородского областного суда от 30.04.2019 г. по делу № 33-4851/2019.
17. Апелляционное определение Новосибирского областного суда от 17.08.2017 по делу № 33-7782/2017.
18. Апелляционное определение Новосибирского областного суда от 12.10.2017 г. по делу № 33-9263/2017.
19. Апелляционное определение Оренбургского областного суда от 20.06.2017 г. по делу № 33-4320/2017.
20. Апелляционное определение Санкт-Петербургского городского суда от 26.03.2019 г. № 33-4314/2019 по делу № 2-4433/2018.
21. Апелляционное определение Санкт-Петербургского городского суда от 29.05.2019 г. № 33-11444/2019 по делу № 2-5365/2018.
22. Апелляционное определение Санкт-Петербургского городского суда от 07.07.2020 №33а-13473/2020 по делу №2а-769/2020.
23. Апелляционное определение Санкт-Петербургского городского суда от 27.02.2020 № 33-648/2020 по делу № 2-1855/2019.
24. Апелляционное определение Свердловского областного суда от 22.12.2017 г. по делу № 33а-21308/2017.
25. Апелляционное определение Свердловского областного суда от 21.08.2018 г. по делу № 33-14121/2018.
26. Кассационное определение Второго кассационного суда общей юрисдикции от 31.07.2020 г. №88а-17020/2020.
27. Определение Верховного Суда РФ от 29.01.2018 № 305-КГ17-21291 по делу № А40-5250/2017.
28. Определение Верховного Суда РФ от 05.03.2018 №307-КГ18-101 по делу № А42-342/2017.
29. Определение Воронежского областного суда от 22.07.2021 г. по делу № 33–4431/2021.
30. Определение Восьмого кассационного суда общей юрисдикции от 19.12.2019 №88–1005/2019.
31. Определение Восьмого кассационного суда общей юрисдикции от 31.01.2020 г. № 16-275/2020.
32. Определение Пятого кассационного суда общей юрисдикции от 28.09.2021 №88–7100/2021.
33. Определение Третьего кассационного суда общей юрисдикции от 15.07.2020 г. по делу № 88-8222/2020.
34. Определение Третьего кассационного суда общей юрисдикции от 01.06.2020 г. № 88-9326/2020.
35. Определение Четвертого кассационного суда общей юрисдикции от 18.02.2020 по делу № 88-5815/2020.
36. Определение Четвертого кассационного суда общей юрисдикции от 25.11.2021 по делу № 88–20323/2021.

37. Определение Четвертого кассационного суда общей юрисдикции от 08.06.2021 по делу № 88–13314/2021.
38. Постановление Арбитражного суда Московского округа от 09.11.2017 г. № Ф05-16382/2017 по делу № А40-5250/2017.
39. Постановление Арбитражного суда Северо-Западного округа от 21.11.2017 №Ф07-11732/2017 по делу №А42-342/2017.
40. Постановление Второго кассационного суда общей юрисдикции от 07.07.2020 г. по делу №16-3770/20.
41. Постановление Девятого арбитражного апелляционного суда от 27.07.2017 г. № 09АП-31744/2017 по делу № А40-5250/17.
42. Постановление Девятого арбитражного апелляционного суда от 06.02.2018 г. по делу № А40–18827/17.
43. Постановление Девятого арбитражного апелляционного суда от 08.07.2021 г. по делу № А40–18827/17.
44. Постановление Конституционного Суда РФ от 25.05.2021 № 22-П «По делу о проверке конституционности пункта 8 части 1 статьи 6 Федерального закона “О персональных данных” в связи с жалобой общества с ограниченной ответственностью “МедРейтинг”».
45. Постановление Мирowego судьи судебного участка № 374 Таганского района г. Москвы от 13.02.2020 г.
46. Постановление Мирowego судьи судебного участка № 422 Таганского района г. Москвы от 05.04.2019 г. по делу № 5–618/19.
47. Постановление Суда по интеллектуальным правам от 24.07.2018 г. по делу № А40–18827/2017.
48. Постановление Четвертого кассационного суда общей юрисдикции от 16.10.2020 №16–894/2020.
49. Решение Арбитражного суда г. Москвы от 05.05.2017 г. по делу № А40-5250/17–155–51.
50. Решение Арбитражного суда г. Москвы от 12.10.2017 г. по делу № А40-18827/17–110–180.
51. Решение Арбитражного суда г. Москвы от 22.03.2021 г. по делу № А40–18827/17–110–180.
52. Решение Кинешемского городского суда Ивановской области от 27.05.2021 по делу №2–873/2021.
53. Решение Кировского районного суда города Саратова от 01.06.2021 по делу №2–2354/2021.
54. Решение Лискинского районного суда Воронежской области от 09.07.2018 №12–35/2018.
55. Решение Санкт-Петербургского городского суда от 29.10.2019 г. № 7-1848/2019 по делу № 12-577/2019.
56. Решение Таганского районного суда г. Москвы от 16.03.2020 г.
57. Решение Щербинского районного суда г. Москвы от 29.10.2021 г. по делу № 2–1328/21.