

Дайджест

Значимые события и инициативы по комплаенсу персональных данных в 2026г.

Актуальность материала: **05.05.2026**

1. Федеральные законы

№	Наименование	Описание	Статус
1.1	Федеральный закон от 28.12.2025 № 508-ФЗ о передаче дел по ст.13.11 КоАП из ведения арбитражных судов в суды общей юрисдикции	Пунктом «б» части 12 статьи 1 Закона предусмотрено, что дела по нарушениям ст.13.11 КоАП больше не будут рассматриваться судьями арбитражных судов, как это было с 30.05.2025 согласно 420-ФЗ.	01.01.2026 - вступает в силу
1.2	Федеральный закон от 29.12.2025 № 575-ФЗ о внесении изменений в законы о рекламе и о регулировании азартных игр	□ Законом создается перечень физических лиц, отказавшихся от участия в азартных играх, который ведется единым регулятором азартных игр. На организаторов азартных игр и некоторых иных лиц накладывается обязанность проверять наличие информации о физическом лице в этом перечне и отказывать в участии в азартных играх, доступу к личному кабинету на сайте организатора азартных игр, либо совершать иные указанные в законе действия. Среди прочего, предусмотрен запрет на направление лицам, включенным в перечень, рекламы организаторами азартных игр или лицами, действующими по их поручению. Для внесения и исключения записей в/из перечень(-ня) человек должен подать заявление с приложенным согласием на обработку персональных данных (СОПД). Формы СОПД, представляемых вместе с заявлениями на внесение/исключение записей, должны быть разработаны ФНС по согласованию с РКН до 29 марта 2026 г. P.S. В связи с принятием закона в Каталог ПД добавлен новый п.105 «сведения об участии (отказе от участия) в азартных играх».	01.09.2026 - вступает в силу
1.3	Федеральный закон от 08.03.2026 № 52-ФЗ об обязательной геномной регистрации военных и правоохранителей	Закон предусматривает обязательную государственную геномную регистрацию для отдельных категорий граждан. Среди них — военные-контрактники, граждане, пребывающие в добровольческих формированиях, и сотрудники органов внутренних дел. В документе отмечается, что данные граждан будут храниться до достижения ими возраста 100 лет.	07.06.2026 - вступает в силу

№	Наименование	Описание	Статус
1.4	New Федеральный закон от 08.03.2026 № 55-ФЗ о новом порядке предоставления органами МВД адресно-справочной информации	□ Внесены изменения в статьи 2 и 3 Закона РФ «О праве граждан Российской Федерации на свободу передвижения, выбор места пребывания и жительства в пределах Российской Федерации». Документ устанавливает новый механизм взаимодействия физических и юридических лиц при поиске граждан через органы МВД. □ До принятия закона органы внутренних дел отказывали в удовлетворении подавляющего большинства запросов о предоставлении контактных данных граждан в связи со строгими требованиями законодательства о защите ПД, запрещающими передачу сведений без согласия субъекта. □ Внедряется процедура оповещения искомого лица, при которой МВД выступает посредником, не раскрывая ПД заявителю: 1□ Заявитель направляет запрос в территориальный орган МВД (в т.ч. через ЕПГУ), указывая свои контактные данные и причину обращения. 2□ Орган МВД устанавливает адрес пребывания/жительства искомого лица и направляет ему почтовое уведомление с контактами инициатора. 3□ Искомое лицо самостоятельно принимает решение о целесообразности обратной связи. Право гражданина на неприкосновенность частной жизни сохраняется в полном объеме. □ В тексте закона официально закреплены и конкретизированы понятия «адресно-справочная информация» и «адресно-справочная работа».	05.09.2026 – вступает в силу

№	Наименование	Описание	Статус
1.5	New Федеральный закон от 02.05.2026 № 130-ФЗ о запрете на использование в агитационных материалах изображений и голоса людей, в том числе вымышленных и умерших	□ Президент РФ подписал закон о совершенствовании избирательного законодательства, предусматривающий, в том числе, запрет на использование в агитационных материалах сгенерированных искусственным интеллектом изображений людей. □ Изменения внесены в законы «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации» и «О выборах депутатов Государственной думы Федерального собрания Российской Федерации». □ Устанавливается запрет на использование в агитационных материалах изображений и голоса людей, в том числе вымышленных и умерших, созданных с применением ИИ. Генерация с помощью нейросетей изображений и голоса допускается только в отношении кандидатов и лиц, давших согласие на использование своих изображений. □ Допускается использование в предвыборной агитации фотографий и голоса граждан РФ старше 18 лет с их письменного согласия. Ранее в агитации разрешалось использовать фотографии только самих кандидатов, в том числе в окружении неопределенного круга лиц. Использовать в агитации изображение или голос лица, аффилированного с иностранным агентом, можно будет только с соответствующим указанием.	02.05.2026 – вступает в силу

2. Акты Президента и Правительства

№	Наименование	Описание	Статус
2.1	Указ Президента ПФ от 26.02.2026 №116 об образовании комиссии при Президенте РФ по развитию технологий ИИ	□ Основная задача комиссии — координировать действия федеральных, региональных органов власти, Банка России и других заинтересованных госорганов для создания, развития и внедрения технологий ИИ. Кроме того: 1□ разработка стратегии для внедрения ИИ; 2□ разработка подходов для адаптации отраслей экономики, социальной сферы и сферы госуправления к активному использованию ИИ; 3□ координация действий по внедрению ИИ в учебный процесс «в целях формирования гармонично развитой личности»; 4□ подготовка педагогов и специалистов в области ИИ; 5□ подготовка предложений по развитию международного сотрудничества в области ИИ и другие. □ В состав комиссии также вошли глава Минобороны России Андрей Белоусов, губернатор Московской области Андрей Воробьев, глава Сбербанка Герман Греф, спецпредставитель президента по вопросам цифрового и технологического развития Дмитрий Песков, глава Минцифры Максуд Шадаев.	26.02.2026 – вступает в силу

№	Наименование	Описание	Статус
2.2	Постановление Правительства РФ от 27.11.2025 № 1912 о новых правилах предоставления гостиничных услуг	1□ В случае отсутствия паспорта РФ (или иных основных документов, удостоверяющих личность), допускается заселение граждан РФ по предъявлении российского национального водительского удостоверения. Водительское удостоверение официально закреплено как альтернативный материальный носитель для верификации личности в гостиничном секторе. 2□ Вводится правовое основание для использования цифровых способов подтверждения личности при заселении: □ЕБС: Идентификация и/или аутентификация может проводиться с использованием Единой биометрической системы. □Госуслуги: Допускается использование мобильного приложения ФГИС «Единый портал государственных и муниципальных услуг». 3□ Регламентированы условия заселения несовершеннолетних, требующие внимания к сбору согласий законных представителей: □Малолетние до 14 лет: Заселение возможно только с родителями или сопровождающими лицами. Сопровождающие обязаны предоставить согласие родителей (законных представителей). □Несовершеннолетние от 14 лет: Могут заселяться самостоятельно при наличии документа, удостоверяющего личность, и согласия родителей (законных представителей). □При заселении с сопровождающими (не родителями) также требуется согласие законных представителей. □Для несовершеннолетних также предусмотрена возможность идентификации через ЕБС или Госуслуги (при наличии соответствующих согласий и технических возможностей). 4□ Процедуры передачи данных в органы регистрационного учета (МВД) остаются привязанными к действующим Правилам регистрации граждан РФ (ПП РФ № 713) и миграционного учета иностранцев (ПП РФ № 9). Новые правила лишь уточняют способы сбора первичных данных для этих процессов.	01.03.2026 – вступает в силу
2.3	Распоряжение Правительства Российской Федерации от 06.03.2026 № 435-р об утверждении состава подкомиссии по развитию ИИ и автономных систем	Утверждён состав подкомиссии по развитию и внедрению технологий искусственного интеллекта, в том числе автономных систем искусственного интеллекта, правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности.	06.03.2026 – вступает в силу

3. Ведомственные и иные акты

№	Наименование	Описание	Статус
3.1	Письмо Минцифры России от 29.12.2025 №П12-130083 по вопросам массовых и (или) автоматических телефонных вызовов (далее - массовые вызовы), а также маркировки вызовов	Определение критериев массовых вызовов осуществляется операторами связи самостоятельно, а Правительства РФ или Минцифры такими полномочиями не наделены. Согласие на массовые вызовы должно получаться до совершения самого вызова, однозначно идентифицировать абонента и устанавливать его волеизъявление, а специальных требований к такому согласию не предусмотрено. Оператор связи вправе блокировать массовые вызовы, совершаемые с нарушением требований законодательства. Выборочный отказ абонента от массовых вызовов невозможен, т.е. не предполагает выбора категории и (или) инициатора вызова. Договор о совершении массовых вызовов и договор об оказании услуг телефонной связи – это разные документы. Для оператора связи, в сети которого начинается вызов от компании/ИП, пока нет ответственности за нарушение требований к маркировке этих звонков.	29.12.2025 - опубликовано
3.2	План обязательных профилактических визитов Роскомнадзора в отношении обработки персональных данных в 2026г. (утв. приказом Роскомнадзора от 19.12.2025 №390)	Общее число профилируемых операторов составляет 1156 организаций/ИП, и включает как крупные компании, так и многочисленные государственные учреждения, школы и медицинские центры. Например, в Москве и МО к профвизиту стоит подготовиться 65 операторам. Распознанная текстовая версия плана.	10.01.2026 - опубликован

№	Наименование	Описание	Статус
3.3	Приказ Минцифры России от 03.03.2026 № 173 о методических рекомендациях для подготовки требования о предоставлении обезличенных ПД в НСУД	□ Документ утверждает методические рекомендации, которые определяют, как именно Министерство цифрового развития (Минцифры) должно готовить и направлять операторам запросы (требования) на предоставление обезличенных персональных данных в ГИС «Единая информационная платформа национальной системы управления данными» (ЕИП НСУД). □ Согласно приказу, для подготовки требования о предоставлении обезличенных данных Минцифры может направить запросы пользователям интересующих министерство составов данных; также Минцифры вправе привлекать подведомственное ему учреждение, выполняющее работы по сопровождению подсистемы обработки обезличенных данных (ПООД) ЕИП НСУД. □ Этот приказ принят в рамках реализации новых законодательных норм (ст. 13.1 закона № 152-ФЗ), согласно которым государство формирует централизованные массивы (датасеты) обезличенных персональных данных для их последующего использования (например, для развития технологий искусственного интеллекта и проведения исследований), а бизнес обязан такие данные по запросу Минцифры предоставлять.	03.03.2026 – вступает в силу

№	Наименование	Описание	Статус
3.4	ГОСТ Р 72514-2026 «Искусственный интеллект. Оценка воздействия системы искусственного интеллекта»	Этот стандарт — руководство по созданию прозрачных и заслуживающих доверия систем. Он представляет собой модифицированную версию международного стандарта ISO/IEC 42005:2025, адаптированную под российские реалии и технологии. Что внутри? Оценка воздействия (AI system impact assessment) теперь определяется как задокументированный процесс выявления и оценки влияния ИИ на людей и социальные группы. Стандарт устанавливает, как и когда проводить такие оценки на разных стадиях жизни системы — от проектирования до развертывания. Процесс должен быть бесшовно встроен в общую систему менеджмента ИИ (ГОСТ Р ИСО/МЭК 42001) и управление рисками организации. Особое внимание уделяется «высокорисковому» (sensitive use) и «ограниченному» использованию систем, которые могут оказать значительное влияние на права человека или финансовое положение. Стандарт требует детального документирования: - Качества данных (включая проверку на нежелательную предвзятость). - Параметров алгоритмов и моделей. - Среды развертывания, включая географический и культурный контекст. - Таксономии вреда и пользы: от прозрачности и объяснимости до экологической устойчивости. Стандарт актуален для любых организаций, которые разрабатывают или используют ИИ, независимо от их масштаба. Внедрение этого стандарта помогает не только соблюдать требования, но и управлять ожиданиями заинтересованных сторон.	01.05.2026 – вступает в силу

4. Проекты федеральных законов

№	Наименование	Описание	Статус
4.1	Законопроект о противодействии навязчивому преследованию	Предлагается закрепить понятие навязчивого преследования как действий, причиняющих психические страдания и вызывающих опасения за безопасность (даже после просьбы прекратить). К таким действиям отнесут систематическую слежку, попытки установить контакт (звонки, СМС, подарки) и использование персональных данных для заказа товаров или услуг.	24.12.2025 - внесен в Госдуму

№	Наименование	Описание	Статус
4.2	Законопроект о втором пакете мер по противодействию телефонному и кибермошенничеству («Антифрод-2»)	Статья 5 законопроекта про изменения в 152-ФЗ «О персональных данных»: - Точечная правка ст. 10 (про специальные категории ПД): в ч. 3 уточняется формулировка — речь прямо про «обработку специальных категорий». - Добавляется новая ч. 3¹ ст. 10: допускается обработка спецкатегорий ПД об участии граждан РФ в СВО и/или КТО, а также о принадлежности к их семьям — гос/муниципальными органами в пределах полномочий и иными лицами в случаях и порядке, определяемых федеральными законами. Статья 4 законопроекта про изменения в 149-ФЗ «Об информации, ИТ и о защите информации»: - Добавляется норма, что Правительство РФ может установить случаи, когда при авторизации по адресу электронной почты такой адрес должен быть создан с использованием доменных имён, входящих в группы доменных имён, составляющих российскую национальную доменную зону. - Вводится требование подтверждать совершение в интернете «значимых действий» (перечень утверждает Правительство): подтверждение идёт кодом из SMS + кодом/сообщением через МАХ, отправляемыми владельцем ресурса (российское ЮЛ/гражданин РФ, деятельность в РФ). Для банков/финрынка перечень дополнительно согласуется с ЦБ. - Запрет на распространение «вводящей в заблуждение» информации: под видом достоверных сообщений, создающей угрозу имущественного ущерба и/или неправомерного доступа к ПД/иной информации пользователя (вводится как отдельная категория). Статья 8 законопроекта про изменения в 572-ФЗ (про идентификацию/аутентификацию с биометрией, ЕБС и др.): - В ст. 4 добавляются ч. 18-19: если доступ к учётной записи в ЕСИА ограничен (в т.ч. из-за выявленного несанкционированного доступа), восстановить доступ можно одним из перечисленных способов: ЕБС; сайт/мобильное приложение банка; УКЭП; МАХ; МФЦ; органы/организации, имеющие право выдавать ключи ПЭП для гос/мунуслуг. 09.02.2026: Минцифры предложило смягчить запрет на входящие международные звонки	09.02.2026 - принят в первом чтении
4.3	Законопроект о разрешении получать данные владельцев земли для решения споров	Предлагается внести изменения в Гражданский процессуальный кодекс РФ. Так, по делам об установлении границ земельных участков, об исправлении ошибок в едином государственном реестре недвижимости и по другим аналогичным спорам информация о владельце участка будет предоставляться по запросу суда органами Фонда пенсионного и социального страхования, налоговыми или органами внутренних дел, а также ППК «Роскадастр».	26.12.2025 - внесен в Госдуму
4.4	Законопроект о внесении изменений в статьи 137 и 138 УК РФ	Предлагается создать более жесткие и детализированные правовые инструменты для борьбы с нарушениями требований безопасности персональных данных и неприкосновенности частной жизни. «Статьи 137 и 138 Уголовного кодекса дополняются в части квалифицирующих признаков состава преступления. Статьи о нарушении неприкосновенности частной жизни и нарушении тайны переписки, телефонных переговоров дополняются субъектами, которые действовали из корыстной заинтересованности или группой лиц по предварительному сговору, организованной группой. Ранее речь шла только о лицах, совершивших преступление с использованием служебного положения», - отметил председатель правления Ассоциации юристов России (АЮР) Владимир Груздев. Он рассказал, что в Уголовном кодексе также появится новый состав - нарушение требований к оказанию услуг подвижной радиотелефонной связи иностранному лицу и лицу без гражданства лицом, подвергнутым административному наказанию.	14.01.2026 - публикация в СМИ
4.5	Законопроект об обязательном информировании абонентов об автоматизированных вызовах	Предлагается дополнить ст. 44.1-1 Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи» правилом для заказчиков массовых вызовов или операторов связи – обязательно информировать абонентов о характере массовых и (или) автоматизированных вызовов в самом начале разговора. Речь идёт о массовых вызовах с использованием синтезированной речи, автоматизированной записи, голосового робота или иных автоматизированных средств без участия человека. Парламентарии в пояснительной записке отметили, что сейчас доверие граждан к телефонным коммуникациям снижается из-за отсутствия такого обязательного уведомления. Эта ситуация создает риски недобросовестного использования данных абонентов и затрудняет осознанное взаимодействие.	20.01.2026 - внесен в Госдуму

№	Наименование	Описание	Статус
4.6	Законопроект об обработке биометрии лиц, содержащихся в СИЗО	Минюст России разработал законопроект, который позволит обрабатывать биометрические данные подозреваемых, обвиняемых и осужденных без их согласия, соответствующий документ размещен на портале проектов нормативных правовых актов. «Обработка биометрических персональных данных подозреваемых и обвиняемых. Обработка сведений, которые характеризуют физиологические и биологические особенности подозреваемых и обвиняемых в местах содержания под стражей, может осуществляться администрацией места содержания под стражей для установления их личности без согласия субъекта персональных данных», - говорится в законопроекте. Предполагается, что обработка биометрии указанных категорий лиц применяется в целях обеспечения безопасности на объектах органов и учреждений уголовно-исполнительной системы.	22.01.2026 – опубликован на федеральном портале проектов нормативных правовых актов
4.7	Законопроект о корректировке правил доступа на объекты (СКУД) с использованием биометрии	Минцифры предложило упростить использование биометрии на контрольно-пропускных пунктах госорганов, ЦБ, госкорпораций и предприятий оборонно-промышленного, атомного и топливно-энергетического комплексов. Организация сможет сохранять цифровые векторы сотрудников во внутренней информационной системе и сверять данные желающих войти на территорию предприятия с ними, не обращаясь каждый раз к государственной единой биометрической системе (ЕБС). Жесткие требования сохраняются только для идентификации (установления личности) — она по-прежнему только через ЕБС. А вот для аутентификации (подтверждения личности на проходной) вводятся послабления. Сейчас каждый проход сотрудника стоит денег (запрос в ЕБС). Законопроект разрешает аккредитованным организациям (госорганам, ЦБ, госкорпорациям) использовать векторы ЕБС (математические шаблоны) в своих локальных системах.	24.01.2026 - внесен в Госдуму
4.8	Законопроект о дополнении ст.272.1 УК РФ понятием «автоматизированная обработка»	Согласно статье 272.1 Уголовного кодекса, сейчас ответственность наступает за незаконные использование или передачу (распространение, предоставление, доступ), сбор или хранение компьютерной информации с персональными данными, если они были получены в результате взлома или иного незаконного доступа. Группа депутатов фракции «Справедливая Россия» во главе с ее руководителем Сергеем Мироновым предложили внести в ч.1 ст.272.1 УК РФ понятие «автоматизированная обработка» как преступное деяние, благодаря чему к ответственности можно будет привлечь за сам факт незаконной алгоритмической обработки чужих персональных данных — даже если они не были впоследствии распространены или сохранены. Авторы инициативы указали, что термин «автоматизированная обработка» является законодательно устоявшимся и согласуется с понятийным аппаратом Закона «О персональных данных», что гарантирует единство правового пространства и корректное применение уголовно-правовой нормы.	06.02.2026 - возвращен инициаторам для устранения недостатков
4.9	Законопроект о противодействии stalkingу	Авторы инициативы предлагают установить отдельный федеральный закон «О противодействии навязчивому преследованию». Законопроектом вводятся понятия «навязчивое преследование», «охранный ордер», «преследователь», «лицо, подвергнутое навязчивому преследованию». Под определением навязчивое преследование понимается систематическая слежка, попытки контакта, отправка подарков, использование персональных данных жертвы для заказов, корреспонденции. Сейчас в КоАП РФ нет отдельной статьи о навязчивом преследовании, а действующие положения не охватывают всех форм stalkingа и позволяют вводить запрет на приближение только в рамках уголовного дела. Предлагается ввести механизм охранных ордеров – они установят для stalkера запрет на приближение к жертве, на контакты с ней и пр. Преследователя могут привлечь к уголовной ответственности за продолжение stalkingа.	04.02.2026 - внесен в Госдуму

№	Наименование	Описание	Статус
4.10	Законопроект о создании полигона для тестирования ИИ-систем на безопасность	□ Для систем искусственного интеллекта (ИИ) высокого и критического уровня риска потребуется получить сертификат на соответствие требованиям безопасности Федеральной службы по техническому и экспертному контролю (ФСТЭК) и Федеральной службы безопасности (ФСБ). Это следует из законопроекта правительства «О применении систем искусственного интеллекта органами, входящими в единую систему публичной власти, и внесении изменений в отдельные законодательные акты». □ Тестирование на соответствие ИИ-систем этим требованиям будет проходить на специальном полигоне, созданном Минцифры. Если тестирование пройдет успешно, системы будут допущены к использованию на объектах критической информационной инфраструктуры (к ней относятся сети связи и информационные системы госорганов, энергетических, транспортных, финансовых, телекоммуникационных и ряда других компаний). □ Новый законопроект вводит четыре уровня критичности ИИ-систем: 1 □ минимальный, когда системы не оказывают существенного влияния на права и безопасность (например, рекомендательные системы); 2 □ ограниченный, когда системы должны сообщать пользователям о том, что они работают с нейросетью; 3 □ высокий, когда системы используются на объектах критической информационной инфраструктуры; 4 □ критический, когда системы угрожают жизни или здоровью человека, безопасности государства, а также разработки, способные к принятию решений без вмешательства человека. □ Определять уровень критичности той или иной системы будет новая структура — Национальный центр искусственного интеллекта в сфере госуправления при правительстве. Также центр будет вести реестр допущенных к критической информационной инфраструктуре систем. Требования для получения обязательного сертификата ФСБ и ФСТЭК для критических и ИИ-систем с высоким уровнем будут установлены позже отдельным документом. Одним из них станет наличие ИИ-системы в реестре российского или евразийского софта.	10.02.2026 - публикация в СМИ
4.11	Законопроект об ужесточении мер защиты генетических данных россиян	□ Передачу генетических данных россиян за границу планируется ограничить для обеспечения их сохранности и защиты. Такую инициативу Министерства науки и высшего образования одобрила правительственная комиссия по законопроектной деятельности. Законопроект предлагает распространить действие закона о государственном регулировании в области генно-инженерной деятельности на сферу обращения генетических данных человека. □ В случае принятия инициатива вступит в силу с 1 сентября 2026 г. В тексте законопроекта указано, что передача генетических данных за рубеж допускается исключительно в целях оказания медицинской помощи российским гражданам, разработки для них лекарств и биомедицинских продуктов, а также в рамках международного сотрудничества в сферах здравоохранения и биологической безопасности. Представлять генетическую информацию будет возможно как в натуральной, так и в цифровой форме. □ Порядок и условия передачи генетических данных за пределы России будет определять правительство, сказано в тексте законопроекта. Оно также будет устанавливать требования к физическим лицам и организациям, осуществляющим такую передачу. Минобрнауки также предусмотрело запрет на передачу иностранным физическим и юридическим лицам результатов популяционных генетических и иммунологических исследований. Под это определение подпадают любые действия, в результате которых информация становится доступной иностранцам как на территории России, так и за ее пределами. В частности, передачей генетических данных будет считаться их пересылка, распространение и размещение в интернете, а также предоставление доступа к ним.	13.02.2026 - принят в первом чтении

№	Наименование	Описание	Статус
4.12	Законопроект об изменениях в законодательстве РФ о выборах и референдумах	□ Передачу генетических данных россиян за границу планируется ограничить для обеспечения их сохранности и защиты. Такую инициативу Министерства науки и высшего образования одобрила правительственная комиссия по законопроектной деятельности. Законопроект предлагает распространить действие закона о государственном регулировании в области генно-инженерной деятельности на сферу обращения генетических данных человека. □ В случае принятия инициатива вступит в силу с 1 сентября 2026 г. В тексте законопроекта указано, что передача генетических данных за рубеж допускается исключительно в целях оказания медицинской помощи российским гражданам, разработки для них лекарств и биомедицинских продуктов, а также в рамках международного сотрудничества в сферах здравоохранения и биологической безопасности. Представлять генетическую информацию будет возможно как в натуральной, так и в цифровой форме. □ Порядок и условия передачи генетических данных за пределы России будет определять правительство, сказано в тексте законопроекта. Оно также будет устанавливать требования к физическим лицам и организациям, осуществляющим такую передачу. Минобрнауки также предусмотрело запрет на передачу иностранным физическим и юридическим лицам результатов популяционных генетических и иммунологических исследований. Под это определение подпадают любые действия, в результате которых информация становится доступной иностранцам как на территории России, так и за ее пределами. В частности, передачей генетических данных будет считаться их пересылка, распространение и размещение в интернете, а также предоставление доступа к ним.	19.02.2026 - внесен в Госдуму

№	Наименование	Описание	Статус
4.13	Законопроект о регулировании технологий ИИ	Впервые на уровне федерального закона закрепляются понятия: модель ИИ, система ИИ, сервис ИИ, большие фундаментальные модели, доверенные модели, а также — «эксплуатация уязвимостей человека». Выстраивается чёткая цепочка субъектов: разработчик → оператор → владелец сервиса → пользователь. Каждому — свои обязанности и своя мера ответственности. Одна из отличительных черт — концепция «суверенных» и «национальных» больших фундаментальных моделей. Разработка, обучение и эксплуатация — на территории РФ, силами российских граждан и юрлиц, на российских данных. Государство берёт на себя обязательство создавать благоприятные условия для их развития. Для госсистем и критической инфраструктуры вводится реестр доверенных моделей ИИ. Попасть в него можно при подтверждении требований по безопасности и качеству. По сути — формируется контур «допуска» ИИ к чувствительным сферам. Закон фиксирует несколько важных гарантий: - уведомление о том, что решение принимает ИИ, а не человек - право отказаться от взаимодействия с ИИ и получить услугу «по-человечески» - досудебное обжалование решений, принятых с помощью ИИ - право на компенсацию вреда В статье 4 (общие принципы) персональные данные и неприкосновенность частной жизни упоминаются как часть принципа верховенства прав человека. Также в статье 5 указано, что при регулировании ИИ учитывается «категория обрабатываемой информации» — общедоступная или ограниченного доступа. Отдельной статьи о защите персональных данных при обучении моделей, о правилах обработки данных пользователей сервисов ИИ, о праве на удаление данных из датасетов или об ограничениях профилирования — в тексте нет. Синтезированный контент (аудио, визуал, иное) должен содержать предупреждение — и в человекочитаемом, и в машиночитаемом формате. Платформы с аудиторией 100K+ обязаны проверять наличие маркировки и удалять немаркированный AI-контент. При этом по договору с пользователем можно отказаться от «видимой» маркировки — но машиночитаемая остаётся. Каждый субъект отвечает соразмерно степени вины. Разработчик, оператор и владелец сервиса могут быть освобождены от ответственности, если докажут, что предприняли исчерпывающие меры. Пользователь отвечает за умышленное использование ИИ в противоправных целях. Предусмотрено и регрессное требование оператора к разработчику. Результаты, созданные с помощью ИИ, охраняются по ГК РФ — при соответствии критериям охраноспособности. Отдельно закреплено: извлечение информации из защищённых объектов для создания датасетов и обучения ИИ — не является нарушением авторских и патентных прав (при правомерном доступе к материалу). Для центров обработки данных, включённых в специальный перечень, предусмотрены: приоритетное подключение к электросетям, сниженные тарифы, налоговые льготы, долгосрочные контракты на энергию и инфраструктурная поддержка. Фактически — режим «зелёного коридора» для вычислительной базы ИИ. Отдельные статьи посвящены международному сотрудничеству: формирование «единого пространства доверенных технологий», продвижение российских подходов к оценке ИИ, экспорт технологий, совместные исследования и образовательные программы. Закон вступает в силу 1 сентября 2027, а многие конкретные требования будут определяться подзаконными актами Правительства. По сути, закон задаёт архитектуру: кто за что отвечает, где границы допустимого, и как государство намерено поддерживать развитие ИИ. 27.04.2026 законопроект был обновлен: (1) убраны требования к наборам данных, которые используются для обучения моделей; (2) исключены требования о разработке и обучении суверенных и национальных моделей ИИ исключительно гражданами России - теперь достаточно, чтобы разработчиком было российское юрлицо; (3) снято требование для сервиса с аудиторией более 500 000 пользователей регистрироваться в качестве организатора распространения информации (ОРИ)	18.02.2026 - опубликован на федеральном портале проектов нормативных правовых актов
4.14	Законопроект о доступе Минобороны к реестру ЗАГС	Законопроект предполагает предоставление Минобороны России доступа к данным из единого реестра ЗАГС и предусматривает, что Минобороны сможет в электронном виде получать сведения о военнослужащих, гражданском персонале, уволенных с военной службы, а также о членах их семей. Как поясняют авторы инициативы, это позволит упростить предоставление социальных гарантий и компенсаций, а также улучшить ведение воинского учета.	23.03.2026 - внесен в Госдуму

№	Наименование	Описание	Статус
4.15	Законопроект о гарантиях цифровых прав россиян	Депутаты от ЛДПР разработали законопроект, которым предлагается закрепить право граждан на доступ к интернету, свободу выражения мнений в сети, выбор способов общения и защиту персональных данных. Инициатива подготовлена в ответ на обращения граждан, обеспокоенных ограничениями в работе интернета и связи. «ЛДПР подготовила законопроект «О гарантиях цифровых прав граждан России», в него вошли положения о доступе к информации: о праве каждого на доступ к интернету; о свободе выражения мнений в интернете; о свободе выбора способа общения в интернете; о конфиденциальности и защите данных и другие. В ближайшее время совместно с профессиональными сообществами и экспертами мы доработаем эту инициативу», - сообщил лидер партии Леонид Слуцкий. Он отметил, что первые обсуждения законопроекта пройдут в Госдуме. К работе будут приглашены профильные сообщества, эксперты и представители бизнеса. «Наши депутаты проведут обсуждения на базе региональных законодательных собраний», - заключил парламентарий.	23.03.2026 - публикация в СМИ
4.16	Законопроект о наказании за дипфейки	Сенатор Владимир Кожин в середине марта направил в аппарат правительства законопроект о введении штрафов и уголовной ответственности за создание дипфейков. Проект предлагает поправки в закон «Об информации, информационных технологиях и защите информации», которые ограничивают создание и использование недостоверного изображения, видеозаписи и записи голоса граждан, то есть дипфейков. Без участия гражданина создание дипфейков, их хранение, распространение или организация доступа к ним будут запрещены, за исключением ряда случаев. Предлагается штрафовать от 500 тысяч рублей за подделки фото-, видео- или аудиоматериалов при помощи нейросетей; за те же дипфейки с участием представителей власти, министров или губернаторов лишать свободы на срок от трёх до семи лет.	30.03.2026 - публикация в СМИ
8.1	Законопроект о годовом запрете на перепродажу телефонного номера	Группа депутатов думской фракции КПрФ внесла в ГД законопроект, которым предлагается ввести запрет на предоставление оператором связи номера телефона новому владельцу в течение года после расторжения договора с его предыдущим владельцем. Изменения предлагается внести в федеральный закон «О связи». В настоящее время срок выделения новому владельцу номера телефона регулируется только внутренними правилами оператора. «В случае расторжения договора об оказании услуг подвижной радиотелефонной связи, оператор связи имеет право выделять абонентский номер, который ранее был в употреблении, иным лицам не ранее чем по истечении 1 года с момента расторжения договора», - говорится в тексте проекта закона. По мнению авторов проекта, в настоящее время перепродажа абонентских номеров операторами связи после расторжения договора с предыдущими владельцами создает риски возможной утечки персональных данных бывших владельцев номеров, мошеннические действия с использованием старых номеров, недовольство новых абонентов при получении номеров с негативной историей, а также сложности в идентификации личности при использовании государственных сервисов.	10.04.2026 - внесен в Госдуму
4.17	New		
4.18	New Законопроект о расширении круга лиц, дающих согласие на обработку персональных данных умерших	На текущий момент сложилось противоречие между двумя федеральными законами: - Согласно закону «О персональных данных», согласие на их обработку после смерти гражданина могут давать только его наследники (если иное не было указано при жизни). - Закон «О погребении и похоронном деле» позволяет брать на себя обязанности по захоронению не только родственникам, но и иным лицам, фактически взявшим на себя эту ответственность. - В результате ритуальные службы зачастую отказывают таким лицам в оформлении необходимых документов, так как без статуса наследника они не имеют юридического права давать согласие на обработку данных покойного. Предлагается разрешить предоставлять согласие на обработку ПД лицам, взявшим на себя обязанность по погребению (даже если они не являются наследниками). Такие полномочия предлагается давать исключительно для совершения действий, связанных с организацией похорон, во избежание злоупотреблений. Правительство РФ, рассмотрев документ, назвало предлагаемые изменения избыточными — перечень лиц в законопроекте не полностью совпадает с перечнем лиц, которым по закону о погребении уже обеспечиваются государственные гарантии (супруги, родственники, законные представители и иные лица).	внесен в Госдуму

№	Наименование	Описание	Статус
4.19	^{New} Законопроект о создании единого федерального реестра домашних животных	- Создание Единого реестра домашних животных, который объединит существующие региональные базы данных, что исключит необходимость повторной регистрации питомца при переезде в другой субъект РФ. - Установление требования по обязательной идентификации (маркированию) и регистрации животных в государственной информационной системе. - Наделение Правительства правом определять перечень видов животных, подлежащих учету, а также устанавливать порядок, сроки и состав сведений, вносимых в реестр. - В контексте интприватности: реестр будет содержать сведения, идентифицирующие владельцев животных, что усилит риски неконтролируемого обмена ПД и потребует проработки модели взаимодействия операторов реестра с физическими лицами.	внесен в Госдуму

5. Проекты постановлений Правительства

№	Наименование	Описание	Статус
5.1	Проект постановления Правительства РФ о биометрической регистрации на авиарейс и посадку в самолет	- Упрощенный способ идентификации и аутентификации пассажиров планируют протестировать на внутрироссийских маршрутах. Минцифры России подготовило проект о проведении соответствующего эксперимента. - Речь идет о возможности использования биометрических персональных данных: при регистрации на рейс, в также для допуска пассажиров в перевозочный сектор зоны транспортной безопасности аэропорта и выхода на посадку на борт воздушного судна гражданской авиации. - Участниками эксперимента станут, в частности, международные аэропорты Пулково в Санкт-Петербурге и Шереметьево в Москве. Другие авиаперевозчики и аэропорты могут присоединиться к эксперименту на добровольной основе. Тестирование пройдет в период с 1 июня 2026-го по 1 декабря 2027 года. По итогам его проведения будут подготовлены предложения по развитию и масштабированию применения технологии идентификации и аутентификации пассажиров с использованием биометрии.	04.01.2026 – опубликован на федеральном портале проектов нормативных правовых актов

№	Наименование	Описание	Статус
5.2	Проект изменений в постановления Правительства РФ о праве подтверждать биометрию в салонах связи	□Минцифры предложило дать мобильным операторам право подтверждать биометрию и аккаунты россиян на «Госуслугах» в салонах связи. Это следует из проекта постановления ведомства. Сейчас подтверждать учетную запись и данные в Единой биометрической системе можно онлайн в банках-партнерах либо очно — в МФЦ или в отделениях банков. □Цель изменений — «повышение доступности услуг и сервисов для физических лиц на основе биометрических персональных данных, развитие инфраструктуры цифровой идентификации и создание дополнительных точек обслуживания физических лиц в рамках биометрических сервисов», указано в пояснительной записке. □Подтверждать биометрию и аккаунт на «Госуслугах» нужно для доступа к более широкому функционалу, пояснили в Минцифры. Без подтверждения биометрии можно будет, например, оплатить покупки на кассе или проезд в метро, а удаленно открыть счет в банке — нет.	02.04.2026 – опубликован на федеральном портале проектов нормативных правовых актов

6. Проекты ведомственных и иных актов

№	Наименование	Описание	Статус
6.1	Проект приказа Россельхознадзора об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных	Документ подготовлен в соответствии с ч.5 ст.19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» для определения угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных Россельхознадзора, эксплуатируемых при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки.	29.12.2025 – опубликован на федеральном портале проектов нормативных правовых актов
6.2	Проект методического документа ФСТЭК России «Мероприятия и меры по защите информации, содержащейся в информационных системах»	Документ распространяется на госорганы, госучреждения и организации, являющиеся субъектами КИИ, а также иные организации, попадающие под данные требования (например, в рамках Указа № 250). Требования к защите обычных ИСПД де-факто подтягиваются до уровня значимых объектов КИИ. Операторам придется перестраивать процессы (особенно DevSecOps) и закупать специализированные средства защиты (песочницы, WAF, сканеры контейнеров).	06.02.2026 – опубликован на портале ФСТЭК России

№	Наименование	Описание	Статус
6.3	Проект приказа Минцифры о порядке обработки биометрических персональных данных	В Минцифры считают, что текущий сценарий регистрации биометрических данных в Единой биометрической системе (ЕБС) не учитывает людей с врожденными или приобретенными особенностями лица (например, из-за травм, операций) и речевой функции (включая нарушения дикции, немоту или последствия инсульта). В связи с этим в приказе о порядке обработки биометрических персональных данных предлагается закрепить требования к биометрическим образцам людей с врожденными или приобретенными деформациями, аномалиями развития и последствиями травм лица. Также предлагается сократить время записи голоса с 30 до 10 секунд. Для таких образцов введут специальную метку при регистрации биометрии. Кроме того, проект приказа предоставляет возможность гражданам размещать в ЕБС любые биометрические данные, включая фотографии и записи голоса, либо отдельные их виды. Это разрешат сделать независимо от способа сбора биометрии в системе.	18.03.2026 - опубликован на федеральном портале проектов нормативных правовых актов

7. Правоприменительная практика

№	Наименование	Описание	Статус
7.1	Ответ ЦА Роскомнадзора об обработке персональных данных для фармаконадзора в рамках «Правил надлежащей практики фармаконадзора Евразийского экономического союза» от 03.11.2016 г. №87	Вопрос: Будет ли правомерной обработка ПД, осуществляемая фармацевтическими компаниями в рамках фармаконадзора, в случаях и в порядке, предусмотренном п.п. 382-406 «Правил надлежащей практики фармаконадзора Евразийского экономического союза» от 03.11.2016 г. №87 - при условии соблюдения требований 152-ФЗ «О ПД» и 61-ФЗ «Об обращении лекарственных средств»? Роскомнадзор: Обработка фармацевтическими компаниями ПД во исполнение федеральных законов, подзаконных актов, а также Правил надлежащей практики фармаконадзора ЕАЭС от 03.11.2016 №87 подпадает под правовые основания, предусмотренные п. 2 ч. 1 ст. 6 152-ФЗ «О ПД» и не требует получения согласия субъекта ПД в письменной форме. В случае осуществления фармацевтическими компаниями деятельности по сбору, учету, обработке, анализу и хранению сообщений о нежелательных реакциях с привлечением третьих лиц (колл-центры, поставщики ИТ-систем), указанная деятельность подлежит оформлению в соответствии с ч. 3 ст. 6 152-ФЗ «О ПД».	25.11.2025 - опубликован Privacy Advocates

№	Наименование	Описание	Статус
7.2	По данным МВД, за десять месяцев 2025 года по ст.272.1 УК РФ зарегистрировано 923 преступления	□Власти сообщали об успешном применении ст.272.1 УК РФ против администраторов ботов: в начале года прекратил работу крупный бот «Глаз Бога», а в ноябре был арестован Игорь Морозкин — владелец сервиса Userbox. □К ответственности по статье 272.1 начали привлекать не только владельцев ботов. Например, в марте 2025 года в Кировской области сотрудника салона связи задержали за передачу через мессенджер нескольких десятков записей с персональными данными. В том же месяце в Кировске 20-летнего работника салона сотовой связи обвинили в передаче персональных данных певца Shaman (Ярослав Дронов) и других абонентов. В ноябре по той же статье в Башкирии задержали 38-летнего мужчину, который с помощью спецоборудования активировал тысячи сим-карт, а суд отправил под домашний арест начальницу отдела судебных приставов в одном из районов Перми Надежду Шабунину.	15.01.2026 - публикация в СМИ

№	Наименование	Описание	Статус
7.3	Арбитражный суд Москвы: ФИО и адрес пользователя, оставившего отзыв, могут не быть персональными данными	ИП обратился в суд с заявлением об оспаривании отказа Управления Роскомнадзора по ЦФО в возбуждении дела об административном правонарушении в отношении ООО «ВебСайтСофт». Заявитель утверждал, что на сайте Otvovik.com, администрируемом ООО «ВебСайтСофт», был размещен отзыв, содержащий его персональные данные и порочащие сведения. Суд установил, что ФИО в спорной публикации были частично скрыты символами (звездочками), что делает невозможной идентификацию конкретного физического лица. Также суд выяснил, что указанный в отзыве адрес относится к складским помещениям в Москве, тогда как заявитель зарегистрирован в Туле, следовательно, адрес не является его персональными данными. Дополнительно было отмечено, что заявитель не предоставил доказательств, подтверждающих его отношение к компании «Роботоп», о которой шла речь в отзыве. ООО «ВебСайтСофт» выступает информационным посредником (т.е. не является СМИ или соцсетью с аудиторией более 500 тыс./сутки - см. ст.10.6 149-ФЗ) и не несет ответственности за информацию, размещенную третьими лицами, без знания о ее незаконности (см. Постановление Конституционного Суда РФ от 09.07.2013 № 18-П). Ответственность посредника наступает только когда он узнал или должен был узнать о нарушении (получил претензию или запрос Роскомнадзора) и бездействовал. Суд пришел к выводу, что Роскомнадзор правомерно отказал в возбуждении дела в связи с отсутствием состава и события административного правонарушения по ст. 13.11 КоАП РФ. В удовлетворении заявленных требований ИП было отказано в полном объеме.	Решение от 07.11.2025г. по делу №А40-236948

№	Наименование	Описание	Статус
7.4	Безруков взыскал с белгородки 200 тысяч компенсации за продажу масок с его портретом	Хамовнический райсуд Москвы частично удовлетворил иск актера Сергея Безрукова к белгородской индивидуальной предпринимательнице, которая продавала на маркетплейсах Wildberries и Ozon карнавальные и тканевые маски с изображением лица артиста. Суд обязал белгородку удалить из объявлений о продаже персональные данные господина Безрукова (его имя, фамилию и изображение), а также взыскал с предпринимательницы 200 тыс. руб. в качестве компенсации морального вреда. «Обнаружив свои данные в объявлениях и тканевых масках, истец Безруков испытал нравственные и физические страдания, в частности, в чувстве негодования, возмущения, и иные негативные эмоции от несогласованного использования его персональных данных, включая изображение, в общедоступных источниках в сети Интернет», - сказано в решении суда.	20.01.2026 - публикация в СМИ
7.5	В Краснодаре с банка «Уралсиб» в пользу вкладчика взыскано ₽46 млн за действия бывшей сотрудницы, которая передала злоумышленникам данные вкладчика	Четвертый кассационный суд общей юрисдикции отклонил жалобу ПАО «Банк «Уралсиб»», которое оспаривало взыскание нанесенного клиенту ущерба в сумме 46 млн руб., сообщает пресс-служба суда. Кредитное учреждение должно нести ответственность за действия бывшей сотрудницы, которая передала злоумышленникам данные вкладчика — жителя Краснодара. После этого преступники сняли средства со счета в одном из офисов банка в Москве по подложному паспорту. Пострадавший вкладчик обратился в «Уралсиб» за возмещением убытков, но ему было отказано. Тогда он направил иск в суд. Прикубанский районный суд Краснодара и Краснодарский краевой суд встали на сторону вкладчика, указав на грубые нарушения банком законодательства о банковской тайне. Суды признали, что сотрудники допустили утечку персональных данных клиента, а затем проявили халатность при выдаче крупной суммы, не обратив внимания на поддельный паспорт. С банка «Уралсиб» была взыскана полная сумма вклада — 27,5 млн руб., проценты за неправомерное удержание средств, компенсация морального вреда и штраф, в общей сложности свыше 46 млн руб. Кассационный суд, рассмотрев жалобу банка, не нашел оснований для отмены решений. Суд подчеркнул, что именно банк как работодатель в полной мере отвечает за действия своих сотрудников, говорится в решении кассации.	21.01.2026 - публикация в СМИ

№	Наименование	Описание	Статус
7.6	Роскомнадзор зафиксировал снижение числа утечек персональных данных в 2025 году	Количество зафиксированных случаев компрометации баз персональных данных в России снизилось в 2025 году до 118 случаев, в сеть попали более 52 млн записей. В 2024 году ведомством было зафиксировано 135 утечек баз данных, содержащих свыше 710 млн записей о россиянах.	22.01.2026 - публикация в СМИ
7.7	Компании удалось добиться замены штрафа на предупреждение после хакерской атаки и утечки данных	□ В июле 2025 года ООО ТД «АСК» подверглось DDoS-атаке. Злоумышленники выгрузили и опубликовали в Telegram и на других ресурсах персональные данные сотрудников (ФИО, паспорта, адреса, телефоны и др.). Пострадали данные 2 сотрудников. Компания сама уведомила Роскомнадзор об инциденте, однако регулятор все равно составил протокол по ч. 1 ст. 13.11 КоАП РФ (штраф для юрлиц от 150 до 300 тыс. руб.). □ Роскомнадзор настаивал на штрафе, утверждая, что нормы о замене наказания на предупреждение (ст. 4.1.1 КоАП) здесь неприменимы, так как нарушение выявлено не в ходе планового госконтроля, а в ходе административного расследования. ⚖ Суд встал на сторону компании и заменил штраф на предупреждение: □ Статус МСП: Компания является малым предприятием и включена в реестр МСП. □ Отсутствие реального ущерба: Не доказано причинение вреда жизни, здоровью или имущественного ущерба гражданам. □ Добросовестность: Компания признала вину, сотрудничала со следствием и совершила правонарушение впервые. ⚠ Важный прецедент по ч.3 ст.3.4 и ст. 4.1.1 КоАП: Суд отверг довод Роскомнадзора о том, что административное предупреждение возможно только при определенных видах проверок. Судья указал, что понятие «государственный контроль» нужно толковать широко. Иное нарушало бы принцип равенства перед законом. □ Вывод для бизнеса: даже если факт утечки доказан, оперативная реакция (уведомление РКН), статус МСП и отсутствие тяжких последствий — реальный шанс избежать денежного взыскания.	26.11.2025 - решение Арбитражного суда Кемеровской области по делу №А27-27136/2025

№	Наименование	Описание	Статус
7.8	ВС РФ: Ошибка подрядчика не спасает оператора от штрафа за утечку	□ Верховный Суд РФ поставил точку в споре о том, несет ли заказчик ответственность за утечку, произошедшую на стороне подрядчика. □ Суть дела: Минтруд РФ был оштрафован на ₽100 тыс. по ч.1 ст.13.11 КоАП РФ. Инцидент произошел еще в ноябре 2023 года: в сеть утекли данные сотрудников Министерства и их родственников. □ Позиция защиты: Минтруд пытался доказать невиновность, ссылаясь на то, что утечка произошла из-за взлома инфраструктуры подрядной организации, которая не обеспечила должную защиту. □ Суд оставил штраф в силе, отвергнув доводы Министерства: □ Статус оператора ПД обязывает принимать организационные и технические меры защиты. Передача обработки или инфраструктуры подрядчику не снимает ответственности с заказчика. □ Минтруд не уведомил Роскомнадзор об инциденте самостоятельно. Факт утечки был подтвержден Министерством только после запроса от надзорного органа. Это сталоотягчающим обстоятельством, указывающим на бездействие. □ Суд отметил, что в материалах дела нет доказательств того, что Министерство осуществляло внутренний контроль или аудит соответствия обработки ПД требованиям закона (ст.ст. статей 18.1, 19, 22.1 152-ФЗ).	21.01.2026 - постановление Верховного Суда РФ №5-АД25-119-К2

№	Наименование	Описание	Статус
7.9	ВС РФ признал неправомерным использование образов, созданных ИИ, в политической агитации	□ Верховный суд России признал неправомерным использование в политической агитации изображений людей, сгенерированных нейросетями. То есть не конкретных граждан, а неких образов, созданных искусственным интеллектом. Ориентиром для практики должно стать дело из Челябинской области, где коммунисты использовали в ходе избирательной кампании листовки, нарисованные искусственным интеллектом. На листовке была изображена счастливая семья. □ Суд первой инстанции тогда поддержал коммунистов. Однако Второй апелляционный суд общей юрисдикции, наоборот, согласился с избиркомом. □ «В гражданском законодательстве понятие «физическое лицо» не содержится. Однако из положений статей 17, 19, 21 Гражданского кодекса Российской Федерации можно сделать вывод, что под ним понимается любой человек, выступающий в качестве субъекта гражданских правоотношений и наделенный правами и обязанностями, обладающий правоспособностью и дееспособностью», - сказано в апелляционном определении Судебной коллегии по административным делам Второго апелляционного суда общей юрисдикции. □ Также апелляционная инстанция сослалась на правовые позиции Конституционного суда России, который в одном из своих определений указал: установленное специальное регулирование предвыборной агитации направлено прежде всего на то, чтобы не допустить возможность формирования у избирателей искаженного представления о кандидате, а также на обеспечение равенства прав кандидатов и защиту прав и интересов граждан, не являющихся кандидатами. □ Проще говоря, у людей пытались вызвать живые эмоции с помощью неживых картинок. «В качестве требований к изображениям людей, сгенерированным с помощью нейросетей, в агитационном материале являлось формирование положительных образов, призванных вызвать симпатию у избирателей (например, образ рабочего завода должен передавать силу, надежность, образ молодого предпринимателя - позитивный настрой и деловитость, образ учителя - доброжелательность и профессионализм)», - говорится в материалах дела. Второй апелляционный суд счел, что это незаконно. Верховный суд России согласился с такой правовой позицией.	04.02.2026 - определение Верховного Суда РФ №48-ИКАД26-1-А2

№	Наименование	Описание	Статус
7.10	Ответственность за неуведомление о трансграничной передаче ПД по ч.10 ст.13.11 КоАП РФ	□ Организация занималась отправкой несовершеннолетних на обучение в Великобританию. В июне 2025 года в рамках исполнения договора оператор направил принимающей стороне (британскому учебному центру) персональные данные 9 детей. □ В ходе прокурорской проверки было установлено, что оператор не направил уведомление в Роскомнадзор о намерении осуществлять трансграничную передачу до начала такой деятельности, как того требует ч. 3-4 ст. 12 ФЗ-152 «О персональных данных». □ Арбитражный суд Республики Башкортостан (решение от 08.09.2025 по делу № А07-27941/2025) признал директора виновным в совершении административного правонарушения по ч.10 ст.13.11 КоАП РФ. Однако, принимая во внимание первичность нарушения и отсутствиеотягчающих обстоятельств, суд применил положения ст.4.1.1 КоАП РФ и заменил административный штраф на предупреждение. □ Проблема правовой квалификации: директору вменили ч.10 ст.13.11 КоАП РФ («Невыполнение обязанности... по уведомлению уполномоченного органа... о намерении осуществлять обработку персональных данных»). Однако с юридической точки зрения здесь наблюдается коллизия: □ Неподача уведомления о трансграничной передаче (ст.12 ФЗ-152), которое законодательно отделено от уведомления о начале обработки (ст.22 ФЗ-152). □ Формально непредоставление сведений в госорган образует состав ст.19.7 КоАП РФ. Санкции по этой статье значительно ниже, а срок давности короче. △ Тем не менее, практика идет по пути расширительного толкования: надзорные органы приравнивают нарушение порядка уведомления о трансграничной передаче к нарушению общего порядка уведомления об обработке, применяя более строгую статью 13.11 КоАП.	08.09.2025 - решение Арбитражного суда Республики Башкортостан по делу №А07-27941/2025

№	Наименование	Описание	Статус
7.11	Разработчика чата для знакомств из Португалии оштрафовали за повторную нелокализацию баз с ПД	□ Арбитражный суд Москвы оштрафовал компанию-разработчика игр и приложений Bad Kitty`s Dad из Португалии на ₽ 6 млн за повторное нарушение российского законодательства о локализации баз с персональными данными граждан РФ. Протокол в августе 2025 года составило Управление Роскомнадзора по Центральному федеральному округу. □ Речь идет об интернет-сервисе Ome.TV (видеочате для общения со случайными собеседниками), при регистрации в котором пользователи должны предоставить адрес электронной почты, имя, возраст, фотографию и информацию из профилей в социальных сетях. В нарушение закона база собранных данных хранится на территории Европейского союза (ЕС).	05.02.2025 - решение Арбитражного суда города Москвы по делу №А40-348409/2025

№	Наименование	Описание	Статус
7.12	Прецедент РЖД: суд сломал практику объективного вменения при утечках данных	☐ Девятый арбитражный апелляционный суд отменил штраф ОАО «РЖД» за утечку данных 17 млн строк. ☐ Суть дела: Роскомнадзор выявил в Telegram-каналах (включая проукраинские хакерские группы) базу данных сотрудников РЖД — более 17 млн строк (ФИО, должности, email). Суд первой инстанции оштрафовал компанию на ₽ 150 тыс. по ч.1 ст.13.11 КоАП РФ, посчитав, что оператор не обеспечил защиту данных. ☐ Линия защиты: РЖД не согласились со штрафом. Их ключевой аргумент: утечка произошла не из-за халатности, а в результате целенаправленной кибератаки. Компания обратилась в МВД и ФСБ, в результате чего было возбуждено уголовное дело по ч.1 ст.272.1 УК РФ (незаконные использование и (или) передача, сбор и (или) хранение компьютерной информации, содержащей персональные данные). ☐ Ключевой вывод суда: апелляция разрушила привычную логику регулятора, сославшись на ч. 2 ст. 2.1 КоАП РФ (понятие вины юридического лица). 1. Сам факт утечки ≠ вина компании. Суд указал, что административная ответственность наступает только при наличии вины. Нельзя штрафовать компанию просто за то, что инцидент произошел (объективное вменение). РКН обязан доказать, какие именно меры компания могла принять, но не приняла. 2. Субъективная сторона правонарушения. Суд подчеркнул: в деле нет доказательств того, что РЖД бездействовало. Напротив, доступ к данным получили третьи лица (хакеры) в результате преступления (ст. 272.1 УК РФ). Если воля компании была направлена на защиту, а вред нанесен преступниками, вины оператора в административном смысле нет. 3. Презумпция невиновности. Вывод РКН о единоличной вине РЖД суд назвал преждевременным, пока не завершено расследование уголовного дела о взломе. ☐ Контекст имеет значение: суд официально принял во внимание напряженную геополитическую обстановку вокруг РФ и рост хакерских атак со стороны недружественных государств как общеизвестный факт, снижающий степень вины атакуемого бизнеса.	16.02.2025 - решение Девятого арбитражного суда города Москвы по делу №09АП-62551/2025

№	Наименование	Описание	Статус
7.13	Суд признал Realtimeboard Inc. dba Miro и NIC. UA LLC виновными в нарушении требований о локализации баз с персональными данными россиян	Мировой судья судебного участка №422 Таганского района Москвы признал американскую онлайн-платформу для совместной работы Realtimeboard Inc. dba Miro и украинскую компанию по регистрации доменов NIC. UA LLC виновными в нарушении требований о локализации баз с персональными данными россиян (ч.5 ст.18 152-ФЗ). «Realtimeboard Inc. dba Miro назначено наказание в виде административного штрафа в размере 2 млн рублей, NIC. UA LLC - в размере 6 млн рублей», - сообщили в суде. «Американская компания признана виновной в нарушении требования о локализации данных российских пользователей на территории России (ч. 8 ст. 13.11 КоАП РФ). Украинская организация признана виновной в повторном нарушении данного требования. (ч. 9 ст. 13.11 КоАП РФ).	26.02.2025 - публикация в СМИ

№	Наименование	Описание	Статус
7.14	Суд запретил Авито требовать видео и паспорт для разблокировки профиля	Пользователь судился с ООО «КЕХ еКоммерц» (Авито) из-за блокировки аккаунта, которым беспрепятственно пользовался 10 лет. Платформа закрыла доступ из-за «подозрительной активности» и потребовала пройти проверку: записать видео с поворотом головы, а позже добавила требование предоставить фото паспорта или водительских прав. Пользователь наотрез отказался раскрывать свои биометрические данные. Суд обязал Авито восстановить доступ к профилю без предоставления видеоизображения и фотографий личных документов. Главный аргумент суда строился на п. 13 ст. 13 Закона № 572-ФЗ: отказ физического лица от биометрической идентификации не может служить основанием для отказа ему в оказании услуг. Также суд сослался на ФЗ-152 «О персональных данных», напомнив, что согласие на обработку должно быть свободным, а собираемые данные не должны быть избыточными по отношению к целям обработки. Важные инсайты по делу: 1 Дело рассматривалось по иску о защите прав потребителей. Это подтверждает, что Авито имеет статус «владельца агрегатора», на которого в полной мере распространяются жесткие требования ЗоЗПП, а не просто внутренние пользовательские соглашения. 2 Суд не стал упоминать профильную ст. 11 152-ФЗ (которая как раз регулирует биометрию), зато 572-ФЗ о единой биометрической системе стал для суда важным аргументом. 3 «Проверку благонадежности» суды могут интерпретировать именно как процедуру установления личности. Особенно когда она проводится повторно при появлении сомнений в результатах прошлых (в т.ч. небиометрических) проверок. 4 Точка в споре еще не поставлена — на данное решение суда уже поданы 2 апелляционные жалобы.	04.12.2025 - решение Московского районного суда по делу №2-2087/2025 ~ М-1409/2025

№	Наименование	Описание	Статус
7.15	Суд: использование ИИ не может быть поводом снижать гарантии для граждан или каким-либо образом ухудшать их положение	□ ООО «Дегустаторстрой» оспорило в суде требование Межрайонной инспекции Федеральной налоговой службы №2 по Волгоградской области об уплате пени на сумму ₽ 926 тыс. Налогоплательщик указал на отсутствие в материалах дела расчёта спорных пеней. Налоговый орган, вместо того чтобы просто раскрыть формулу, занял бескомпромиссную позицию. Представитель инспекции заявил, что Налоговый кодекс РФ вообще не предусматривает обязанность предоставлять расчёт сумм пени. □ Апелляционный суд напомнил, что любые начисления подлежат проверке, и сделать их понятными — прямая обязанность налогового органа. Суд сформулировал ряд прецедентных тезисов об использовании автоматизированных систем, в т.ч. ИИ: 1□ Использование для расчётов начислений ИИ не является основанием презюмировать правильность произведённых расчётов и не снимает ответственность за полученный результат с налогового органа. 2□ Суд признаёт, что внедрение ИИ — свершившийся и необратимый факт, но считает, что его использование не может быть поводом снижать гарантии для граждан или каким-либо образом ухудшать их положение. 3□ Все начисления, которые будут недоступны пониманию, проверке и оценке со стороны суда, априори являются незаконными. 4□ Нет ни правовых, ни фактических оснований для презумпции правильности расчётов, произведённых при помощи программного обеспечения. 5□ ИИ не является субъектом, это инструмент, который не может вытеснить человека и должен использоваться под контролем ответственного лица. 6□ Внедрение в деятельность налоговых органов ИИ и исключение из актов сумм пеней не снимают с налогового органа процессуальных обязанностей по доказыванию правильности начислений. □ В итоге, ФНС по требованию суда всё-таки смогла выгрузить и предоставить понятный расчёт. И он оказался математически верным. Однако точка в этом концептуальном споре еще не поставлена. Компания не смирилась с решением, и на 17.03.2026 назначено заседание суда кассационной инстанции.	09.12.2025 - решение Московского районного суда по делу №А12-8377/2025

№	Наименование	Описание	Статус
7.16	Компанию Battlestate Games оштрафовали на ₽ 2 млн за нелокализацию баз с данными россиян	Мировой судья судебного участка №422 Таганского района города Москвы 3 марта 2026 года признал виновным в совершении административного правонарушения по ч.8 ст.13.11 КоАП РФ (невыполнение оператором при сборе персональных данных предусмотренной законодательством РФ обязанности по обеспечению записи, систематизации, накопления, хранения, уточнения персональных данных граждан РФ) компанию Battlestate Games Limited и назначил наказание в виде административного штрафа в размере ₽ 2 млн. Battlestate Games Limited - российская независимая компания, разработчик и издатель компьютерных игр. Ее юридическое лицо зарегистрировано в Лондоне, офис организации расположен в Санкт-Петербурге. Компания разрабатывает программное обеспечение для компьютерных игр, создает и обновляет его, поддерживает программное обеспечение, занимается графическим дизайном и дизайном веб-сайтов. Компания создала игру Escape from Tarkov - стелс-шутер от первого лица в визуальной стилистике пост-СССР.	04.03.2026 - публикация в СМИ

№	Наименование	Описание	Статус
7.17	Пассажирка выиграла суд у российской авиакомпании из-за рекламной рассылки	□ Суд в Уфе встал на сторону пассажирки российского авиаперевозчика, которая начала получать рекламную рассылку без согласия. □ Женщина получила рекламу от одной из российских авиакомпаний на электронную почту, из-за чего сделала вывод, что ее персональные данные были обработаны без свободного и невынужденного согласия. В этой связи она обратилась в суд с иском о защите прав потребителей, так как «указанными действиями ответчик вторгся в частное пространство». □ Из отзыва представителя авиакомпании на иск следует, что заявительница как клиент компании предоставила свое согласие на получение сообщений на свою электронную почту при оформлении бронирования, а от рассылок она может отказаться в любое время. Однако суд установил, что истица не давала свободное согласие на обработку ее персональных данных не только для целей бронирования (приобретения) билетов, но и для целей направления рекламы по сетям электросвязи. □ В результате с авиакомпании в пользу заявительницы взыскали пять тысяч рублей компенсации морального вреда и шесть тысяч рублей компенсации судебных расходов. Также фирму оштрафовали на 2,5 тысячи рублей за неудовлетворение требования потребителя в добровольном порядке, кроме того, в доход бюджета была взыскана госпошлина в три тысячи рублей.	09.03.2026 - публикация в СМИ
7.18	Официальный комментарий ФАС России о размещении рекламы в Instagram, Facebook, YouTube, Telegram, WhatsApp	□ В связи с принятием Роскомнадзором мер по ограничению доступа к социальным платформам Инстаграм и Фейсбук, видеохостингу Ютуб, ВПН-сервисам, мессенджерам Телеграм и Вотсап ФАС России усматривает в размещении рекламы на данных ресурсах признаки нарушения части 10.7 статьи 5 Федерального закона «О рекламе». □ Ответственность за нарушение указанной нормы Федерального закона «О рекламе» в силу статьи 38 данного закона несут как рекламодатель, так и рекламораспространитель.	10.03.2026 - публикация на портале ФАС России

№	Наименование	Описание	Статус
7.19	Германская SSI International оштрафована на 6 млн рублей за нелокализованные данные россиян	Мировой судья судебного участка № 422 Таганского района Москвы признал германскую компанию SSI International GmbH виновной в нарушении российского законодательства в области персональных данных и назначил ей административный штраф в 6 млн рублей. Об этом сообщили в суде. Компания признана виновной по ч. 9 ст. 13.11 КоАП (повторное нарушение требования о локализации данных российских пользователей на территории России). SSI International GmbH - международная организация, специализирующаяся на обучении дайвингу, фридайвингу, плаванию и snorklinгу.	10.03.2026 - публикация в СМИ

№	Наименование	Описание	Статус
7.20	Дело ООО «ПКР Аналитика» и пределы объективного вменения при утечках данных	☐ Арбитражный суд города Санкт-Петербурга и Ленинградской области рассмотрел дело об утечке персональных данных в результате хакерской атаки. Решение демонстрирует, как суды первой инстанции подходят к оценке вины операторов, и представляет интерес для сравнения с недавним прецедентом РЖД. ☐ Осенью 2025 года компания подверглась кибератаке, в результате которой в открытый доступ (в Telegram-канал) попала база данных интернет-ресурса компании - 70 000 субъектов (представители и сотрудники юридических лиц). Состав данных: ФИО, должность, служебный адрес электронной почты, служебный номер телефона. Компания своевременно направила в Роскомнадзор первичные и вторичные уведомления об инциденте. ☐ В ходе заседания оператор ходатайствовал о приостановлении производства по делу, ссылаясь на наличие материала проверки в правоохранительных органах (КУСП № 18075 от 15.08.2025). Суд отклонил ходатайство, не найдя оснований для невозможности рассмотрения административного дела. Суд признал компанию виновной по ч.13 ст.13.11 КоАП РФ. Однако, учитывая, что правонарушение совершено впервые, суд применил положения ст. 4.1.1 КоАП РФ и заменил административный штраф на предупреждение. ☐ Ключевые выводы: 1☐ Даже при подтвержденной вине и значительном объеме скомпрометированных данных (70 тыс. субъектов), институт замены штрафа на предупреждение (ст. 4.1.1 КоАП РФ) эффективно работает для первого правонарушения. 2☐ Простая подача заявления в полицию (доследственная проверка) и получение выписки из КУСП не имеет такой же юридической силы для защиты в суде, как вынесенное постановление о возбуждении уголовного дела, которое помогло РЖД. 3☐ Несмотря на позитивный прецедент апелляции по РЖД, суды первой инстанции продолжают применять объективное вменение, требуя от оператора доказывать, что он предпринял все возможные меры защиты.	26.02.2026 - решение Московского районного суда по делу №А56-4733/2026

№	Наименование	Описание	Статус
7.21	Суд подтвердил дисциплинарную ответственность за хранение работником паролей на рабочем столе	Шестой кассационный суд общей юрисдикции 05.03.2026 рассмотрел трудовой спор в рамках дела №88-3939/2026 и подтвердил правомерность наказания работника за сам факт создания угрозы информационной безопасности (хранение паролей на виду), даже если негативные последствия (взлом, утечка) не наступили. Работник ПАО АНК «Башнефть» был привлечен к дисциплинарной ответственности в виде замечания. Основанием послужил выявленный службой безопасности факт: сотрудник хранил пароли доступа к корпоративным информационным ресурсам (включая СЭД и «СПАРК-Интерфакс») в открытом текстовом файле на рабочем столе своего компьютера. Работник пытался оспорить приказ работодателя, ссылаясь на следующие обстоятельства: - Рабочий кабинет имеет строгий пропускной режим, и доступ к нему есть только у трех человек. - Вход в сам рабочий компьютер защищен двухфакторной аутентификацией. - Утечки конфиденциальной информации не произошло, и пароли третьим лицам не передавались. - Работодатель не проинформировал о наличии специализированной защищенной программы для хранения паролей. Суды всех инстанций признали действия работодателя законными и отказали работнику в иске: - Локальными нормативными актами (ЛНА) компании, включая Правила внутреннего трудового распорядка и политики ИБ, прямо запрещено сохранять пароли в открытом виде, в том числе в текстовом виде на рабочем столе. - Сотрудник был ознакомлен с должностной инструкцией и требованиями ЛНА под роспись. - Тот факт, что работодатель не предложил программу для хранения, не оправдывает работника: при возникновении трудностей с запоминанием паролей сотрудник должен был самостоятельно запросить у работодателя информацию о легитимных защищенных способах их хранения. - Отсутствие фактической утечки данных или несанкционированного доступа не отменяет факта дисциплинарного проступка (нарушения правил безопасности).	05.03.2026 - определение Шестого кассационного суда общей юрисдикции по делу №88-3939/2026

№	Наименование	Описание	Статус
7.22	Уголовное дело за слежку в отношении коллеги на работе	□ Белокурихинским межрайонным следственным отделом следственного управления Следственного комитета Российской Федерации по Алтайскому краю завершено расследование уголовного дела в отношении 52-летней жительницы Солонешенского района, обвиняемой в совершении преступления, предусмотренного ч. 3 ст. 30 ч. 1 ст. 137 УК РФ (покушение на незаконное соби́рание сведений о частной жизни лица, составляющих его личную тайну, без его согласия). □ По данным следствия, обвиняемая длительное время испытывала личные неприязненные отношения к своему коллеге по работе, считая, что он ненадлежащим образом исполняет свои должностные обязанности и много времени уделяет личным делам. Чтобы доказать начальству недобросовестность коллеги, в октябре 2025 года фигурантка тайно проникла в его кабинет и положила на шкаф включенный диктофон. Довести умысел на сбор сведений о частной жизни ей не удалось по независящим обстоятельствам – диктофон был обнаружен сотрудником организации.	20.03.2026 - публикация на портале Следственного комитета РФ по Алтайскому краю
7.23	Официальный комментарий ФАС России: до конца 2026 года служба не будет привлекать к ответственности за размещение рекламы в Telegram и на YouTube	□ Согласно части 10.7 статьи 5 Федерального закона «О рекламе» не допускается распространение рекламы на информационных ресурсах, доступ к которым ограничен в соответствии с законодательством Российской Федерации. Направленная Роскомнадзором информация находится на рассмотрении в ФАС. □ По фактам размещения рекламы в Telegram и Youtube ФАС анализирует содержание рекламы, дату заключения договора, дату введения ограничений на работу платформы, дату публикации рекламы, основания её размещения, в том числе договоры и платежные поручения. □ Очевидно, что хозяйствующим субъектам требуется время для адаптации к новым правилам и переориентированию на другие рекламные каналы. Поэтому в отношении рекламы в Telegram и Youtube необходим переходный период до конца 2026 года, в течение которого меры ответственности за распространение рекламы на таких ресурсах применяться не будут. □ При этом контроль за соблюдением законодательства о рекламе при размещении рекламы на платформах, ограничения в отношении которых были введены ранее (Instagram*, Facebook**), а также на VPN-сервисах будет продолжен с применением соответствующих мер ответственности. Размещение рекламы на таких ресурсах не допускается.	25.03.2026 - публикация на портале ФАС России

№	Наименование	Описание	Статус
7.24	Change.org и Padi Americas оштрафованы за нелокализацию в РФ баз с персональными данными	Мировой судья судебного участка №422 Таганского района Москвы привлёк платформу для петиций Change.org Pbc к административной ответственности по ч. 8 ст. 13.11 КоАП РФ (невыполнение оператором при сборе персональных данных их накопления, хранения, уточнения с использованием российских баз данных). Платформе назначили штраф в размере 1 млн. Суд оштрафовал также за нарушение закона о персональных данных разработчика приложения для аквалангистов Padi Americas Inc. (организация признана нежелательной на территории РФ), назначив штраф в размере 6 млн. Первый административный штраф был назначен Padi Americas Inc. 11 июля 2023 г. Судья назначил компании штраф в размере 1,5 млн по ч. 8 ст. 13.11 КоАП РФ.	25.03.2026 - публикация в СМИ
7.25	Duolingo и eNom оштрафованы за нелокализацию в РФ баз с персональными данными	Мировой судья судебного участка №422 Таганского района города Москвы 26 марта 2026 года признал виновной в совершении административного правонарушения по ч. 8 ст. 13.11 КоАП РФ платформу для изучения иностранных языков «Дуолинго, Инк.» (Duolingo, Inc.). Назначено административное наказание в виде штрафа в размере 2 млн руб. Также по аналогичной статье на 2 млн руб оштрафована компания «еНом ЛЛС.» (eNom LLC.), занимающаяся регистрацией доменных имен и веб-хостингом, отметили в суде.	26.03.2026 - публикация в СМИ

№	Наименование	Описание	Статус
7.26	ВС РФ запретил организациям ЖКХ требовать дополнительные персональные данные жильцов	Ресурсоснабжающая компания обратилась в межмуниципальное управление МВД с запросом о предоставлении персональных данных жителей ряда домов Оренбургской области, включая Ф. И. О., дату и место рождения, а также паспортные реквизиты. Эти сведения, по мнению организации, были необходимы для корректного начисления платы за коммунальные услуги. Ведомство отказало, указав, что передача такой информации невозможна без согласия граждан и противоречит закону «О полиции». Суд первой инстанции поддержал позицию МВД, отметив, что необходимые сведения можно получить из других источников, например, через ГИС ЖКХ или ЕГРН. Однако апелляционный и кассационный суды заняли противоположную позицию, признав, что компания вправе запрашивать и обрабатывать персональные данные без согласия граждан. Представители МВД не согласились с таким подходом и обратились в Верховный Суд России, ссылаясь на то, что удовлетворение требований в рамках настоящего дела приведет к необоснованному расширению полномочий общества как ресурсоснабжающей организации, которые не предусмотрены жилищным законодательством, а именно допуску к оперативным ресурсам полиции. Судебная коллегия по экономическим спорам, рассмотрев кассационную жалобу, признала доводы заявителя заслуживающими внимания и оставила в силе решение суда первой инстанции об отказе компании в предоставлении персональных данных жильцов.	01.04.2026 - публикация в СМИ

№	Наименование	Описание	Статус
7.27	Апелляция отменила решение по делу «Авито vs биометрия»: видеопроверка — не сбор биометрии	Рязанский областной суд 11.03.2026 отменил решение первой инстанции, которым Авито обязали восстановить пользователю доступ к профилю без видеопроверки и фото документов (дело № 33-342/2026). Напомним: в декабре 2025 года Московский районный суд г. Рязани встал на сторону пользователя, сославшись на п.13 ст.13 572-ФЗ и нормы 152-ФЗ о ПД. Апелляционная коллегия пришла к противоположным выводам: 1. Видеопроверка благонадежности (liveness check) не является обработкой биометрических ПД, поскольку не используется для установления личности пользователя. Цель — подтвердить, что аккаунтом управляет живой человек. 2. Ответчик не сохраняет видеоизображения пользователей, что технически исключает возможность биометрической идентификации. 3. Отсутствие факта обработки биометрических данных прямо подтверждено Минцифры России, Роскомнадзором, а также партнёром ответчика — ПАО «МТС». 4. 572-ФЗ неприменим к проверкам на Авито — он регулирует идентификацию через государственную ЕБС. Неприменимость закона подтверждена заключением Минцифры. 5. Пользователь сам нарушил правила Авито (использовал два профиля в одной категории), что дало платформе основание для проведения проверки в соответствии с разделом 7 Условий использования. 6. Подтвержден приоритет договорной свободы (ст.421 ГК РФ): принятые при регистрации Условия обязывают пользователя, а освобождение нарушителя от проверки означало бы индивидуальные привилегии. Истец скончался 24.01.2026. Коллегия рассмотрела жалобы по существу, руководствуясь разъяснениями ВС РФ. Позиция апелляции не бесспорна: Довод о том, что видеопроверка не является сбором биометрии, потому что платформа «не устанавливает личность», в значительной степени опирается на декларации самой платформы — порядок обработки и хранения видеозаписи классифайдом остался не исследован. Отсутствие альтернативных способов верификации (вход через Госуслуги, подтверждение по почте/телефону) создаёт ситуацию, в которой пользователь фактически лишён выбора.	11.03.2026 - апелляционное определение Судебной коллегии по гражданским делам Рязанского областного суда по делу № 33-342/2026 (2-2087/2025)

№	Наименование	Описание	Статус
7.28	Апелляция отказала Роскомнадзору в привлечении к ответственности сервиса DLBI за мониторинг утечек	Роскомнадзор, использовавший собственную систему мониторинга (АС МПД), настаивал на том, что DLBI выступает посредником, предоставляющим пользователям доступ к нелегальным базам данных (в том числе из Даркнета) без правовых оснований (ч. 1 ст. 13.11 КоАП РФ). Ведомство ссылалось на результаты собственного мониторинга, где зафиксировало функционал поиска по утечкам. DLBI указал на ошибочность объединения двух разных процессов: обработки данных посетителей сайта (где DLBI является легальным оператором) и работы поискового алгоритма: DLBI не хранит и не обрабатывает ПД в открытом виде (номера телефонов или e-mail). Вместо этого используются хеши (зашифрованные слепки), которые не позволяют восстановить исходную информацию. Кроме того, сам функционал проверки предоставляется не напрямую через сайт, а через партнеров (например, систему «Защитник» от МТС). Арбитражный суд Москвы в решении от 10.12.2025 по делу А40-201075/25 отказал в удовлетворении иска Роскомнадзора и указал, что: Сервис обрабатывает не ПД, но все данные, в которых производится поиск признаков наличия в них ПД пользователей, а Роскомнадзор не смог доказать принадлежность анализируемых сервисом сведений к «персональным данным», охраняемым законом. Деятельность DLBI соответствует мировой практике и направлена на предупреждение об утечках, тогда как система РКН сфокусирована на проверке формального соблюдения закона операторами. Девятый арбитражный апелляционный суд оставил в силе решение Арбитражного суда Москвы от 10.12.2025, отказал в удовлетворении апелляционной жалобы Роскомнадзора.	08.04.2026 - постановление Девятого арбитражного апелляционного суда № 09АП-68401/2025

№	Наименование	Описание	Статус
7.29	New Дело ООО «Комлайн» (ГК «Орион Телеком»): утечка ПД, штраф заменён предупреждением, несмотря на статус потерпевшего по уголовному делу	□ Арбитражный суд Кемеровской области (дело № А27-23786/2025) привлёк оператора связи ООО «Комлайн» к ответственности по ч.12 ст.13.11 КоАП РФ. В июне 2025 г. в результате атаки группировки BO_Team-UA были скомпрометированы данные 4 225 абонентов (ФИО, паспортные данные, адреса, телефоны), которые 29.07.2025 опубликовали в Telegram-канале. □ В деле фигурирует отчет BI.ZONE, подготовленный по заказу самого «Орион Телеком» в рамках внутреннего расследования и направленный оператором в Роскомнадзор как часть уведомления о результатах расследования. Документ зафиксировал системные провалы инфобеза: □ активная учётная запись сотрудника, уволенного в 2022 г.; □ пароли не менялись с 2019 г.; □ ПО с критическими уязвимостями; □ доступ к инфраструктуре получен 30.05.2025, обнаружили утечку только 12.06.2025. ✳ Ключевые выводы суда: 1□ Возбуждение уголовного дела по ст.272.1 УК РФ против хакеров не освобождает оператора от административной ответственности — статьи разграничивают ответственность злоумышленника и оператора. 2□ Принадлежность к КИИ 3 категории не даёт права на утечку — ни один НПА такого послабления не содержит. 3□ Ссылки на затягивание процесса (ходатайства об экспертизе через 5 месяцев) суд расценил как злоупотребление правом. 4□ Несмотря на санкцию 3–5 млн руб., штраф заменён на предупреждение по ст.4.1.1 КоАП РФ — оператор относится к МСП, правонарушение совершено впервые. □ Практика по утечкам ПД пока не устоялась: в деле РЖД уголовное дело против хакеров стало щитом, в делах «Комлайн» и «ПКР Аналитика» — нет. Решающими факторами становятся качество доказательств вины оператора, состояние систем ИБ и статус МСП.	28.04.2026 - решение АС Кемеровской области по делу № А27-23786/2025

№	Наименование	Описание	Статус
7.30	^{New} На Кубани районного чиновника оштрафовали за нелокализацию данных	□ Заместитель главы администрации Абинского района в Краснодарском крае оштрафована на 100 тыс. руб. по ч. 8 ст. 13.11 КоАП РФ — за нарушение требований о локализации баз персональных данных граждан РФ. □ Администрация Абинского района является оператором ПД интернет-ресурса, в исходном коде страниц которого используется платформа, принадлежащая иностранной компании из США. □ Привлечена к ответственности именно куратор направления — заместитель главы администрации района (как должностное лицо). Кейс наглядно демонстрирует расширение практики персональной ответственности должностных лиц-операторов за нарушения локализации, в т.ч. в части использования зарубежных аналитических и иных инструментов в исходном коде сайтов.	27.04.2026 - публикация в СМИ

8. Инициативы и события

8.2	МФО обсуждают с ЦБ альтернативные пути для работы с обязательной биометрией	□ Некоторые крупные МФО, которые имеют статус микрофинансовой компании (МФК), собираются перенаправлять часть обратившихся к ним за онлайн-займами клиентов в «дочки» – микрокредитные компании (МКК). Еще один путь – менять статус с МФК на МКК, но у него есть ряд ограничений. Эти действия связаны с тем, что с 1 марта 2026 г. все МФК при выдаче онлайн-займов должны будут идентифицировать заемщиков по биометрии из Единой биометрической системы (ЕБС), а для МКК такая обязанность появится только с 1 марта 2027 г. □ В конце 2025 г. Банк России и Минцифры провели рабочую встречу с представителями МФО, где среди прочего обсуждались варианты популяризации использования биометрии и наполнения базы новыми данными, так как сейчас их количество мало, рассказал «Ведомостям» исполнительный директор Webbankir Денис Сидоров. □ Сейчас сервисами с использованием биометрии из ЕБС могут воспользоваться до 50 млн россиян, сказал «Ведомостям» представитель Минцифры. Он также подтвердил встречу министерства с ЦБ и МФО: она была плановой, на ней обсуждалась подготовка к реализации требований нового федерального закона. Представитель Минцифры заметил, что МФК демонстрируют высокую техническую готовность к внедрению идентификации клиентов по биометрии. При этом использование биометрии является добровольным, напомнил представитель министерства: возможность взять займ в МФО без нее сохраняется — сделать это можно, обратившись в офис организации.	20.01.2026 - публикация в СМИ
-----	---	--	-------------------------------

8.3	Ассоциация больших данных (АБД) направила в Минцифры свои предложения относительно регулирования ИИ-технологий	□АБД (объединяет «Яндекс», VK, «Сбер», Газпромбанк, Т-Банк, Россельхозбанк, «Мегафон», «Ростелеком», Билайн, МТС и др.) 19 января направила министру цифрового развития Максуту Шадаеву письмо с предложениями по совершенствованию регулирования в сфере ИИ-технологий. □Предложения АБД сделаны во исполнение поручения вице-премьера Дмитрий Григоренко, который попросил «заинтересованные организации» представить свои идеи по регулированию ИИ в Минцифры до 20 января 2025 года. Регулятор вместе с аналитическим центром при правительстве до конца февраля проанализирует их и до 13 марта представит в правительство. □Среди эффектов, которых хочет добиться АБД — повышение доступности данных для обучения ИИ при соблюдении прав граждан на неприкосновенность частной жизни, ускорение внедрения технологий повышения конфиденциальности для обработки чувствительных данных, безопасное распределение данных между более широким кругом экономических агентов, увеличение объемов и разнообразия данных, доступных для обучения моделей ИИ, появление новых видов инновационных продуктов, услуг и сервисов на основе данных. □В частности, нужно конкретизировать порядок отнесения информации к персональным данным и сведениям, составляющим защищаемые законом тайны (включая банковскую), в случае применения технологий повышения конфиденциальности. Также наборы данных необходимо ввести в гражданский оборот, полагают в АБД. «До сих пор не существует правовой режим для датасетов, нет ни их рыночного оборота, ни подходов к определению их стоимости как объекта имущественных прав, не реализован их потенциал в качестве ценного актива», — указывают в АБД. Для этого в Гражданский кодекс и стандарты бухучета нужно ввести нормы о включении датасетов в состав охраняемых результатов интеллектуальной деятельности, сформировать правовой режим их гражданского оборота и защиты прав их обладателей. Бизнесу это даст расширение имущественной базы, рост активов и капитала, государству — рост налоговых поступлений. □Еще одно назревшее изменение, по мнению ассоциации, заключается в появлении модели взимания платы за доступ к госданным. Должен быть предусмотрен бесплатный доступ либо возмещение предельных затрат по обеспечению доступа к данным «для снижения издержек доступа к информации, содействия инновациям и максимизации общественного благосостояния». Именно такова мировая практика в том, что касается доступа к данным госсектора, констатируют в АБД. О том же свидетельствует доклад аналитического центра (АЦ) при правительстве «Доступ к данным госсектора: вопросы конкуренции».	21.01.2026 - публикация в СМИ
-----	--	--	-------------------------------

8.4	ЦБ введет наказание для топ-менеджеров банков за слабую киберзащиту	Топ-менеджеры банков, ответственные за информационную безопасность, могут быть уволены и лишены в течение 10 лет возможности занимать аналогичную позицию в другом банке в случае системных нарушений в защите клиентов от мошенников. Для топ-менеджеров некредитных финансовых организаций этот срок составит пять лет. Об этом сообщил заместитель председателя Банка России Герман Зубарев. «Если в течение года к банку неоднократно применялись меры за такие нарушения, профильный топ-менеджер должен будет покинуть свою должность и не сможет занять аналогичную позицию в другом банке в течение десяти лет. Топ-менеджер некредитной финансовой организации - в течение пяти лет», - сказал Зубарев. Замглавы регулятора пояснил, что Банк России прорабатывает квалификационные требования к топ-менеджерам финансовых организаций по информационной безопасности. Ко второму чтению готовится законопроект, который дополняет квалификационные требования еще одним критерием - нарушение требований по противодействию кибермошенничеству.	06.02.2026 - публикация в СМИ
8.5	Омбудсмен предложила ограничить размещение в СМИ данных о пострадавших детях	Ограничения на распространение в СМИ информации о пострадавших детях с описанием деталей происшествия необходимо ввести в России. Исключением является информация от официальных органов, такое мнение высказала на пресс-конференции в ТАСС уполномоченный по правам ребенка в Санкт-Петербурге Анна Митянина. По словам детского омбудсмена, она обратилась в Законодательное собрание Петербурга для разработки инициатив по вопросам совершенствования законодательства в области информационной безопасности. «Наша задача не ограничить общество и людей в получении информации, не введение цензуры, как полагают отдельные представители СМИ, а защита детей от вбросов ложной информации, фейков и комментариев, которые распространяются недобросовестными людьми», - подчеркнула Митянина.	11.02.2026 - публикация в СМИ

8.6	ИИ ограничат в принятии решений в социально значимых сферах	□ В РФ могут законодательно закрепить правило сохранения решающей роли человека при применении искусственного интеллекта (ИИ) в общественно значимых сферах: в здравоохранении, судопроизводстве, образовании и общественной безопасности. Это следует из материалов правительства, в которых собраны предложения к законопроекту по регулированию искусственного интеллекта. □ Подготовленный с учетом пожеланий документ Минцифры должно направить на согласование в правительство к концу февраля, сообщил источник, близкий к нескольким профильным ведомствам. □ Отсутствие требования о решающей роли человека при использовании ИИ несет системные риски, считает член комитета Госдумы по информполитике, федеральный координатор партийного проекта «Цифровая Россия» Антон Немкин.	13.02.2026 - публикация в СМИ
8.7	ЦБ: в реестре банковских карт не будет персональных данных об их владельцах	□ Реестр банковских карт не будет содержать персональную информацию о владельцах платежных средств, заявила журналистам глава департамента национальной платежной системы Банка России Алла Бакина в кулуарах Уральского форума «Кибербезопасность в финансах». □ Ранее статс-секретарь - заместитель министра цифрового развития РФ Иван Лебедев сообщил, что Банк России в течение года подготовит единую базу с информацией о банковских картах, оформленных у каждого гражданина РФ. В пресс-службе ЦБ подтвердили проработку создания единого реестра банковских карт граждан для учета их общего количества в рамках проекта «Антифрод 2.0».	20.02.2026 - публикация в СМИ
8.8	Предложено упростить отзыв согласия на обработку персональных данных	□ Лидер ЛДПР Леонид Слуцкий предложил закрепить в российском законодательстве обязанность операторов персональных данных предоставлять пользователям возможность отзывать согласие на обработку данных в той же форме, в которой оно было получено. Соответствующее обращение в адрес главы Минцифры РФ Максута Шадаева. □ Слуцкий в тексте обращения отметил, что действующее законодательство РФ регулирует порядок получения согласия, но не обязывает операторов обеспечивать симметричную процедуру его отзыва, добавил он. □ «В результате для отзыва согласия, данного онлайн, гражданину часто требуется направлять официальное письмо в адрес организации, которое в большинстве случаев игнорируется. Это влечет дополнительные временные и материальные затраты и существенно затрудняет реализацию гражданином своих прав», - говорится в письме.	21.02.2026 - публикация в СМИ

8.9	Бизнес попросил Госдуму узаконить покупку конкретных сведений из баз МВД	□ «Ассоциация больших данных» (АБД), объединяющая «Сбер», «Яндекс», VK и других крупных игроков, предложила дать компаниям — участникам единой антифрод-системы доступ к отдельным категориям данных из баз МВД. Инициатива направлена главе IT-комитета Госдумы Сергею Боярскому. □ Речь идет о сведениях о подозреваемых и обвиняемых, в том числе по административным правонарушениям, о розыске, постановке на учет и дееспособности. Авторы письма указывают, что это «позволит кредитным и иным организациям выстраивать более комплексные антифрод-системы, учитывающие большее число параметров». □ «Предложение “Ассоциации больших данных” заслуживает всестороннего анализа и проработки с коллегами из компетентных органов», — заявил Боярский. □ Операторы связи поддерживают инициативу. В «МегаФоне» считают, что это позволит «лучше и иногда быстрее выявлять мошеннические схемы». Любой обмен данными, особенно теми, что позволяют верифицировать риски, так или иначе приносит пользу, отмечает руководитель дирекции по предотвращению кибермошенничества Альфа-банка Евгений Винокуров.	24.02.2026 - публикация в СМИ
-----	--	--	-------------------------------

8.10	В Госдуме предложили создать сервис отзыва согласия на обработку данных	□Глава комитета Госдумы по развитию гражданского общества, вопросам общественных и религиозных объединений Яна Лантратова («Справедливая Россия») предложила создать единый сервис отзыва согласия на обработку персональных данных на портале «Госуслуги». □Соответствующее обращение было направлено в адрес главы Минцифры России Максута Шадаева. Парламентарий отметила, что действующее правовое регулирование не закрепляет унифицированный и гарантированный механизм отзыва согласия на обработку персональных данных. Как следствие, на практике формируются неоднородные процедуры, которые определяются исключительно внутренними правилами операторов персональных данных. □В письме уточняется, что функционал подобного сервиса может предусматривать отображение перечня организаций, которым гражданин предоставлял согласие на обработку персональных данных, возможность дистанционного отзыва согласия посредством электронного интерфейса, автоматическое уведомление операторов о поступлении соответствующего отзыва, а также фиксацию сроков исполнения обязанностей по прекращению обработки данных. □Кроме того, парламентарий предлагает законодательно закрепить право гражданина отзываться согласие любым удобным способом: через интернет, «Госуслуги», личный кабинет на сайте оператора, по электронной почте, через МФЦ или письменно. □Лантратова также полагает целесообразным установить, что способ отзыва такого согласия не должен быть сложнее, чем способ получения согласия. Операторов также предлагается обязать принимать отзыв независимо от способа его направления, регистрировать обращения и уведомлять заявителя о результате.	01.04.2026 - публикация в СМИ
8.11	Набиуллина призвала регуляторов дать банкам доступ к «госозеру» данных	□Глава Центробанка Эльвира Набиуллина призвала регуляторов решить проблему доступа и обмена данными для разработчиков в банковской отрасли. С таким предложением она выступила на пленарной сессии форума Data Fusion 8 апреля. □Согласно проведенному ЦБ опросу, 2/3 опрошенных организаций считают, что без доступа к данным они не смогут применять решения, основанные на ИИ, рассказала Набиуллина. При этом, по ее словам, в финансовой сфере не у всех есть доступ к данным: есть группа лидеров, у которых много данных, а есть финансовые организации, у которых такого доступа нет.	10.04.2026 - публикация в СМИ

8.12	New Совет Федерации обсудил вопросы ответственности за воспрепятствование адвокатской деятельности и защиту прав адвоката в цифровой среде	15 апреля в Совете Федерации состоялся круглый стол на тему «Ответственность за воспрепятствование адвокатской деятельности. Защита прав адвоката в цифровой среде». Участники отметили, что несмотря на формальные гарантии, адвокаты сталкиваются с системными нарушениями, а цифровизация создает новые риски для адвокатской тайны. Александр Терновцов (Общественная палата РФ) предложил внести в Закон о персональных данных и Закон о бесплатной юридической помощи изменения, предусматривающие специальный облегченный режим обработки ПД для адвокатов, оказывающих БЮП, и освобождение их от обязанности направлять уведомления об обработке ПД в государственные органы. Елена Авакян (советник ФПА РФ – руководитель цифровой трансформации адвокатуры) обозначила одну из ключевых проблем: доступ к цифровым доказательствам и реестрам. В отличие от прокурора, адвокат не имеет доступа к реестрам — на адвокатские запросы приходят отказы, а если адвокат находит информацию иным способом, его обвиняют в незаконном получении ПД. Для решения проблемы необходимы изменения в Закон о персональных данных и Закон об адвокатуре.	16.04.2026 - публикация в СМИ
8.13	New Главврача скорой помощи Вологды уволили за утечку данных пациентов	В ходе внеплановой проверки на Вологодской станции скорой медицинской помощи им. Н.Л. Турупанова выявлены многочисленные нарушения информационной безопасности. Информация направлена в контрольно-надзорные органы. Ведомственная проверка установила, что главврач передавал данные пациентов, поступивших по скорой помощи, третьим лицам. Главврач уволен. Случай показателен в контексте управления инсайдерскими рисками в здравоохранении и контроля доступа сотрудников медицинских учреждений к ПД пациентов.	22.04.2026 - публикация в СМИ

8.14	^{New} Минцифры заявило о планах расширить обязательное применение биометрии	□ В Единой биометрической системе (ЕБС) более 100 млн образцов лица и голоса россиян; ~40 млн записей — это записи голоса. Пользователями ЕБС являются 69 млн граждан: 6 млн с подтвержденной биометрией при личном визите, 24 млн — стандартное подтверждение, 7 млн сдали данные в дистанционном формате. □ Количество транзакций с применением биометрии превысило 32 млрд. Из них 320 млн — биоэквайринг (платеж «улыбкой»), 17 млн — проезд в метро, 13 млн — заключение договоров связи с иностранцами и второй фактор идентификации на «Госуслугах» и в банках. □ Минцифры планирует: 1 □ Нарастить масштабы использования биометрических данных и расширить каналы сбора (в т.ч. дистанционная сдача биометрии через специальные приложения). 2 □ Расширить сценарии обязательной биометрической идентификации: иностранные граждане при заключении договоров связи; маркетплейсы (антифрод-поправки); МФО с 1 марта 2026 г.; микрокредитные компании — через год.	29.04.2026 - публикация в СМИ
------	---	--	--------------------------------------

9. Информационные и аналитические материалы

№	Наименование	Описание	Статус
9.1	Методологический материал Privacy Advocates об отрицательной селекции применимости законного интереса к обработке персональных данных	□ Материал содержит схему фильтрации обработок ПД на применимость п.7 ч.1 ст.6 152-ФЗ, а также пример такой фильтрации в отношении следующих сценариев: - организация пропускного режима на территорию, где располагается оператор; - рассмотрение вопроса о трудоустройстве соискателя и сопутствующая обработка данных его родственников; - проведение внутренних и внешних аудитов оператора; - проведение расследований инцидентов, связанных с безопасностью ПД, в отношении субъектов оператора. □ Селекция не заменяет/подменяет полноценную оценку применимости ЗИ, а служит задаче исключения ложных представлений о возможности легализации некоторых обработок ПД посредством опоры на ЗИ – без проведения полноценной и углубленной оценки применимости ЗИ, посилой для крупных операторов, но недоступной для МСП.	23.12.2025 - публикация в "Альманахе" Privacy Advocates

№	Наименование	Описание	Статус
9.2	Презентация и статья Алексея Мунтяна про рациональный подход к выполнению требования о локализации баз с персональными данными в РФ	□ Мировой опыт: ранжирование типов локализации по степени ограничения свободы оборота данных □ Локализация данных в РФ □ Эволюция требования о локализации баз с данными граждан РФ □ Комментарии к изменениям в требованиях о локализации □ Интерпретация Роскомнадзором уточненных требований о локализации □ Варианты интерпретации уточненных требований о локализации □ Компромиссная интерпретация уточненных требований о локализации □ Общие выводы по уточненным требованиям о локализации □ Ретроспектива правоприменительной практики 2016-2025гг. □ Определение БД с ПД □ Сбор ПД не как действие, а как единый процесс □ Сбор и иные способы получения ПД □ Декомпозиция источников ПД – на примере online-обучения □ Экспресс-схема определения подлежащих локализации БД □ Стратегии реагирования на требование локализации □ Сложности выбора стратегии локализации □ Походы к оценке стоимости стратегий локализации □ Оценка расходов на реализацию стратегий локализации □ Риски и последствия несоблюдения требований о локализации □ Оценка рисков при реализации стратегий локализации □ Формула оценки привлекательности стратегий □ Калькулятор оценки стратегий локализации □ Пример ранжирования стратегий локализации □ Пример калькулятора расчета привлекательности стратегий локализации	03.01.2026 - публикация в "Альманахе" Privacy Advocates

№	Наименование	Описание	Статус
9.3	Заметка Алексея Мунтяна «Квантовая запутанность персональных данных»	Один из фундаментальных постулатов квантовой теории – принцип неопределенности Гейзенберга – гласит, что невозможно одновременно точно измерить координату и импульс частицы. Как только вы фиксируете, где именно в моменте находится объект наблюдения, вы перестаёте точно знать, куда и с какой скоростью он движется. Квантовая теория это один из возможных инструментов для понимания процессов, происходящих в информационном обществе. Только теперь в социальной системе в роли квантов выступает информация о человеке – его персональные данные, – а эффект наблюдателя начинает работать лишь тогда, когда субъект понимает, что его персональные данные собирают, анализируют и используют.	07.01.2026 - публикация в "Альманахе" Privacy Advocates
9.4	Комментарий Алексея Мунтяна «Инфляция смыслов в медиа и дефляция сложности в инфоприватности»	Феномен «инфляционного сторителлинга» описывает критическое перенасыщение цифровой среды контентом низкой смысловой плотности («медиазаполнителями»). Для инфоприватности это явление имеет прямые и тревожные последствия, выходящие за рамки медиа-теории. В условиях перенасыщения способность пользователя давать полноценное согласие де-факто аннигилируется. Субъект ПД, находящийся в состоянии когнитивного истощения, воспринимает запросы на дачу согласия для обработки данных как еще один вид информационного шума. Нажатие кнопки «Согласен» становится механическим ритуалом избавления от помехи, а не осознанным юридическим действием.	15.01.2026 - публикация в "Альманахе" Privacy Advocates
9.5	Презентация Алексея Мунтяна о ретроспективе комплаенса персональных данных в 2025г. и о перспективах на 2026-2028гг.	□ Основные регуляторные новеллы 2025 года и прогноз трендов на 2026: деприоритизация согласий и отраслевые стандарты обработки данных. □ Изменения правил контрольно-надзорных мероприятий Роскомнадзора и практика мониторинга прав субъектов персональных данных в Интернете. □ Итоги судебной практики 2025 года по утечкам данных и перспективы 2026 года с учетом возвращения некоторых категорий дел в суды общей юрисдикции.	19.01.2026 - публикация в "Альманахе" Privacy Advocates

№	Наименование	Описание	Статус
9.6	Ассоциация больших данных (АБД) совместно с IT-компанией HFLabs и Privacy Advocates представила аналитический доклад «Технологии защищенной обработки данных. Обезличивание»	Исследование посвящено методам обезличивания данных и их практическому применению в аналитике, обучении ИИ-моделей и межкорпоративных сценариях работы с информацией. Аналитический доклад рассматривает основные подходы к обезличиванию данных, примеры их применения в реальных бизнес-сценариях, а также риски повторной идентификации и правовые аспекты использования обезличенных данных. В документе также представлены рекомендации для компаний, которые выстраивают или пересматривают процессы обезличивания. Отдельный раздел доклада посвящен правовым аспектам обезличивания персональных данных. Эксперты отмечают, что регуляторные требования в этой области продолжают развиваться, а их практическое применение требует учета как рекомендаций регулятора, так и внутренних процессов организаций.	22.01.2026 - публикация в "Библиотека практик" АБД

№	Наименование	Описание	Статус
9.7	Статья Алексея Мунтяна «Квантовая механика информационной приватности: Корпускулярно-волновой дуализм персональных данных и тензорная теория регулирования»	□ Представьте, что законы о персональных данных (все эти галочки «Я согласен») написаны для мира, где информация — это физический предмет, как кирпич или письмо в конверте. Если затереть на конверте имя (анонимизировать), то никто не узнает, чье оно. Это «ньютоновская механика» — старый, понятный мир. □ Но мы живем в цифровом мире. Здесь данные ведут себя не как кирпичи, а как свет или волна в квантовой физике. Они могут быть в двух местах одновременно, менять свои свойства в зависимости от того, кто на них смотрит, и мгновенно связываться друг с другом. □ Автор статьи попытался собрать разрозненные мысли научного сообщества в единую Тензорную теорию регулирования обработки персональных данных, которая предлагает перестать безуспешно обновлять аналоговые законы и мучить людей бесконечной дачей согласий на обработку их данных. Вместо этого может применяться цифровая автоматика регулирования оборота данных, работающая по законам физики и математики: 1□ Она взвешивает данные по «массе» (уникальность и чувствительность). 2□ Смотрит на «скорость» их циркуляции и использования. 3□ Сверяет различные «направления» (цели и контекст) использования данных. ♣ Если риск (импульс) использования данных слишком велик или направление не совпадает — система просто не даст обработать данные. Это превращает защиту приватности из бюрократии в точную науку.	02.02.2026 - публикация в "Альманахе" Privacy Advocates

№	Наименование	Описание	Статус
9.8	Калькулятор Индекса атрибутивности данных	Это инструмент, который оценивает вероятность того, что конкретный набор данных позволит нам узнать (определить) конкретного человека. □ Формула расчета Индекса: $\text{Индекс} = \text{Свойства данных} \times \text{Контекст}$ □ Свойства («масса») данных: насколько данные уникальны и неизменны. □ Контекст (мультипликатор): есть ли у нас техническая возможность и юридическая цель связать эти данные с человеком. □ Три зоны риска обработки данных: □ Зеленая зона (низкий индекс): мы обрабатываем данные, но не знаем людей. Требования 152-ФЗ нас почти не касаются. □ Желтая зона (средний индекс): имен нет, но мы можем «вычислить» человека или его устройство. Закон начинает действовать. □ Красная зона (высокий индекс): мы точно знаем, чьи данные обрабатываем. Включается полный спектр требований регулятора. □ Зачем использовать этот индекс? 1. «Счетчик калорий» для данных (Data Minimization). Индекс работает как диета для баз данных. Каждое лишнее поле (даже «безобидное») повышает балл риска. Это наглядно объясняет маркетингу и HR: сбор данных «на всякий пожарный» — это не бесплатно, а юридически дорого. Решение: удалять лишнее или снижать точность (например, диапазон возраста вместо даты рождения), чтобы вернуться в «зеленую зону». 2. Справедливость и экономия (Privacy by Design). Индекс математически доказывает: уникальность данных $\neq$ персональные данные. Если мы храним сложные хеши или GUID сессий, но используем их только для техподдержки (контекст!), а не для поиска человека, риск остается низким. Это позволяет не тратить бюджет на защиту технических логов так же строго, как на защиту кадровой базы. □ Индекс атрибутивности помогает провести четкую черту в спорных ситуациях и подходить к работе с данными осознанно, фокусируя защиту там, где это действительно необходимо для приватности людей.	17.02.2026 - публикация в "Альманахе" Privacy Advocates

№	Наименование	Описание	Статус
9.9	Статья Алексея Мунтяна «Цена защиты: как дело РЖД демонстрирует новый подход судов к утечкам данных»	□ Дело РЖД формально не создает прецедента, а спор рассматривался в арбитражном суде, тогда как с 1 января 2026 года дела по утечкам и другим нарушениям в области персональных данных возвращаются в ведение судов общей юрисдикции, но для бизнеса это дело еще раз показывает актуальность того, что утечка — это не «если», а «когда». Также можно сформулировать ряд практических выводов для бизнеса: 1. Документирование превентивных мер. Компаниям необходимо иметь четкую, актуальную и документально подтвержденную историю выполнения мероприятий и внедрения мер защиты персональных данных. В случае инцидента именно эти документы станут главным аргументом, подтверждающим, что бизнес принял все зависящие от него меры для недопущения утечки. 2. Проактивная позиция при инцидентах. Замалчивание утечки — худшая стратегия. Подача заявления в правоохранительные органы, информирование уполномоченных органов (Роскомнадзор, Национальный координационный центр по компьютерным инцидентам) и активное содействие расследованию инцидента становятся необходимыми элементами юридической защиты компании и ее партнеров. 3. Обоснование мастерства кибератаки. В суде потребуются доказывать не просто факт взлома систем компании, а уровень его сложности и профессионализма: использование злоумышленниками специфического ПО, обход существующих (и работающих) контуров безопасности, изощренность техник кибератаки.	21.02.2026 - публикация в Forbes

№	Наименование	Описание	Статус
9.10	Презентация Алексея Мунтяна «Копипаст личности: Правовой статус дипфейков дома и за рубежом»	В презентации кратко освещено следующее: □ Масштаб угрозы и эволюция мошенничества □ Анатомия синтетических личностей □ Риски тотальной криминализации дипфейков □ Переход к прозрачности: маркировка дипфейков □ Административная ответственность и терминология □ Глобальный ландшафт регулирования □ Саморегулирование платформ и медиаиндустрии □ Баланс интересов	27.02.2026 - публикация в "Альманахе" Privacy Advocates
9.11	Форма предварительной оценки (чек-лист) соблюдения третьими лицами требований к обработке и защите персональных данных	Чек-лист состоит из 15 основных и дополнительных контролей соблюдения третьими лицами требований к обработке и защите ПД, объединённых в три раздела: 1. Базовые требования (при любой передаче ПД) 2. Дополнительные требования при поручении обработки ПД 3. Дополнительные требования при трансграничной передаче ПД	02.03.2026 - публикация в "Альманахе" Privacy Advocates
9.12	Требования к обезличиванию ПД и методы обезличивания ПД с 01.09.2025	Схема, описывающая регуляторные требования к обезличиванию ПД и методы обезличивания ПД в РФ.	11.03.2026 - публикация в "Альманахе" Privacy Advocates

№	Наименование	Описание	Статус
9.13	Презентация Алексея Мунтяна «Квантовая механика информационной приватности: почему данные — это цифровой океан, а не песок?»	□ Мир цифровых данных изменился, и старые подходы к защите (как сортировка песчинок) больше не работают. □ Алексей Мунтян, управляющий Privacy Advocates, предлагает взглянуть на приватность через призму физики цифрового потока - в продолжение статьи о Корпускулярно-волновом дуализме персональных данных и тензорной теории регулирования. □ Данные имеют агрегатные состояния: □ Твёрдое (архивы): минимальная кинетическая энергия, но огромный потенциал риска. □ Жидкое (активные БД): текут, но сдерживаются «вязкостью» регуляций. ▲ Газообразное (API): стремятся заполнить весь доступный объём. □ Плазма (ИИ): данные необратимо отрываются от контекста, как электроны от атома. □ Опасные переходы: Утечка архива — это сублимация (мгновенный переход из льда в газ). А обучение ИИ — это ионизация, после которой данные начинают жить своей жизнью. □ Эффект стазиса: Когда скорость потока данных запредельна, система защиты может «замереть» — она фиксирует атаку, но не успевает на неё среагировать. □ Что делать? Переходить к тензорному регулированию. Вместо статичных бумажек — математическая оценка рисков через вектор целей, массу и скорость данных. □ Приватность будущего — это не запреты, а «умные контейнеры» и цифровые силовые поля.	20.03.2026 - публикация в "Альманахе" Privacy Advocates

№	Наименование	Описание	Статус
9.14	Электронная почта, мессенджеры и ВКС: как использовать без нарушений законодательства о ПД?	□ Разобрали четыре ключевых вопроса, которые возникают у операторов ПД при работе с коммуникационными сервисами: Можно ли вообще передавать ПД через почту, мессенджеры и ВКС — и что не так с личными аккаунтами сотрудников? Распространяются ли требования о локализации и трансграничной передаче на переписку в иностранных сервисах? Когда мессенджер или почтовый сервис становится ИСПД — а когда нет? Запрет на использование иностранных мессенджеров для информирования граждан и особенности статуса национального мессенджера (МАХ) □ В материале — актуальные позиции Роскомнадзора и Минцифры 2025-2026 гг., анализ рисков и конкретные рекомендации.	24.03.2026 - публикация в "Альманахе" Privacy Advocates
9.15	Обновленный проект Положения об организации обработки и обеспечении безопасности персональных данных	□ Что внутри документа? □ Информационная брошюра, созданная для того, чтобы персоналу было легче познакомиться с Положением и сфокусироваться на наиболее важных аспектах работы с ПД. □ Детальный текст проекта Положения, включающий 12 разделов. □ Главные фишки Положения: □ В Положении применяется эффективный механизм распределения ролей при работе с ПД — модель RACI (Исполнитель, Ответственный, Консультирующий, Уведомляемый). □ Каждый тематический раздел (со 2 по 11) обязательно включает: применяемые правила с нормативными ссылками, распределение ролей, перечень документированной информации (артефакты) и связанные документы. □ Документ может использоваться и модифицироваться любыми заинтересованными лицами без ограничений, при условии добросовестного использования.	31.03.2026 - публикация в "Альманахе" Privacy Advocates

№	Наименование	Описание	Статус
9.16	Регулирование авторизации пользователей на информационных ресурсах в РФ	□ С 01.12.2023 вступили в силу требования к способам входа на российские информационные ресурсы. □ Что разрешено: □ Номер мобильного телефона □ ЕСИА (портал Госуслуг) □ ЕБС (биометрические данные) □ Собственные системы авторизации (VK ID, Яндекс ID и др.) □ Email на российском домене (законопроект) □ Что запрещено: Apple ID, Google Sign-In и прочие иностранные сервисы авторизации на российских ресурсах □ Кого касается: Российские компании и ИП – владельцы сайтов, приложений, информационных систем и ПО	07.04.2026 - публикация в "Альманахе" Privacy Advocates
9.17	Регулирование рекомендательных технологий в РФ	□ Рекомендательные технологии (РТ) – комплекс алгоритмов, которые анализируют ваши предпочтения и предсказывают, что вас заинтересует. Это социальные сети, видеохостинги, маркетплейсы, стриминговые платформы, поисковые системы. □ Что запрещено: □ Применять алгоритмы, нарушающие права граждан □ Использовать РТ для распространения фейков и контента, нарушающего законодательство РФ □ Искусственно создавать «информационные пузыри», ограничивающие взгляды пользователя □ Что обязательно: 1□ Опубликовать правила применения РТ (на русском, доступно, без скрытия) - описание процессов сбора данных о предпочтениях - методы обработки информации - виды и источники данных 2□ Разместить уведомление на всех страницах - текст: «На информационном ресурсе применяются рекомендательные технологии» - ссылка на подробное описание ⚠ Ответственность: Роскомнадзор направляет требования об устранении нарушений. При неисполнении – блокировка ресурса. □ Кого касается: российские компании и ИП – владельцы любых интернет-ресурсов, использующих РТ для пользователей в РФ.	08.04.2026 - публикация в "Альманахе" Privacy Advocates

№	Наименование	Описание	Статус
9.18	Эффективное управление рисками обработки персональных данных	□ Три кита дата-прагматизма: — Классический privacy-комплаенс — Бережливая обработка данных — Технологии защищённой обработки данных (ТЗОД) ✂ Ключевой алгоритм включает три этапа: 1□ анализ контекста и интенсивности обработки 2□ выявление отклонений 3□ управление рисками □ Оценка риска строится на двух параметрах: — виктимность обработки = насколько «привлекательна» ваша обработка для злоумышленников и регулятора — критичность отклонений = насколько существенны нарушения требований □ Excel-калькулятор рисков обработки ПД — готовый инструмент для самостоятельной оценки любого процесса обработки персональных данных в вашей организации. Три листа: анализ обработки → выявление отклонений → управление рисками. Баллы и уровень риска считаются автоматически. □ Обучающий материал к калькулятору — пошаговые инструкции на живом кейсе: совместная маркетинговая кампания через платформу Marketo с участием двух компаний. Разбираем все 10 параметров анализа и 10 групп контролей с подсказками и примерами. □ Схема алгоритма риск-менеджмента обработки ПД — наглядная карта трёх этапов с полным перечнем параметров, баллами и инсайтами. Удобна как памятка при проведении оценки и как материал для обучения команды.	08.04.2026 - публикация в "Альманахе" Privacy Advocates

№	Наименование	Описание	Статус
9.19	New Материал «Регулирование оборота биометрических персональных данных в РФ» в «Альманахе» Privacy Advocates	□ Понятие и виды биометрии — статические (отпечатки пальцев, радужка, геном, фото) и динамические (голос, подпись, поведенческие паттерны) характеристики в контексте ч. 1 ст. 11 152-ФЗ. □ Позиции ведомств — сравнительная таблица писем Минцифры и Роскомнадзора по вопросу: является ли фотография биометрическими персональными данными? Спойлер: единого ответа до сих пор нет. ⚖ Судебная практика — два массива дел: когда суды признавали сведения биометрией (фото на пропусках, рисунок вен, видеозаписи с камер в общей собственности) и когда — нет (городские камеры МВД, видео с мобильного телефона, запись спящего сотрудника). □ Прецедент с ФСБ и Росгвардией — разбор реального дела 2022 г.: бизнес-центр «Зеленоград», 170 фотографий детей без согласия родителей, штраф по ч. 2 ст. 13.11 КоАП РФ. □ ЕБС и 572-ФЗ — типы биометрии (упрощённая, стандартная, подтверждённая), транзакционная и векторная модели взаимодействия, требования по аккредитации. □ 7 ограничений при встраивании биометрии в ИТ/ИИ-продукты: закрытый перечень ЕБС, запрет трансграничной передачи, обязательная аккредитация, особый режим согласия, защита несовершеннолетних, пределы точности (FAR/FRR), только векторная модель для аккредитованных. ⚠ 7 ключевых рисков: необратимость утечки, штрафы до 500 млн ₽ и уголовная ответственность, дискриминация ИИ-моделей по данным NIST FRVT, deepfake-атаки, function creep, репутационные риски, прокурорские проверки. □ Рекомендации для продуктовых команд — архитектурные (on-device, векторное хранение, liveness-детекция) и процессные (оценка рисков до запуска, журналы согласий, уведомление РКН в 24/72 ч.).	16.04.2026 - публикация в "Альманахе" Privacy Advocates

№	Наименование	Описание	Статус
9.20	^{New} Расширение Каталога персональных данных в «Альманахе» Privacy Advocates: новые группы ПД	□ В Каталог ПД добавлены новые группы персональных данных: □ 125. Нейроданные потребительского характера □ 139. Нейроданные медицинского характера □ 154. Данные запахов тела и состава выдыхаемого воздуха □ 155. Данные дыхания □ 156. Данные движения губ □ 157. Данные микровибрации пальцев □ 158. Данные акустического отклика среднего уха □ 159. Данные биоакустической подписи □ 160. Данные структуры кожи и эпителия □ 161. Данные биохимических характеристик □ 162. Данные динамики подписи □ 172. Нейроданные биометрического характера □ Расширение каталога отражает развитие технологий распознавания и идентификации (включая нейроинтерфейсы), что требует пересмотра подходов к классификации ПД и оценке рисков их обработки.	29.04.2026 - публикация в "Альманахе" Privacy Advocates

From:

<https://wiki.privacy-advocates.ru/> - Privacy Advocates | Альманах

Permanent link:

<https://wiki.privacy-advocates.ru/dst2026>

Last update: 2026/05/18 12:34

