Дата поступления рукописи в редакцию: 05.06.2026 г. **DOI: 10.24412/2949-0871-2026-4-23-30**
Дата принятия рукописи в печать: 11.09.2026 г.

РОЧЕВА София Сергеевна,
бакалавр Высшей школы юриспруденции и судебно-технической экспертизы,
Санкт-Петербургский политехнический университет Петра Великого,
Санкт-Петербург, Россия,
e-mail: snrchv@gmail.com

ПРИМЕНЕНИЕ ЗАРУБЕЖНОГО ОПЫТА ПРАВОВОГО РЕГУЛИРОВАНИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В РОССИЙСКОЙ ПРАВОВОЙ СИСТЕМЕ

АННОТАЦИЯ. В статье рассматриваются пределы и условия применения зарубежного опыта правового регулирования защиты персональных данных в российской правовой системе после законодательных изменений 2025 г., затронувших согласие субъекта, локализацию баз данных, обезличивание сведений, административную ответственность операторов и правовой режим высокорисковой цифровой обработки. Особое внимание уделено соотношению российских реформ с зарубежными механизмами подотчетности контролера, оценки воздействия на защиту данных, трансграничных гарантий, алгоритмической прозрачности и риск-ориентированного надзора. Методологическую основу исследования составили формально-юридический, сравнительно-правовой, системный методы и элементы функционального анализа правовых конструкций. Формально-юридический метод использован для оценки действующих обязанностей оператора по Федеральному закону от 27 июля 2006 г. № 152-ФЗ «О персональных данных» в редакции с учетом изменений 2024-2025 гг.; сравнительно-правовой метод позволил сопоставить российскую модель регулирования с подходами Европейского союза, Совета Европы, Бразилии, Калифорнии и Китайской Народной Республики; системный метод применен для определения места зарубежных механизмов в российской системе конституционных гарантий, информационного законодательства, административного надзора и локального регулирования деятельности операторов. Научная новизна выражается в обосновании постреформенной модели функциональной адаптации зарубежного опыта, при которой иностранные правовые механизмы оцениваются не как образцы для законодательного копирования, а как инструменты восполнения конкретных пробелов российского регулирования. Обоснован вывод о том, что после реформ 2025 г. перспективными направлениями развития остаются риск-профилирование операций обработки, методически оформленная оценка воздействия при высокорисковой обработке, внутреннее заключение о допустимости трансграничной передачи, содержательная алгоритмическая прозрачность и специальные гарантии против повторной идентификации обезличенных данных.

КЛЮЧЕВЫЕ СЛОВА: персональные данные, защита данных, российское право, зарубежный опыт, реформа 2025 года, подотчетность оператора, оценка воздействия, обезличенные данные, трансграничная передача, автоматизированная обработка.

ROCHEVA Sofia Sergeyevna,
Bachelor, Higher School of Jurisprudence and Forensic Technical Expertise,
Peter the Great St. Petersburg Polytechnic University,
St. Petersburg, Russia

APPLICATION OF FOREIGN EXPERIENCE IN THE LEGAL REGULATION OF PERSONAL DATA PROTECTION WITHIN THE RUSSIAN LEGAL SYSTEM

ANNOTATION. The article examines the limits and conditions for applying foreign experience regarding the legal regulation of personal data protection within the Russian legal system following the legislative changes of 2025. These changes affected data subject consent, database localization, data anonymization, the administrative liability of data controllers (operators), and the legal regime governing high-risk digital processing. Particular attention is paid to the relationship between Russian reforms and foreign mechanisms concerning controller accountability, data protection impact assessments, cross-border safeguards, algorithmic transparency, and risk-based supervision. The methodological framework of the study comprises formal-legal, comparative-legal, and systemic methods, alongside elements of the functional analysis of legal constructs. The formal-legal method was used to assess the current obligations of data controllers under Federal Law No. 152-FZ of July 27, 2006, «On Personal Data,» as amended in 2024–2025; the

comparative-legal method enabled a comparison of the Russian regulatory model with approaches adopted by the European Union, the Council of Europe, Brazil, California, and the People's Republic of China; and the systemic method was applied to determine the place of foreign mechanisms within the Russian system of constitutional guarantees, information legislation, administrative supervision, and the internal regulation of data controller activities. The scientific novelty lies in the substantiation of a post-reform model for the functional adaptation of foreign experience, wherein foreign legal mechanisms are evaluated not as templates for legislative replication, but as tools to address specific gaps in Russian regulation. The study substantiates the conclusion that, following the 2025 reforms, promising areas for development include risk profiling of processing operations, methodologically structured impact assessments for high-risk processing, internal assessments regarding the permissibility of cross-border transfers, substantive algorithmic transparency, and specific safeguards against the re-identification of anonymized data.

KEY WORDS: personal data, data protection, Russian law, foreign experience, 2025 reform, controller accountability, impact assessment, anonymized data, cross-border transfer, automated processing.

Развитие цифровой экономики, платформенных сервисов, биометрической идентификации, искусственного интеллекта и государственных информационных систем существенно изменило содержание правовой охраны персональных данных. В современных условиях личная информация сохраняет значение объекта конфиденциальности, одновременно приобретая статус ресурса административного управления, коммерческой аналитики, кредитного скоринга, медицинской диагностики, образовательных платформ, маркетинговой сегментации и алгоритмического прогнозирования поведения граждан. Вследствие подобной трансформации правовое регулирование персональных данных постепенно смещается от модели разового согласия к модели управляемого жизненного цикла данных, включающей оценку риска, документирование решений оператора, проверяемость обработки, контроль трансграничных потоков и защиту субъекта от непрозрачных автоматизированных решений.

Указанное изменение технологической среды непосредственно влияет на постановку исследовательской проблемы. Если ранее сравнительно-правовой анализ чаще строился вокруг вопроса о возможности заимствования европейской модели защиты данных, то в настоящее время подобный подход нуждается в уточнении. Российское законодательство в 2024-2025 гг. существенно усилило публично-правовую составляющую регулирования: Федеральным законом от 30 ноября 2024 г. № 420-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» расширена административная ответственность за нарушения в сфере персональных данных; Федеральным законом от 28 февраля 2025 г. № 23-ФЗ «О внесении изменений в Федеральный закон «О персональных данных» и отдельные законодательные акты Российской Федерации» введены новые положения об обезличенных данных и изменены правила локализации отдельных операций с персональными данными граждан Российской Федерации; Федеральным законом от 24 июня 2025 г. № 156-ФЗ «О создании многофункционального сервиса обмена информацией и о внесении изменений в отдельные законодательные акты Российской Федерации» закреплено требование об отдельном оформлении согласия на обработку персональных данных, поэтому зарубежный опыт уже не может рассматриваться как внешний образец для прямого переноса; он должен оцениваться через способность усилить ту модель, которая формируется в российском праве после названных реформ.

В научной литературе защита персональных данных традиционно раскрывается через несколько взаимосвязанных плоскостей: правовой статус субъекта, обязанности оператора, пределы цифрового оборота сведений, институциональная роль надзорного органа и соотношение частноправовых и публично-правовых средств защиты. Э. В. Талапина подчеркивает, что российское регулирование персональных данных развивается в европейском контексте, однако не может сводиться к формальному воспроизведению внешних правовых моделей [1, с. 124]. Данная позиция сохраняет значение и после реформ 2025 г., поскольку обновление российского законодательства не отменяет сравнительно-правовой перспективы, но требует более строгого отбора зарубежных механизмов. В развитие рассматриваемого подхода А. В. Минбалеев указывает на необходимость модернизации законодательства с учетом новых технологических угроз, включая обработку больших массивов данных, нейросетевые технологии и возрастание риска неправомерного использования персональной информации [2, с. 86].

Логическим продолжением названной дискуссии становится вопрос о том, за счет каких регулятивных средств возможно обеспечить не декларативную, а проверяемую защиту субъекта персональных данных. В данном отношении показательно исследование И. А. Шелудченко, где защита персональных данных рассматривается через призму делегированного правотворчества: автор обращает внимание на возрастающую зависимость фактической эффективности регулирования от подзаконных, методических, технических и организационных правил, конкретизирующих поведение операторов [3, с. 82]. Следовательно, при оценке зарубежного опыта

принципиально важно учитывать содержание заимствуемой нормы в связи с инфраструктурой ее исполнения: методическими разъяснениями, надзорной проверкой, локальными процедурами и профессиональной практикой операторов.

Переход от общего сравнения правопорядков к анализу исполнимых механизмов особенно заметен в условиях формирования экономики данных. С. А. Быстрякова справедливо связывает развитие правового регулирования персональных данных с расширением цифрового оборота информации и необходимостью поиска баланса между экономической ценностью данных и гарантиями прав граждан [4, с. 180]. Названная позиция позволяет уточнить предмет настоящего исследования: зарубежный опыт интересен не сам по себе, а постольку, поскольку он помогает определить процедуры, способные соединить технологическую обработку с правовой проверяемостью, минимизацией рисков и реальным контролем субъекта над собственными сведениями.

Переход к подобной постановке вопроса требует разграничения правовой трансплантации и функциональной адаптации: в теории сравнительного правоведения правовая трансплантация традиционно понимается как перенос нормы либо института из одной системы в другую. Однако критики данной концепции обоснованно указывают, что норма не существует вне языка правопорядка, судебной практики, административных процедур, профессиональной культуры и институциональной среды [5, с. 114]. Применительно к персональным данным данное возражение приобретает особое значение: подотчетность, оценка воздействия, алгоритмическая прозрачность или договорные гарантии трансграничной передачи не являются самодостаточными формулами. Их результативность зависит от методики оценки, компетентного надзора, локальных регламентов, ответственных подразделений оператора, понятных критериев проверки и санкционного механизма.

Из чего следует, что функциональная адаптация зарубежного опыта должна строиться не на внешнем сходстве правовых конструкций, а на проверке их пригодности для российской правовой системы. Первый критерий проверки – конституционная совместимость, предполагающая соответствие заимствуемого механизма гарантиям неприкосновенности частной жизни, личной и семейной тайны, судебной защиты и допустимых пределов ограничения прав. Второй критерий – институциональная исполнимость, выражающая способность оператора выполнить обязанность без чрезмерной нагрузки, особенно если речь идет о малом и среднем бизнесе, образовательных, медицинских и муниципальных организациях. Третий критерий – надзорная проверяемость, позволяющая Роскомнадзору оценить соблюдение требования не декларативно, а через документы, журналы учета, локальные акты, отчеты об инцидентах и внутренние заключения оператора. Четвертый критерий – технологическая нейтральность, обеспечивающая применимость нормы к биометрии, искусственному интеллекту, облачным сервисам, рекомендательным алгоритмам, цифровым профилям и будущим технологиям без постоянного фрагментарного изменения закона. Пятый критерий – правозащитная результативность, предполагающая способность механизма снижать реальный риск утечки, повторной идентификации, дискриминационного профилирования, незаконной трансграничной передачи либо принятия юридически значимого решения без понятного для субъекта объяснения.

После определения методологических критериев становится возможным перейти к конкретным зарубежным механизмам, сохраняющим значение для российского права после реформ 2025 г. Первым среди них выступает подотчетность контролера. В европейской модели данная категория охватывает обязанность соблюдать требования закона и одновременно предполагает способность доказать соблюдение правовых принципов применительно к конкретным операциям обработки. Л. А. Байгрейв характеризует современное право защиты данных как систему, в которой формальные права субъекта должны обеспечиваться организационными обязанностями лица, определяющего цели и средства обработки [6, с. 74]. О. Лински, развивая сходную позицию, связывает европейское регулирование с переходом от узкого понимания конфиденциальности к более широкой модели институциональной ответственности за информационную власть [7, с. 97]. Для российского права данный подход имеет существенное значение, однако его нельзя представлять как полностью отсутствующий: ст. 18.1 Федерального закона № 152-ФЗ уже закрепляет обязанность оператора принимать необходимые и достаточные меры, издавать локальные акты, осуществлять внутренний контроль, оценивать возможный вред и подтверждать принятие мер по запросу уполномоченного органа.

Именно по данной причине практическая адаптация подотчетности должна состоять не в простом введении новой обязанности, а в конкретизации уже имеющегося регулирования применительно к высокорисковым операциям обработки. В российской модели следует развивать не общий массив документов для всех операторов, а риск-профиль обработки, включающий цель, правовое основание, категории данных, категории субъектов, срок хранения, круг получателей, техническую инфраструктуру, наличие трансграничного элемента, вероятность повторной идентификации, использование автоматизированного решения и меры минимизации вреда. Предложенная конструкция не дублирует ст. 18.1 Федерального закона № 152-ФЗ, а наполняет уже существующую обязанность содержанием, при-

годным для последующей надзорной проверки.

Следующим элементом, связанным с подотчетностью, выступает оценка воздействия на защиту данных. Если подотчетность отвечает на вопрос о том, способен ли оператор подтвердить правомерность своих действий, то оценка воздействия позволяет определить, были ли риски выявлены до начала обработки. В европейском праве данная процедура применяется при обработке, способной создать высокий риск для прав и свобод физических лиц, особенно при использовании новых технологий, масштабной обработке чувствительных сведений, систематическом наблюдении и профилировании. Современные зарубежные исследования показывают, что оценка воздействия должна пониматься не как технический отчет, а как инструмент защиты фундаментальных прав, позволяющий заранее выявить риск дискриминации, непропорционального вмешательства и утраты субъектом контроля [8, с. 8].

Вместе с тем оценка воздействия не должна механически переноситься в российское законодательство в максимально широком виде. Если распространить ее на любую обработку персональных данных, она быстро превратится в формальный документ и увеличит административную нагрузку без очевидного правозащитного результата, поэтому для российской системы более обоснован ограниченный, риск-ориентированный вариант: оценка воздействия должна проводиться при масштабной обработке специальных категорий персональных данных, биометрии, данных несовершеннолетних, медицинской и финансовой информации, скоринге, профилировании, обработке для целей машинного обучения, трансграничной передаче в юрисдикции с неопределенным уровнем защиты и использовании автоматизированных решений, влияющих на доступ к работе, кредиту, социальной выплате, образованию или медицинской помощи. В указанном смысле зарубежная модель DPIA может быть адаптирована не как буквальный аналог европейского регулирования, а как российская процедура оценки высокорисковой обработки, соотнесенная со ст. 18.1, ст. 19 и ст. 21 Федерального закона № 152-ФЗ.

Из процедуры оценки риска закономерно вытекает вопрос о трансграничной передаче персональных данных, поскольку именно при выходе сведений за пределы национальной юрисдикции контроль субъекта и надзорного органа объективно осложняется. После изменений последних лет российское право уже содержит достаточно развитую уведомительную и оценочную конструкцию, поэтому предложение о простом усилении уведомления не обладало бы научной новизной. Более точным является вопрос о содержании внутреннего вывода оператора: каким образом он устанавливает допустимость передачи, оценивает получателя, правовой режим иностранного государства, договорные гарантии, меры конфиденциальности, срок хранения, дальнейшие операции и способы защиты субъекта. К. Кунер обоснованно показывает, что трансграничные потоки данных находятся в поле конфликта между защитой частной жизни, экономической необходимостью обмена информацией и различием национальных режимов надзора [9, с. 889]. В развитие рассматриваемой позиции Л. Брэдфорд, М. Абой и К. Лидделл отмечают, что договорные конструкции остаются важным инструментом трансграничной передачи, но нуждаются в связи с оценкой фактической способности импортера соблюдать гарантии защиты [10, с. 17].

Для российской правовой системы перспективна не механическая рецепция европейских стандартных договорных условий, а введение внутреннего заключения о допустимости трансграничной передачи как части документационного досье оператора. Данное заключение должно фиксировать правовое основание передачи, цель, получателя, категорию данных, срок дальнейшего хранения, применяемые организационные и технические меры, порядок реагирования на запросы субъекта, условия прекращения обработки и механизм ответственности иностранного получателя. Подобный документ не заменяет уведомление Роскомнадзора, но делает уведомительную процедуру содержательной, поскольку оператор заранее формирует аргументированную позицию о допустимости передачи и сохраняет ее для последующей проверки.

Наряду с трансграничной передачей особое значение приобретает автоматизированная обработка, поскольку алгоритмические решения способны воздействовать на права субъекта менее заметно, чем традиционные формы сбора и передачи сведений. В российском праве уже существует ст. 16 Федерального закона № 152-ФЗ, посвященная решениям, принимаемым исключительно на основании автоматизированной обработки персональных данных. Следовательно, предложение просто закрепить право на защиту от автоматизированного решения было бы некорректным. Проблема заключается в другом: современная цифровая практика редко сводится к полностью автоматическому решению. Алгоритм может не принимать окончательный акт, но фактически предопределять человеческий выбор через рейтинг, скоринговый балл, цифровой профиль, категорию риска, рекомендацию, предварительный отказ или автоматическое ранжирование.

Данная проблема усиливается нестабильностью границы между персональной и неперсональной информацией. П. М. Шварц и Д. Дж. Солов указывают, что сведения, первоначально не позволяющие идентифицировать лицо, могут приобрести идентифицирующее значение после сопоставления с иными массивами данных [11, с. 1836]. В контексте алгоритмической обработ-

ки данное означает, что субъект может не понимать, какие данные повлияли на результат, почему система отнесла его к определенной группе и каким образом он может оспорить вывод. Российская дискуссия по автоматизированной обработке уже поднимает вопрос о недостаточной конкретизации прав субъекта при принятии решений на основании алгоритмической обработки [12, с. 110]. Одновременно исследования персональных данных в связи с искусственным интеллектом показывают, что ключевым риском является не только утечка информации, но и непрозрачное использование данных для машинного анализа, прогнозирования, классификации и последующего юридически значимого решения [13, с. 72].

Поэтому адаптация зарубежного опыта должна состоять не в требовании раскрывать программный код или математическую модель, а в закреплении минимального стандарта юридически значимой информации. Оператор должен предоставлять субъекту сведения о факте использования автоматизированной обработки, категориях использованных данных, общем характере факторов, повлиявших на результат, возможных юридических последствиях, порядке подачи возражения и лице либо подразделении, ответственном за пересмотр. В зарубежной литературе право на объяснение и человеческое участие рассматривается как один из наиболее сложных элементов регулирования искусственного интеллекта, поскольку чрезмерное требование раскрытия алгоритма может конфликтовать с коммерческой тайной, а слишком общее уведомление не обеспечивает субъекту реальной защиты [14, с. 229]. Для высокорисковых сфер – кредитование, трудоустройство, образование, медицина, социальные выплаты, страхование – требуется не декларативное рассмотрение возражения, а мотивированный пересмотр с участием уполномоченного работника, способного оценить доводы субъекта и при необходимости изменить результат.

Если алгоритмическая обработка демонстрирует сложность объяснения решений, то обезличивание персональных данных раскрывает иную сторону той же проблемы – невозможность считать цифровой риск устраненным за счет одного лишь изменения формы сведений. Российские изменения 2025 г. придали обезличенным данным особое значение, поскольку данная процедура стала рассматриваться как способ снижения риска и одновременно как инструмент формирования составов данных для государственных информационных систем и развития экономики данных. В научной литературе уже отмечается, что правовой режим обезличенных персональных данных не может строиться на презумпции полной безопасности, поскольку современные технологии сопоставления массивов информации сохраняют риск повторной идентификации [15, с. 47]. В. Ю. Туранин характеризует обезличивание как правовой эксперимент, в рамках которого необходимо учитывать возможности развития данных и риски неконтролируемого оборота информации [16, с. 643]. Е. В. Полуянова, анализируя современные подходы к обезличиванию, обращает внимание на необходимость специальной регламентации данной процедуры, поскольку формальное удаление прямых идентификаторов не всегда исключает восстановление связи между сведениями и конкретным лицом [17, с. 423].

Зарубежный опыт в данной части полезен прежде всего через идею непрерывной оценки риска повторной идентификации. Обезличивание не должно пониматься как разовое техническое действие, поскольку оно образует правовой и организационно-технический режим, зависящий от состава исходных данных, доступности дополнительных массивов, числа получателей, способов преобразования сведений, целей последующего использования, длительности хранения и вероятности обратного сопоставления. Для российской правовой системы перспективным является закрепление требований к методам обезличивания в сочетании с процедурным стандартом контроля: оператор должен оценивать риск повторной идентификации до передачи обезличенного массива, после изменения целей использования и при расширении круга получателей. Подобная модель позволит соединить развитие экономики данных с гарантиями частной жизни без ложной презумпции, согласно которой обезличенные сведения всегда утрачивают правозащитную значимость.

Рассмотрение обезличивания, автоматизированной обработки и трансграничной передачи подводит к более общей проблеме – соотношению согласий и отраслевых стандартов. В российской правовой политике 2025 г. отчетливо проявилась критика модели множественных согласий, поскольку гражданин фактически не способен контролировать большое количество разрешений, данных разным операторам в цифровой среде. Однако отказ от абсолютизации согласия не означает снижение уровня защиты. Напротив, он предполагает перенос центра тяжести на законные цели обработки, минимизацию собираемых сведений, отраслевые правила, сроки хранения, запреты на избыточный сбор, обязательные локальные процедуры и надзорную проверяемость. В сравнительно-правовой литературе подобный сдвиг соответствует общей тенденции перехода от индивидуалистической модели «самоуправления приватностью» к институциональной модели управления информационными рисками. Д. Солов указывает, что приватность не может эффективно защищаться только через индивидуальный выбор, поскольку субъект часто не располагает достаточной информацией и реальной переговорной силой [18, с. 188].

Критика модели согласия получает развитие и в исследованиях, посвященных большим данным. Ф. Кейт и В. Майер-Шенбергер отмечают, что традиционная конструкция notice and consent утрачивает эффективность в условиях больших массивов данных, поскольку субъект не способен заранее оценить все будущие способы использования информации [19, с. 69]. И. Рубинштейн, рассматривая Big Data как вызов классическим представлениям о приватности, делает акцент на необходимости перехода от индивидуального контроля к системным гарантиям управления рисками [20, с. 77]. Следовательно, российская модель отдельного согласия, несмотря на свое значение, не должна восприниматься как окончательное решение проблемы: она нуждается в дополнении отраслевыми стандартами, риск-ориентированным надзором и обязанностями оператора по минимизации данных.

В российской системе данный переход должен быть осторожным. Отраслевые стандарты могут повысить определенность для операторов и граждан, если они будут устанавливать перечень допустимых целей, минимальный состав данных, сроки хранения, условия передачи третьим лицам, требования к уничтожению, порядок ответа субъекту и признаки высокорисковой обработки. Вместе с тем передача слишком широких правил на уровень подзаконного или методического регулирования способна вызвать риск размывания законодательных гарантий, по данной причине отраслевые стандарты должны рассматриваться как способ конкретизации закона, а не как замена основных прав субъекта персональных данных.

Наиболее продуктивная модель применения зарубежного опыта в России после реформ 2025 г. может быть представлена через три уровня. Первый уровень – законодательный, где должны закрепляться базовые права субъекта, критерии высокорисковой обработки, общая обязанность оценки риска, право на содержательное объяснение автоматизированного решения и гарантии против повторной идентификации. Второй уровень – методический, где уполномоченный орган может утверждать рекомендации по оценке воздействия, признакам высокорисковой обработки, структуре внутреннего заключения о трансграничной передаче, минимальному содержанию алгоритмического уведомления и документированию мер оператора. Третий уровень – локальный, где конкретный оператор формирует карту процессов обработки, риск-профили, журналы обращений субъектов, порядок реагирования на инциденты, шаблоны заключений, внутренние регламенты пересмотра автоматизированных решений и процедуры контроля обезличенных массивов.

Практические предложения, вытекающие из проведенного анализа, должны быть сформулированы с учетом действующей редакции Федерального закона № 152-ФЗ, чтобы избежать дублирования уже существующих норм. Во-первых, целесообразно развивать не общую «документальную подотчетность», а специальное досье высокорисковой обработки, включающее описание цели, правового основания, категорий данных, субъектов, получателей, срока хранения, технической инфраструктуры, возможного вреда и мер минимизации. Во-вторых, оценка воздействия на защиту персональных данных должна применяться к ограниченному кругу операций: биометрия, специальные категории данных, данные несовершеннолетних, медицинская и финансовая информация, профилирование, машинное обучение, трансграничная передача в юрисдикции с неопределенными гарантиями и автоматизированные решения с юридически значимым эффектом. В-третьих, при трансграничной передаче необходимо формировать внутреннее заключение о допустимости передачи, не заменяющее уведомление Роскомнадзора, но дополняющее его содержательной оценкой рисков. В-четвертых, ст. 16 Федерального закона № 152-ФЗ нуждается не в повторении уже существующего права на возражение, а в конкретизации состава информации, предоставляемой субъекту при автоматизированной обработке, и в установлении мотивированного пересмотра с участием человека. В-пятых, правовой режим обезличенных данных должен включать оценку риска повторной идентификации и контроль последующего использования обезличенных массивов.

Проведенное исследование позволяет прийти к выводу, что зарубежный опыт защиты персональных данных сохраняет значение для российской правовой системы, но после реформ 2025 г. он должен применяться более избирательно. Российское законодательство уже закрепило существенный массив обязанностей оператора, усилило санкционный режим, конкретизировало согласие, изменило подход к локализации и создало специальный правовой режим обезличенных данных. В данной ситуации научная и практическая ценность сравнительно-правового анализа состоит не в предложении «перенести GDPR», а в выявлении тех процедур, которые способны сделать российскую модель более риск-ориентированной, проверяемой и технологически нейтральной. Наиболее перспективными являются оценка высокорисковой обработки, внутреннее заключение о трансграничной передаче, алгоритмическая прозрачность, мотивированный человеческий пересмотр автоматизированных решений и постоянный контроль риска повторной идентификации обезличенных данных. Именно указанные механизмы позволяют соединить превентивный потенциал зарубежного опыта с внутренней логикой российского законодательства, не создавая искусственного копирования внешних нормативных конструкций.

Список литературы:

[1] Талапина Э. В. Защита персональных данных в цифровую эпоху: российское право в европейском контексте // Труды Института государства и права Российской академии наук. 2018. Т. 13. № 5. С. 117-150.

[2] Минбалеев А. В. Перспективные направления правового регулирования персональных данных // Вестник Университета имени О. Е. Кутафина. 2024. № 1. С. 83-91.

[3] Шелудченко И. А. Защита персональных данных в Российской Федерации сквозь призму делегированного правотворчества // Вестник Московского университета. Серия 11. Право. 2025. № 1. С. 77-99.

[4] Быстрякова С. А. Развитие правового регулирования персональных данных в условиях формирования экономики данных в России // Право и государство: теория и практика. 2024. № 2 (230). С. 179-182.

[5] Legrand P. The Impossibility of Legal Transplants // Maastricht Journal of European and Comparative Law. 1997. Vol. 4. № 2. P. 111-124.

[6] Bygrave L. A. Data Privacy Law: An International Perspective. Oxford: Oxford University Press, 2014.

[7] Lynskey O. The Foundations of EU Data Protection Law. Oxford: Oxford University Press, 2015.

[8] Calvi A. Data Protection Impact Assessment under the EU General Data Protection Regulation: A Feminist Critique // Computer Law & Security Review. 2024. Vol. 53. P. 1-20.

[9] Kuner C. Reality and Illusion in EU Data Transfer Regulation Post Schrems // German Law Journal. 2017. Vol. 18. № 4. P. 881-918.

[10] Bradford L., Aboy M., Liddell K. Standard Contractual Clauses for Cross-Border Transfers of Health Data after Schrems II // Journal of Law and the Biosciences. 2021. Vol. 8. № 1. P. 1-35.

[11] Schwartz P. M., Solove D. J. The PII Problem: Privacy and a New Concept of Personally Identifiable Information // New York University Law Review. 2011. Vol. 86. P. 1814-1894.

[12] Ушаков А. С. К вопросу о правах субъекта персональных данных при принятии решений на основании автоматизированной обработки информации // Образование и право. 2024. № 10. С. 108-112.

[13] Окишев Б. А. Особенности правовой охраны персональных данных, обрабатываемых с использованием технологий искусственного интеллекта // Проблемы экономики и юридической практики. 2024. Т. 20. № 2. С. 70-75.

[14] Škorjanc Ž. A Holistic Approach under the GDPR, AI Act, and Directive 2023/2225 to the Right to Explanation of Credit Scores // Global Privacy Law Review. 2025. Vol. 6. № 3. P. 222-240.

[15] Жирнова Н. А., Солдаткина О. Л. К вопросу о правовом режиме обезличенных персональных данных // Вестник Воронежского государственного университета. Серия: Право. 2024. № 4 (59). С. 44-51.

[16] Туранин В. Ю. Обезличивание персональных данных как правовой эксперимент: риски и возможности // Юридическая техника. 2025. № 19. С. 641-646.

[17] Полуянова Е. В. Актуальные вопросы правового регулирования обезличивания персональных данных // Вестник науки. 2025. Т. 4. № 2. С. 421-426.

[18] Solove D. J. The Digital Person: Technology and Privacy in the Information Age. New York: New York University Press, 2004.

[19] Cate F. H., Mayer-Schönberger V. Notice and Consent in a World of Big Data // International Data Privacy Law. 2013. Vol. 3. № 2. P. 67-73.

[20] Rubinstein I. S. Big Data: The End of Privacy or a New Beginning? // International Data Privacy Law. 2013. Vol. 3. № 2. P. 74-87.

References:

[1] Talapina E. V. Personal Data Protection in the Digital Age: Russian Law in a European Context // Proceedings of the Institute of State and Law of the Russian Academy of Sciences. 2018. Vol. 13. No. 5. P. 117-150.

[2] Minbaleev A. V. Promising Directions for the Legal Regulation of Personal Data // Bulletin of the O. E. Kutafin University. 2024. No. 1. P. 83-91.

[3] Sheludchenko I. A. Personal Data Protection in the Russian Federation through the Prism of Delegated Law-Making // Bulletin of Moscow University. Series 11. Law. 2025. No. 1. P. 77-99.

[4] Bystryakova S. A. Development of Legal Regulation of Personal Data Amidst the Formation of a Data Economy in Russia // Law and State: Theory and Practice. 2024. No. 2 (230). P. 179-182.

[5] Legrand P. The Impossibility of Legal Transplants // Maastricht Journal of European and Comparative Law. 1997. Vol. 4. No. 2. P. 111-124.

[6] Bygrave L. A. Data Privacy Law: An International Perspective. Oxford: Oxford University Press, 2014.

[7] Lynskey O. The Foundations of EU Data Protection Law. Oxford: Oxford University Press, 2015.

[8] Calvi A. Data Protection Impact Assessment under the EU General Data Protection Regulation: A Feminist Critique // Computer Law & Security Review. 2024. Vol. 53. P. 1-20.

[9] Kuner C. Reality and Illusion in EU Data Transfer Regulation Post Schrems // German Law Journal. 2017. Vol. 18. No. 4. P. 881-918. [10] Bradford L., Aboy M., Liddell K. Standard Contractual Clauses for Cross-Border Transfers of Health Data after Schrems II // Journal of Law and the Biosciences. 2021. Vol. 8. No. 1. P. 1-35.

[11] Schwartz P. M., Solove D. J. The PII Problem: Privacy and a New Concept of Personally Identifiable Information // New York University Law Review. 2011. Vol. 86. P. 1814-1894.

[12] Ushakov A. S. On the Rights of the Data Subject Regarding Decisions Based on Automated Information Processing // Education and Law. 2024. No. 10. P. 108-112.

[13] Okishev B. A. Specifics of Legal Protection for Personal Data Processed Using Artificial Intelligence Technologies // Problems of Economics and Legal Practice. 2024. Vol. 20. No. 2. P. 70-75.

[14] Škorjanc Ž. A Holistic Approach under the GDPR, AI Act, and Directive 2023/2225 to the Right to Explanation of Credit Scores // Global Privacy Law Review. 2025. Vol. 6. No. 3. P. 222-240.

[15] Zhirnova N. A., Soldatkina O. L. On the Legal Regime of Anonymized Personal Data // Bulletin of Voronezh State University. Series: Law. 2024. No. 4 (59). P. 44-51.

[16] Turanin V. Yu. Anonymization of Personal Data as a Legal Experiment: Risks and Opportunities // Legal Technique. 2025. No. 19. P. 641-646. [17] Poluyanova E. V. Current Issues in the Legal Regulation of Personal Data Anonymization // Bulletin of Science. 2025. Vol. 4. No. 2. P. 421–426.

[18] Solove D. J. The Digital Person: Technology and Privacy in the Information Age. New York: New York University Press, 2004.

[19] Cate F. H., Mayer-Schönberger V. Notice and Consent in a World of Big Data // International Data Privacy Law. 2013. Vol. 3. No. 2. P. 67–73.

[20] Rubinstein I. S. Big Data: The End of Privacy or a New Beginning? // International Data Privacy Law. 2013. Vol. 3. No. 2. P. 74–87.