Локализация данных в Китае, Индии и России: модели реализации концепции цифрового суверенитета

Крестинина Екатерина Владимировна
магистрант, международно-правовой факультет, Московский государственный институт международных отношений (университет) Министерства иностранных дел Российской Федерации, ekkrestinina@gmail.com

В статье выполнен сравнительно-правовой анализ трёх моделей реализации требования о локализации данных, основного юридического инструмента, посредством которого концепция цифрового суверенитета получает нормативное воплощение, в практике Китая, Индии и России в 2024–2026 гг. Автор исходит из того, что при общей идеологической направленности на укрепление цифрового суверенитета названные правопорядки воплощают принципиально различные регулятивные философии: государствоцентричную китайскую модель, субъектоцентричную индийскую модель и гибридную российскую модель, построенную на концепции первичной обработки. Показано, что российское регулирование занимает промежуточное положение на шкале интенсивности локализационных требований и наиболее тесно связано с проблематикой трансграничного коммерческого оборота в условиях односторонних ограничительных мер. На основе сравнительно-правовой доктрины и литературы по международному частному праву обосновывается вывод о том, что сверхимперативный характер (lois de police) норм о локализации порождает нарастающие коллизии с принципами свободы договора и автономии воли сторон в трансграничной торговле, а совмещение локализационных режимов с режимом односторонних ограничительных мер эти коллизии усиливает. Сформулированы предложения de lege ferenda, касающиеся выработки специальных коллизионных подходов и модельных договорных условий о трансграничной обработке данных.
Ключевые слова: локализация данных, цифровой суверенитет, трансграничная передача данных, персональные данные, PIPL, DPDP Act, Федеральный закон № 152-ФЗ, экстерриториальное действие, сверхимперативные нормы, автономия воли сторон.

Введение

За последнее десятилетие концепция цифрового суверенитета прошла путь от политико-доктринального тезиса до самостоятельного правового принципа. Базовым инструментом её нормативного воплощения выступает требование о локализации данных — императивное предписание, обязывающее операторов хранить и (или) обрабатывать персональные данные в пределах национальной территории и осуществлять трансграничную передачу лишь при соблюдении специальных условий и под контролем уполномоченного регулятора.

Настоящая статья посвящена сравнительно-правовому анализу трёх моделей реализации указанного требования — китайской, индийской и российской. Каждая из них демонстрирует принципиально различный регулятивный подход на общем идеологическом фоне укрепления цифрового суверенитета. Актуальность исследования определяется тем, что в 2024–2026 гг. все три правопорядка пережили существенное обновление нормативной базы: в Китае вступило в силу Положение об управлении безопасностью сетевых данных, в Индии были приняты подзаконные акты к Закону о защите цифровых персональных данных, в России изменилась редакция части 5 статьи 18 Федерального закона № 152-ФЗ и появилась уголовная ответственность за нарушения, связанные с трансграничной передачей.

Российская модель, занимающая промежуточное положение на шкале интенсивности локализационных требований и наиболее непосредственно связанная с проблематикой трансграничного коммерческого оборота в условиях односторонних ограничительных мер, рассматривается в работе как концептуально наиболее значимая для целей международного частного и коммерческого права.

Материалы и методы

Эмпирическую базу исследования составили нормативные правовые акты трёх юрисдикций в редакциях, действующих по состоянию на 2026 г., а также акты уполномоченных регуляторов — Государственной канцелярии по вопросам киберпространства КНР, Министерства электроники и информационных технологий Индии, Резервного банка Индии и Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций. Анализ по каждой юрисдикции построен по единой схеме: источники регулирования, нормативное содержание режима, актуальная регулятивная динамика и ключевые проблемы правоприменения. Такая унификация структуры обеспечивает функциональную сопоставимость выводов.

Методологическую основу работы образуют сравнительно-правовой метод (в его функциональном варианте, позволяющем сопоставлять разнородные по юридической технике режимы по решаемой ими регулятивной задаче), формально-юридический метод толкования нормативных предписаний и метод правового моделирования, применяемый при формулировании предложений de lege ferenda.

В юридической науке требование о локализации анализировалось как в критическом, так и в сравнительно-правовом ключе. А. Чандер и У. П. Ле охарактеризовали глобальное распространение локализационных предписаний как форму «информационного национализма», фрагментирующего интернет и возлагающего значительные издержки на трансграничный оборот, тогда как К. Кунер поместил такие меры в более широкий контекст права трансграничных потоков данных. Г. Гринлиф в наиболее полном сравнительном исследовании азиатского законодательства о приватности выстроил соответствующие режимы по оси «торговля — права человека», что позволяет уловить напряжение между охранительной и суверенной функциями локализации. Опираясь на эту литературу, настоящая работа рассматривает локализацию не только как приём защиты данных, но и как инструмент цифрового суверенитета, сверхимперативная природа которого порождает самостоятельные проблемы международного частного права — проблемы, которые сравнительные исследования, сосредоточенные преимущественно на конструкции регулирования, до сих пор затрагивали лишь попутно.

Результаты и обсуждение

1. Китайская модель: строгий централизованный режим

1.1. Источники регулирования и категоризация данных

Правовой каркас локализации в КНР образуют три закона: Закон о кибербезопасности (Cybersecurity Law, CSL) 2017 г., Закон о безопасности данных (Data Security Law, DSL) и Закон о защите персональной информации (Personal Information Protection Law, PIPL), оба 2021 г. Они дополняются актами Государственной канцелярии по вопросам киберпространства (Cyberspace Administration of China, CAC) и Положением об управлении безопасностью сетевых данных, вступившим в силу 1 января 2025 г.

Архитектура регулирования опирается на иерархическую категоризацию данных. Закон о безопасности данных и национальный стандарт GB/T 43697-2024 различают «обычные», «важные» и «ключевые» данные. С 1 января 2025 г. количественный порог отнесения массива персональных данных к «важным» повышен с одного до десяти миллионов субъектов данных. Особый статус имеют операторы критической информационной инфраструктуры (CIIO): согласно статье 37 CSL они обязаны хранить персональные и важные данные, сформированные на территории КНР, на серверах внутри страны, а трансграничная передача допускается только после положительного заключения по итогам государственной оценки безопасности.

1.2. Механизмы трансграничной передачи и экстерриториальное действие

Трансграничная передача регулируется тремя механизмами: государственной оценкой безопасности, проводимой CAC, китайскими стандартными договорными условиями и сертификацией. Государственная оценка безопасности обязательна при передаче важных данных, при передаче персональных данных более чем одного миллиона субъектов либо чувствительных персональных данных более чем десяти тысяч субъектов за календарный год; в остальных случаях доступны стандартные договорные условия или сертификация. Экстерриториальный охват режима значителен: пункт 2 статьи 3 PIPL распространяет действие закона на обработку данных лиц, находящихся в КНР, осуществляемую за пределами страны, если её целью является предложение таким лицам товаров или услуг либо анализ их поведения; такие операторы обязаны назначить представителя в Китае. Статья 36 DSL — «блокирующая» норма — запрещает передачу данных, хранящихся в КНР, иностранным судебным или правоохранительным органам без разрешения китайских властей.

Регулятивная динамика 2024–2025 гг. отражает курс на тонкую настройку режима. Положения о содействии трансграничным потокам данных и их регулировании от 22 марта 2024 г. ввели изъятия: из-под действия обязательного режима выведены передачи в целях исполнения договора, управления персоналом и в чрезвычайных ситуациях. Зоны свободной торговли Пекина, Шанхая, Тяньцзиня, Хайнаня и Чжэцзяна получили право принимать «негативные перечни», за пределами которых данные могут передаваться свободно.

1.3. Промежуточный вывод

Китайская модель является государствоцентричной: данные рассматриваются как стратегический ресурс, находящийся под непосредственным государственным контролем, а защита данных подчинена соображениям национальной и экономической безопасности и инструментализирована ими; в сравнительной литературе этот режим выступает парадигмальным случаем. Основные его проблемы сосредоточены в трёх плоскостях: нормативная неопределённость категории «важных данных» при отсутствии единого федерального каталога; широкая дискреция CAC при проведении оценок безопасности, основанных на политической оценке риска; коллизия между блокирующей нормой статьи 36 DSL и обязанностями по раскрытию информации в иностранных юрисдикциях, создающая для транснациональных корпораций ситуации правовой ловушки.

2. Индийская модель: гибкий режим после принятия DPDP Act 2023

2.1. Эволюция и структура режима

Индийский подход претерпел наиболее длительную эволюцию. Проект Закона о защите персональных данных 2019 г. содержал жёсткие требования о локализации, включая обязанность хранить копию всех персональных данных в Индии и запрет трансграничной передачи «критических» персональных данных; этот проект был отозван в 2022 г. Закон о защите цифровых персональных данных (Digital Personal Data Protection Act, DPDP Act), принятый в августе 2023 г., закрепил противоположный подход. Его окончательная операционализация состоялась 13 ноября 2025 г., когда Министерство электроники и информационных технологий приняло Правила о защите цифровых персональных данных, предусматривающие поэтапное введение в действие в течение двенадцати — восемнадцати месяцев. В сравнительной литературе этот разворот трактуется как отказ Индии от жёсткой локализации в пользу позиции, благоприятствующей торговле, — хотя, как показано ниже, отраслевые предписания сохраняют значительные анклавы строгой локализации.

Закон построен на концепции доверительного управляющего данными (data fiduciary). Особую категорию значимых доверительных управляющих (Significant Data Fiduciaries) по статье 10 образуют лица, на которых правительство возлагает повышенные требования с учётом объёма обрабатываемых данных и сопутствующих рисков; такие лица обязаны назначить находящегося в Индии специалиста по защите данных, проводить оценку воздействия и обеспечивать независимый аудит.

2.2. Трансграничная передача: механизм негативного перечня

Центральной нормой режима трансграничной передачи является статья 16 DPDP Act во взаимосвязи с правилом 15 Правил. Индийский законодатель избрал механизм «негативного перечня» вместо ранее обсуждавшегося «позитивного перечня». Передача за пределы Индии разрешена по умолчанию, за исключением государств, специально включённых центральным правительством в перечень ограничений. По состоянию на настоящее время такой перечень не сформирован, что фактически означает свободу трансграничной передачи при соблюдении общих требований правомерности обработки и наличия согласия субъекта данных. Пункт 2 статьи 16 сохраняет действие более высокого уровня защиты или более строгих ограничений передачи, установленных иными индийскими законами, вследствие чего общий режим не вытесняет отраслевую локализацию.

2.3. Сохраняющаяся отраслевая локализация

Вместе с тем отраслевая локализация выражена отчётливо. Директива Резервного банка Индии 2018 г. требует хранить все платёжные данные исключительно внутри страны; в сфере телекоммуникаций действует требование о хранении биллинговой информации в Индии; отдельные ограничения применяются в сфере государственных закупок и здравоохранения. Таким образом, в целом либеральный режим DPDP Act сосуществует с жёсткими отраслевыми императивами.

2.4. Промежуточный вывод

Индийская модель тяготеет к субъектоцентричной парадигме: общий режим построен вокруг согласия и подотчётности доверительного управляющего, а локализация применяется избирательно. Её основные проблемы — широкие изъятия для государственных органов по статье 17 DPDP Act, обосновываемые интересами суверенитета и безопасности и критикуемые как размывающие общий режим; отнесение «негативного перечня» к компетенции центрального правительства без детальных процедурных гарантий, что превращает его в потенциальный инструмент политически мотивированных ограничений; фрагментация между общим и отраслевыми режимами, поскольку соблюдение DPDP Act не освобождает оператора от требований Резервного банка и иных отраслевых регуляторов.

3. Российская модель: требование первичной обработки на территории Российской Федерации

3.1. Доктринальный и нормативный контекст

Российский режим сформирован на основе Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» в редакции Федерального закона от 21 июля 2014 г. № 242-ФЗ. Его центральной нормой является часть 5 статьи 18: операторы обязаны обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение) и извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории России. Российское регулирование действует не через количественные пороги или категории важности, а через саму природу действий, охватываемых понятием первичной обработки.

3.2. Концепция первичной обработки

Концепция первичной обработки означает, что закон не запрещает трансграничную передачу как таковую, но требует, чтобы первичный сбор и запись данных граждан России осуществлялись в национальных базах данных. Как отмечает А. И. Савельев в ведущем комментарии к закону, обязанность локализации привязана к перечисленным операциям первичного сбора и записи, а не к факту передачи, вследствие чего передача остаётся самостоятельной операцией, подчинённой отдельным правилам; иностранные сервисы, следовательно, могут использоваться лишь в качестве вторичного держателя, но не как точка первичной записи. Именно эта конструкция послужила основанием для блокировки сервиса LinkedIn в 2016 г. и для последующих ограничений работы ряда иностранных платформ. Она же порождает устойчивый вопрос толкования, обострившийся после рассматриваемой ниже поправки июля 2025 г.: не означает ли прямой запрет первичного сбора за рубежом фактического запрета на использование иностранной инфраструктуры на любой стадии обработки.

3.3. Последовательное ужесточение и криминализация

Регулирование последовательно ужесточалось. С марта 2023 г., после внесения изменений в статью 12 Закона № 152-ФЗ, операторы обязаны уведомить Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) и получить её разрешение до начала трансграничной передачи, за исключением передачи в государства, обеспечивающие, по оценке регулятора, адекватный уровень защиты; уведомление рассматривается в течение десяти рабочих дней. С 1 июля 2025 г. вступила в силу изменённая редакция части 5 статьи 18, прямо запрещающая первичный сбор персональных данных граждан России за пределами Российской Федерации, что исключает использование иностранной облачной инфраструктуры в качестве точки первичной записи.

Существенно изменилась система ответственности. Федеральный закон от 30 ноября 2024 г. № 421-ФЗ дополнил Уголовный кодекс статьёй 272.1, действующей с 11 декабря 2024 г. и устанавливающей уголовную ответственность за неправомерное использование, передачу, сбор и хранение компьютерной информации, содержащей персональные данные. Особое значение имеет часть 4 статьи 272.1, предусматривающая повышенную ответственность — до десяти лет лишения свободы — за деяния, связанные с трансграничной передачей таких данных. С 30 мая 2025 г. вступила в силу новая редакция статьи 13.11 Кодекса Российской Федерации об административных правонарушениях, существенно увеличившая административные штрафы и введшая оборотные штрафы за повторные нарушения. Переход к уголовной и оборотной ответственности отражает доктринальное переосмысление локализации как вопроса информационной безопасности и защиты критической информационной инфраструктуры, а не только неприкосновенности частной жизни.

3.4. Пересечение с режимом односторонних ограничительных мер

Особое значение для международного частного и коммерческого права российская модель приобретает в точке наложения локализационного режима на режим односторонних ограничительных мер. Российские компании, действующие на европейском рынке, оказываются одновременно подчинены двум режимам — Закону № 152-ФЗ и Общему регламенту ЕС по защите данных, — логика которых различна, а по отдельным вопросам прямо противоположна. Введение санкций и контрсанкций после 2022 г. резко сократило число юрисдикций, между которыми возможно свободное обращение данных, и одновременно усилило императивный характер национальных локализационных требований. Тем самым требования локализации перестают быть исключительно инструментом защиты прав субъектов данных и становятся элементом более широкой архитектуры экономического суверенитета.

3.5. Открытые вопросы и риски

Проблемы российской модели обусловлены рядом обстоятельств. Концепция первичной обработки технически плохо совместима с архитектурой современных облачных сервисов, использующих географически распределённые центры обработки данных. Криминализация нарушений, связанных с трансграничной передачей, существенно повышает риски для участников международного торгового оборота. Наконец, сокращение после 2022 г. числа стран, признаваемых обеспечивающими адекватный уровень защиты, непосредственно влияет на условия международного коммерческого оборота, поскольку сужает каналы, по которым данные могут правомерно перемещаться при исполнении трансграничных договоров.

Обсуждение: сравнительный анализ и проблема международного частного права

Сопоставление трёх юрисдикций позволяет выстроить условную шкалу интенсивности локализационных требований: Китай — Россия — Индия. Китайская модель государствоцентрична: данные рассматриваются как стратегический ресурс под непосредственным государственным контролем. Российская модель сочетает элементы суверенноцентричного и субъектоцентричного подходов: первичная обработка провозглашается гарантией прав граждан Российской Федерации и одновременно служит инструментом государственного контроля за информационными потоками. Индийская модель тяготеет к субъектоцентричной парадигме с избирательным применением локализации. Вместе с тем все три режима обладают общими структурными признаками: каждый предусматривает экстерриториальное действие (статья 3 PIPL, DPDP Act, Закон № 152-ФЗ), доминирующего регулятора с широкой дискрецией и ограниченный судебный контроль за его решениями.

Ключевая проблема, возникающая на пересечении названных режимов с международным коммерческим оборотом, состоит в их потенциальном конфликте с принципами свободы договора и автономии воли сторон. Стандартные условия международных коммерческих контрактов — о применимом праве, компетентном форуме, языке и месте исполнения — не учитывают локализационных императивов. В терминологии международного частного права такие императивы действуют как сверхимперативные нормы (lois de police): согласно статье 1192 Гражданского кодекса Российской Федерации, это нормы, которые вследствие указания в них самих или ввиду их особого значения для обеспечения прав и охраняемых законом интересов участников гражданского оборота регулируют соответствующие отношения независимо от подлежащего применению права. Поскольку нормы о локализации применяются независимо от избранного сторонами правопорядка, контрагент, действующий на нескольких рынках, вынужден выстраивать множественные и потенциально конфликтующие режимы обработки; использование стандартных договорных условий, разработанных для одного правопорядка, не освобождает его от предписаний, выработанных в другом. Это наложение становится особенно острым, когда локализационные режимы накладываются на режим односторонних ограничительных мер, который сам по себе нередко характеризуется как совокупность сверхимперативных норм.

Заключение

Развитие регулирования в 2024–2026 гг. позволяет сформулировать четыре вывода.

Во-первых, локализация данных является одним из наиболее зрелых инструментов реализации концепции цифрового суверенитета, однако формы её воплощения существенно различаются — от жёсткого централизованного китайского контроля через промежуточную российскую модель, основанную на концепции первичной обработки, к избирательному индийскому отраслевому регулированию. Общим знаменателем всех трёх режимов выступает признание данных самостоятельным объектом правового регулирования, обладающим территориальной привязкой.

Во-вторых, сверхимперативный характер норм о локализации порождает коллизии со свободой договора и автономией воли сторон, которые международное частное право до сих пор не восприняло в полной мере. Это требует выработки специальных коллизионных подходов, рассматривающих требования локализации в качестве сверхимперативных норм и учитывающих их кумулятивное применение в нескольких юрисдикциях, с тем чтобы снизить риск правовой ловушки для транснациональных операторов.

В-третьих, стандартные договорные конструкции нуждаются в адаптации. De lege ferenda следует разработать модельные условия о трансграничной обработке данных, которые прямо распределяли бы риск локализации, предусматривали операционное перенаправление потоков при включении юрисдикции в перечень ограничений и интегрировали механизмы «доверенного держателя данных» и локального обработчика в качестве архитектуры по умолчанию, а не ситуативного обходного решения.

В-четвёртых, российский режим нуждается в уточнении, позволяющем согласовать концепцию первичной обработки с реальностью распределённой облачной инфраструктуры, а национальные требования — с расширяющимся режимом односторонних ограничительных мер. Пересечение локализации и санкций превращает локализацию из инструмента защиты данных в элемент экономического суверенитета; именно этот аспект, по мнению автора, заслуживает дальнейшего углублённого изучения.

Литература

1. Закон Китайской Народной Республики о кибербезопасности (2017); Закон Китайской Народной Республики о безопасности данных (2021); Закон Китайской Народной Республики о защите персональной информации (2021).
2. Положение об управлении безопасностью сетевых данных (Государственный совет КНР, сентябрь 2024 г.; вступило в силу 1 января 2025 г.); Национальный стандарт GB/T 43697-2024.
3. Положения о содействии трансграничным потокам данных и их регулировании (Государственная канцелярия по вопросам киберпространства КНР, 22 марта 2024 г.).
4. Закон о защите цифровых персональных данных № 22 от 2023 г. (Индия); Правила о защите цифровых персональных данных 2025 г. (Министерство электроники и информационных технологий Индии, приняты 13 ноября 2025 г.).
5. Директива Резервного банка Индии о хранении данных платёжных систем от 6 апреля 2018 г.
6. Гражданский кодекс Российской Федерации. Часть третья (статья 1192 — нормы непосредственного применения).
7. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (статья 12; часть 5 статьи 18) в редакции Федерального закона от 21 июля 2014 г. № 242-ФЗ.
8. Федеральный закон от 30 ноября 2024 г. № 421-ФЗ (о дополнении Уголовного кодекса Российской Федерации статьёй 272.1).
9. Федеральный закон от 30 ноября 2024 г. № 420-ФЗ (о внесении изменений в статью 13.11 Кодекса Российской Федерации об административных правонарушениях).
10. Регламент (ЕС) 2016/679 Европейского парламента и Совета от 27 апреля 2016 г. (Общий регламент по защите данных).
11. Chander A., Lê U. P. Data Nationalism // Emory Law Journal. 2015. Vol. 64. No. 3. Pp. 677–739.
12. Greenleaf G. Asian Data Privacy Laws: Trade and Human Rights Perspectives. Oxford: Oxford University Press, 2014. 618 p.
13. Hon W. K. Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction Through a Cloud Computing Lens. Cheltenham: Edward Elgar Publishing, 2017. 448 p.
14. Kuner C. Transborder Data Flows and Data Privacy Law. Oxford: Oxford University Press, 2013. 288 p.
15. Yakovleva S. Personal Data Transfers in International Trade and EU Law: A Tale of Two “Necessities” // The Journal of World Investment & Trade. 2020. Vol. 21. No. 6. Pp. 881–919.
16. Савельев А. И. Научно-практический постатейный комментарий к Федеральному закону «О персональных данных». 3-е изд., перераб. и доп. М.: Статут, 2025. 720 с.
17. Государство, общество и личность: пути преодоления вызовов и угроз в информационной сфере: монография / под ред. Л. К. Терещенко. М.: Инфотропик Медиа, 2024. 296 с.

Data localization in China, India and Russia: models for implementing the concept of digital sovereignty

Krestinina E.V.

MGIMO University (Moscow State Institute of International Relations, Ministry of Foreign Affairs of the Russian Federation)

This paper offers a comparative analysis of three models for implementing the requirement of data localization — the principal legal instrument through which the concept of digital sovereignty is operationalized — in the practice of China, India and Russia in 2024–2026. It argues that, despite a shared ideological orientation toward strengthening digital sovereignty, the three jurisdictions embody fundamentally different regulatory philosophies: a state-centric Chinese model, a subject-centric Indian model, and a hybrid Russian model built on the concept of primary processing. The Russian regime occupies an intermediate position on the spectrum of localization intensity and is most directly connected to the problems of cross-border commerce under unilateral restrictive measures. Drawing on the comparative and private-international-law literature, the paper further argues that the overriding-mandatory (lois de police) character of localization norms generates growing conflicts with the principles of freedom of contract and party autonomy in cross-border commerce, and that these conflicts are amplified by the expanding regime of unilateral restrictive measures. The paper concludes with de lege ferenda proposals concerning the development of special conflict-of-laws approaches and model contractual clauses on cross-border data processing.

Keywords: data localization, digital sovereignty, cross-border data transfer, personal data, PIPL, DPDP Act, Federal Law No. 152-FZ, extraterritorial effect, overriding mandatory provisions, party autonomy.

References

1. Cybersecurity Law of the People’s Republic of China (2017); Data Security Law of the People’s Republic of China (2021); Personal Information Protection Law of the People’s Republic of China (2021).
2. Regulation on Network Data Security Management (State Council of the PRC, September 2024; effective 1 January 2025); National Standard GB/T 43697-2024.
3. Provisions on Promoting and Regulating Cross-Border Data Flows (Cyberspace Administration of China, 22 March 2024).
4. Digital Personal Data Protection Act, No. 22 of 2023 (India); Digital Personal Data Protection Rules, 2025 (MeitY, notified 13 November 2025).
5. Reserve Bank of India, Directive on Storage of Payment System Data of 6 April 2018.
6. Civil Code of the Russian Federation, Part Three (Article 1192, overriding mandatory provisions) (in Russian).
7. Federal Law of the Russian Federation No. 152-FZ of 27 July 2006 “On Personal Data” (Article 12; part 5 of Article 18), as amended by Federal Law No. 242-FZ of 21 July 2014 (in Russian).
8. Federal Law No. 421-FZ of 30 November 2024 (introducing Article 272.1 into the Criminal Code of the Russian Federation) (in Russian).
9. Federal Law No. 420-FZ of 30 November 2024 (amending Article 13.11 of the Code of Administrative Offences of the Russian Federation) (in Russian).
10. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation).
11. Chander A., Lê U. P. Data Nationalism // Emory Law Journal. 2015. Vol. 64. No. 3. Pp. 677–739.
12. Greenleaf G. Asian Data Privacy Laws: Trade and Human Rights Perspectives. Oxford: Oxford University Press, 2014. 618 p.
13. Hon W. K. Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction Through a Cloud Computing Lens. Cheltenham: Edward Elgar Publishing, 2017. 448 p.
14. Kuner C. Transborder Data Flows and Data Privacy Law. Oxford: Oxford University Press, 2013. 288 p.
15. Yakovleva S. Personal Data Transfers in International Trade and EU Law: A Tale of Two “Necessities” // The Journal of World Investment & Trade. 2020. Vol. 21. No. 6. Pp. 881–919.
16. Savelyev A. I. Scientific and Practical Article-by-Article Commentary to the Federal Law “On Personal Data”. 3rd ed., rev. and enl. Moscow: Statut, 2025. 720 p. (in Russian).
17. Government, Society and the Individual: Ways of Overcoming Challenges and Threats in the Information Sphere: monograph / ed. by L. K. Tereshchenko. Moscow: Infotropic Media, 2024. 296 p. (in Russian).