Дата поступления рукописи в редакцию: 18.05.2026 г.
Дата принятия рукописи в печать: 02.06.2026 г.
DOI: 10.24412/2782-3830-2026-5-166-173

МИНАЕВА Валентина Владимировна,
студентка 4 курса Международно-правового факультета
Федерального государственного автономного
образовательного учреждения высшего образования
«Московский государственный институт
международных отношений (университет)
Министерства иностранных дел Российской Федерации»,
e-mail: Minaevavalya19@yandex.ru

Научный руководитель:
КРИВЕЛЬСКАЯ Ольга Валентиновна,
кандидат юридических наук,
заместитель заведующего кафедрой
административного и финансового права по научной работе
Федерального государственного автономного
образовательного учреждения высшего образования
«Московский государственный институт
международных отношений (университет)
Министерства иностранных дел Российской Федерации»,
ORCID ID: 0009-0004-9822-3110,
e-mail: o.krivelskaya@inno.mgimo.ru

ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ АДМИНИСТРАТИВНО-ПРАВОВОГО РЕГУЛИРОВАНИЯ ТРАНСГРАНИЧНОЙ ПЕРЕДАЧИ ДАННЫХ В БАНКОВСКОЙ СФЕРЕ НА ОСНОВЕ DPDP ACT 2023

Аннотация. *В настоящей статье рассматривается действующее регулирование трансграничной передачи данных в Индии с учётом особенностей банковской сферы. Анализируются основные административно-правовые источники права, такие как общий и основополагающий закон The Digital Personal Data Protection Act, подзаконный акт, детализирующий регулирование The Digital Personal Data Protection Rules, а также акты Резервного банка Индии, имеющие особое значение в части регламентирования передачи данных в банковской сфере в том числе в силу прямого указания на это в законе. Именно указанные источники составляют основу правового регулирования процедуры трансграничной передачи данных, устанавливают особенности статуса банков в качестве субъектов, ответственный за обработку особо значимых данных. Отмечается ряд проблем сложившейся системы регулирования, а именно, с одной стороны, гибкость и адаптивность к изменяющимся условиям политики и международной безопасности, но, с другой стороны, отсутствие стабильности, чрезмерные полномочия Правительства в части принятия подзаконных актов по ряду ключевых вопросов регулирования, а также недостаточная конкретность норм, несмотря на принятие детализирующих правил. Также выделяются характерные особенности существующего режима защиты данных в Индии, а именно применение подхода “негативного списка”, акцент на цифровых данных и введение специального субъекта, связанного с особо значимыми данными. Это позволяет сделать вывод о наличии основы для формирования уникального механизма регулирования трансграничной передачи данных, который с учётом особенностей банковской сферы обеспечивает высокий стандарт защиты и предоставляет широкую дискрецию банкам при организации передачи данных в зарубежные юрисдикции.*

Ключевые слова: *трансграничная передача данных, банки, режим защиты данных, персональные данные, DPDP Act, DPDP Rules, Резервный банк Индии, Республика Индия.*

MINAEVA Valentina Vladimirovna,
4nd year student of the International Law Faculty,
Federal State Autonomous Educational

Institution of Higher Education
«Moscow State Institute of International Relations
(University) of the Ministry of Foreign Affairs of
the Russian Federation»

Academic Supervisor:
KRIVELSKAYA Olga Valentinovna,
PhD in Law, Deputy Head of the Department of Administrative and
Financial Law for Research at MGIMO MFA of Russia

PROBLEMS AND PROSPECTS OF ADMINISTRATIVE AND LEGAL REGULATION OF CROSS-BORDER DATA TRANSFER IN THE BANKING SECTOR BASED ON DPDP ACT 2023

Annotation. *This article examines the current regulation of cross-border data transfer in India, taking into account the specifics of the banking sector. It analyzes the main administrative and legal sources, such as the general and fundamental source, The Digital Personal Data Protection Act; the secondary legislation detailing the regulation, The Digital Personal Data Protection Rules; and the regulations of the Reserve Bank of India, which are of particular importance in regulating data transfer in the banking sector due to the direct reference to this regulations in the DPDP Act. These sources form the basis for legal regulation of cross-border data transfer procedures and establish the specific status of banks as entities responsible for processing particularly sensitive data. A number of problems with the existing regulatory system are noted, namely, on the one hand, flexibility and adaptability to changing political conditions and international security; on the other hand, a lack of stability, excessive government powers in terms of adopting secondary legislation on a number of crucial regulatory issues, and insufficient specificity of the regulations, despite the adoption of detailed rules. The article also highlights key features of India's existing data protection regime, including the use of a "negative list" approach, a focus on digital data, and the introduction of a designated entity for sensitive data. This suggests the existence of a foundation for developing a unique regulatory mechanism for cross-border data transfers that, while taking into account the specifics of the banking sector, ensures a high standard of protection and grants banks broad discretion when arranging data transfers to foreign jurisdictions.*

Key words: *cross-border data transfer, banks, data protection regime, personal data, DPDP Act, DPDP Rules, Reserve Bank of India, Republic of India.*

Принятие The Digital Personal Data Protection Act (далее — DPDP Act) является значимым шагом в развитии законодательства Индии в сфере защиты персональных данных, поскольку ранее единое регулирование отсутствовало, было лишь отраслевое регламентирование режима конфиденциальности. При этом значимым фрагментом существовавшего ранее режима защиты данных являлась банковская сфера, где акты Резервного банка Индии восполняли пробелы регулирования. С 2023 года идёт процесс формирования единой системы законодательства и подзаконных актов Индии, в которой DPDP Act занимает значимое, но не исключительно ключевое значение.

Введение

Необходимость создания единого законодательного акта в сфере защиты цифровых персональных данных и конфиденциальности информации в Индии существовала длительное время. Особенно ярко данный пробел в законодательстве был подчеркнут в решении Верховного суда Индии 2017 года по делу судьи К.С. Путтасвами против Союза Индии (Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (India)), которое также называется "Решение о праве на неприкосновенность частной жизни", что стало импульсом к активизации законотворческой деятельности по данному вопросу. Актуальность темы защиты данных именно в банковской сфере в Индии обусловлена тем, что за последние несколько лет количество пользователей банковских услуг в цифровой форме стремительно растёт: на 2025 год оно составляет 350 миллионов клиентов сети из 550 взаимосвязанных банков, использующих 77 мобильных приложений [6, с. 87]. Одновременно с этим возросло количество случаев утечки данных пользователей банковских карт и систем идентификации граждан, что представляет собой угрозу национальной безопасности страны. В связи с этим необходимо было принять новое регулирование, обеспечивающее более высокий уровень защиты данных.

После длительной деятельности нескольких рабочих групп индийского Парламента, проведения общественных слушаний был подготовлен и принят DPDP Act, ставший основой для нового уникального режима защиты данных в Индии.

Анализ положительных и отрицательных сторон действующего регулирования передачи персональных данных в банковской сфере в Индии имеет важное значение по ряду причин. Во-первых, Индия является одной из перспективных юрисдикций для расширения экономических связей, в том числе в банковской сфере при осуществлении международных расчётов, что неизбежно связано с трансграничной передачей данных в условиях глобальной цифровизации экономики. Понимание особенностей регулирования и возможных рисков важно для более успешного взаимодействия при трансграничной экономической деятельности. Во-вторых, изучение опыта государства позволит использовать достижения и избежать сложностей при улучшении отечественного законодательства. DPDP Act является примером попытки индийских законодателей создать сбалансированную систему защиты данных и поддержку национальной безопасности и глобальной цифровой экономической деятельности.

Научных статей, посвящённых анализу данной сферы правового регулирования в праве Индии на русском языке найдено не было. Работы по данной темативе преимущественно написаны индийскими исследователями, в том числе Ганга В. (Ganga V.), Кашяп П. К. (Kashyap P. K.), Каткури С. (Katkuri S.), Кермина М. П. (Kermina M. P.), Сингх Р. К. (Singh R. K.), Тандон У. (Tandon U.), Гупта Н.К. (Gupta N.K.).

DPDP Act в системе актов, регулирующих трансграничную передачу данных

На настоящий момент административно-правовое регулирование трансграничной передачи данных в банковской сфере в Индии осуществляется на основе ряда актов. С 2023 года действует единый закон, регулирующий защиту персональных данных в цифровой среде DPDP Act. Более детализированная процедура реализации требований DPDP Act закреплена в подзаконном акте The Digital Personal Data Protection Rules (далее – DPDP Rules), принятые Министерством электроники и информационных технологий Индии в 2025 году и вводимым в действие в трехэтапном порядке до 2027 года. Такая модель внедрения регулирования создаёт условия, в которых организации имеют возможность осуществить необходимую подготовку к переходу на полное соблюдение требований DPDP Act. Именно в рамках третьего этапа, то есть в 2027 году вступят в силу положения, регулирующие требования при передаче персональных данных к SDF (Rule 13) и порядок трансграничной передачи данных (Rule 15). Важное значение имеют акты Резервного банка Индии, имеющие приоритетное значение для банков в силу прямого закрепления этого правила в DPDP Act (пункт 2 Раздела 16).

Принятый в 2023 году DPDP Act является основным и общим законом, регулирующим защиту персональных данных. Как отмечается в Разделе 38 данного закона, он направлен на дополнение, а не отмену иных действующих законов, однако в случае коллизии применению подлежат положения именно DPDP Act. Его особенностями является включение в сферу регулирования именно данных в цифровой среде, без учёта информации оффлайн (Раздел 3), а также отсутствие разделения данных на специальные категории в зависимости от степени обеспечиваемой защиты, тогда как специальный субъект, ответственный за обработку особо значимых данных специально выделяется (Раздел 10) [5, с. 2].

Соответственно, система административно-правового регулирования трансграничной передачи данных в Индии состоит как из законов, так и из подзаконных актов, причём Правительство управомочено принимать дополнительные указания и иные акты, закрепляющие ограничения в данной сфере (пункт 1 Раздела 16). С одной стороны, это обеспечивает гибкость регламентирующих актов в быстро меняющихся условиях цифровой экономики. С другой стороны, регулирование не является стабильным, что увеличивает риски экономической деятельности в данной сфере [3, с. 22].

Также несмотря на публикацию DPDP Rules, направленных на детализацию положений DPDP Act, режим защиты данных в Индии продолжает быть основанным на чрезмерно широких и гибких формулировках, в связи с чем субъекты, передающие данные, сталкиваются с неопределённостью стандартов, которые они должны соблюдать. В результате может сформироваться непоследовательная правоприменительная практика, основанная на субъективной оценке соблюдения законодательства [2, с. 7]. При этом ответственность за нарушения в сфере персональных данных предусмотрена в виде штрафа в размере до 250 млн рупий.

Правовое регулирование трансграничной передачи данных в Индии

Основными принципами действующего регулирования является согласие и прозрачность, ограничение целей, минимизация данных, точность, ограничение срока хранения, гарантии

безопасности и подотчетность. Использование цифровых персональных данных должно осуществляться исключительно в законных, справедливых и прозрачных целях, при ограничении несанкционированного использования и передачи законного права собственности на данные доверителям [4, с. 113].

Вопросу трансграничной передачи данных посвящён Раздел 16 DPDP Act. В пункте 1 данного раздела содержится указание на правомочие Правительства посредством соответствующего уведомления ограничить передачу персональных данных субъектам, ответственным за обработку данных (Data Fiduciary) в страну или на территорию за пределами Индии. Соответственно, индийское регулирование в сфере трансграничной передачи данных основано на так называемом подходе “негативного списка” («blacklist approach”). Это означает, что передача данных за пределы Индии допустима при отсутствии установления ограничений, в частности, в виде запрета на передачу данных в конкретные юрисдикции посредством принятия Правительством “черного списка” государств в рамках уведомления. Такой подход индийского регулирования отличается от более распространённых механизмов “адекватности”, при котором передающего данные субъекты обязаны самостоятельно оценивать уровень защиты данных в иной юрисдикции, и подхода “белого списка”, при котором устанавливается обязанность передачи данных исключительно в одобренные юрисдикции, содержащиеся в соответствующем перечне [1, с. 2109].

Реализация такого механизма предусматривает перераспределение обязанности оценки соответствия уровня защиты данных национальным критериям между Правительством и субъектом, передающим данные [5, с. 9]. Так дискреция исполнительных органов в данной сфере расширяется, при этом полностью необходимость проверки соблюдения обязанности по оценке рисков субъектом, передающим данные, не исключается, что подчёркивается в Разделе 10, посвящённому обязанностям субъектов, обрабатывающих данные. То есть соблюдение требований DPDP Act о трансграничной передаче данных будет обеспечиваться при учёте ограничений “черного списка” юрисдикций, а субъекты передачи данных обязаны при передаче данных в “разрешённые” юрисдикции продолжают осуществлять проверку соблюдения требований к процедуре передачи данных и условиям её хранения. Таким образом обеспечивается двойная проверка допустимости осуществления трансграничной передачи данных [4, с. 117].

С одной стороны, благодаря этому у индийских стартапов, цифровых платформ и ТНК на международном уровне есть значительная свобода действий при осуществлении трансграничных операций и создании облачных инфраструктур на основе данных. С другой стороны, отсутствует определённость относительно возможного введения ограничений со стороны Правительства в отношении каких-либо юрисдикций в зависимости от политических изменений или интересов национальной безопасности. В связи с этим ведение экономической деятельности в сфере цифровых данных с контрагентами из Индии связано с риском внезапного дополнения “черного списка” юрисдикций [3, с. 23].

Другим важным аспектом деятельности, связанной с применением трансграничной передачи данных является локализация данных. DPDP Act в рассматриваемом Разделе 16 не устанавливает обязанность хранения данных исключительно в Индии. Однако в пункте 2 Раздела 16 DPDP Act содержится следующая норма: «Ничто из изложенного в этом разделе не ограничивает применимость действующего в Индии закона, который предусматривает более высокий уровень защиты персональных данных или ограничения на их передачу ответственным лицом за пределы Индии в отношении любых персональных данных, ответственного лица или их совокупности». То есть DPDP Act не отменяет специальное регулирование, договорную конфиденциальность, обязанности по трудовому праву или профессиональную ответственность, а дополняет их специальной системой управления данными [3, с. 22], закрепляется приоритет более строгих секторальных норм над правилами DPDP Act.

В банковской сфере к таковым источникам норм относятся акты Резервного банка Индии, которые закрепляют специальные и более строгие требования к обработке и передаче данных именно в банковском секторе. Основным актом Резервного банка Индии в сфере обработки банками данных является Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices, вступивший в силу с 1 апреля 2024 года и заменивший ряд отдельных актов. Однако вопросы именно трансграничной передачи данных в данном акта не затрагиваются, только в Разделе 17, посвящённом процедуре обработке данных, предусматриваются требования к механизму передачи данных, которые применимы к аналогичной процедуре трансграничного характера.

Специальное регулирование передачи данных за рубеж содержится в ещё действующем Circular on Storage of Payment System Data 2018 года, который предусматривает жёсткие требо-

вания о локализации хранения данных в Индии при обязательном возврате копии данных в течение 24 часов в случае обработки данных за рубежом. Также ограничения в части передачи данных в виде обязательной локализации клиентских данных действуют в отношении KYC-данных, то есть персональных и идентификационных сведений, используемых в рамках процедуры "Знай своего клиента" в силу положений Know Your Customer (KYC) Master Direction 2016 года.

Ряд иных актов Резервного банка Индии косвенно затрагивает вопрос трансграничной передачи данных в банковской сфере. Например, Master Direction on Outsourcing of Information Technology Services и Master Direction on Managing Risks and Code of Conduct in Outsourcing of Financial Services 2023 года устанавливают требования к управлению рисками, контролю за обработкой данных и соответствии процедуры обработки в иностранных юрисдикциях требованиям законодательства Индии.

Таким образом, акты Резервного банка Индии закрепляют особые требования при трансграничной передаче данных банками в части обязательной локализации хранения в Индии, управлению рисками и контролю за обработкой данных. Это секторальное регулирование не вступает в противоречие с общими требованиями DPDP Act, является специальными актами в сфере трансграничной передачи данных в банковской сфере. Наличие подобных строгих требований обеспечивает повышенный уровень защиты данных, что необходимо в сфере особо значимых данных в банковской среде. Также серьёзный уровень защиты данных укрепляют позиции бизнеса на рынке и может стимулировать дополнительные инвестиции в локальную инфраструктуру передачи данных [1, с. 2117]. При этом выполнение указанных требований связано с увеличением операционных расходов на соответствующие системы обеспечения и центры обработки данных.

Обязанности банков как SDF в контексте DPDP Act

Отчасти регулирование передачи данных в банковской сфере осуществляется в Разделе 10 DPDP Act, в котором закрепляются особые обязанности в сфере персональных данных для Significant Data Fiduciaries — Субъектов, ответственных за обработку особо значимых данных (далее – SDF). Данный статус присваивается субъектам, обладающим персональными данными иных лиц, Правительством на основании оценки ряда факторов, связанных с характером обрабатываемых персональных данных, существующими рисками и их значением для защиты национальных интересов в силу пункта 1 Раздела 10. Соответственно, к таким субъектам отнесены крупные банки и иные финансовые организации, поскольку они имеют доступ к большим объёмам особо чувствительных данных клиентов, и в связи с этим обязаны обеспечивать достаточный уровень их защиты [5, с. 4].

На SDF возложена юридическая обязанность по соблюдению ряда требований к порядку получения, обработки и передачи персональных данных в пункте 2 Раздела 10 DPDP Act. В частности, SDF обязаны назначить специалиста, ответственного за соблюдение законодательства в сфере защите данных, независимого аудитора, осуществляющего периодическую оценку соблюдения требований законодательства относительно порядка обработки значимых данных. Отдельно в данном пункте прописывается, что такая оценка должна включать в себя описание прав субъектов данных и целей обработки их персональных данных, оценку рисков для прав субъектов данных и управление ими, а также другие вопросы, связанные с этим процессом, которые могут быть установлены в законодательных актах.

Обработка данных в банковской сфере, в том числе их передача, связана с повышенными рисками и, соответственно, повышенными обязанностями ответственных субъектов. В индийском законодательстве повышенные обязанности проявляются в императивном требовании о наличии в ответственной за обработку значимых персональных данных организации двух специальных сотрудников: специалиста по соблюдению правил в сфере персональных данных и аудитора в данной сфере. Вероятно, именно данные специалисты будут участвовать в процедуре оценки уровня защиты персональных данных в иностранной юрисдикции при осуществлении трансграничной передачи данных. Также открытый список требований, которые должны быть соблюдены и на соответствие которых будет проводить проверку аудитор свидетельствует о значимости специального секторального регулирования в банковской сфере в виде актов, издаваемых Резервным банком Индии.

Отдельное регулирование статуса SDF содержится в Правиле 13 DPDP Rules. В частности, закрепляются следующие обязанности данных субъектов: проведение оценки воздействия на защиту данных и соответствующего аудита для обеспечения эффективного соблюдения положений законодательства один раз в 12 месяцев и направление отчёта по итогам проверки и аудита в Совет по защите данных (создан в силу Главы 5 DPDP Act); осуществление осмотрительной проверки безопасности технических мер, используе-

мых при работе с персональными данными; соблюдение требований об ограничении в сфере трансграничной передачи персональных данных, принимаемых соответствующим комитетом Правительства.

Дополнения к регулированию в части регулирования трансграничной передачи данных в Правиле 15 DPDP Rules отсутствуют. Отличие заключается лишь в том, что акцент смещён с необходимости соответствия требования об уровне защиты данных в иностранной юрисдикции на обязанность субъекта, передающего данные, соблюдать требования общих и специальных распоряжений Правительства о предоставлении персональных данных любому иностранному субъекту. Из буквального толкования данного Правила можно сделать вывод о том, что ограничения в сфере трансграничной передачи данных могут быть введены не только в рамках "чёрного списка" юрисдикций, но и в иной форме, поскольку отмечаются "общие и специальные распоряжения Правительства". В связи с этим возможно ограничение не только по кругу юрисдикций, но и по категориям данных, которые допустимо передавать в зарубежные юрисдикции. Однако на настоящий момент какое-либо дополнительное регулирование, в том числе устанавливающее "черный список", ещё не принято. При этом необходимо отметить, что к самому договору о передаче данных дополнительные требования не предъявляются, что отличает индийское регулирование в данной сфере [2, с. 9]. С одной стороны, это снижает административную нагрузку на субъектов, передающих данные. При этом само регулирование является гибким, есть возможность при необходимости адаптировать его к изменениям в международной политике, тенденциям международного правового регулирования в данной сфере или отраслевым рискам. Но, с другой стороны, передающие данные субъекты обязаны особо внимательно следить за обновлениями законодательства, чтобы оценивать перспективные риски введения ограничений как на определённые юрисдикции, так и на конкретные виды данных.

В части определения понятия субъекта, передающего данные, вне зависимости от того, является ли он SDF или нет, ключевой проблемой индийского регулирования является отсутствие категории "совместных субъектов, обрабатывающих данные". Данный институт выделяется в иных регулированиях в целях возможности разделения как полномочий при принятии решений, так и ответственности за деятельность в сфере обработки данных, что особенно часто применяется в банковской сфере в рамках отдельных видов предоставления финансирования. В частности, кредитор и платёжный агрегатор совместно влияют на процедуру обработки данных. Вследствие отсутствия категории "совместных субъектов" возможна ситуация, когда ответственность будет либо исключаться в отношении обоих участвующих субъектов, либо дублироваться в пересекающихся областях ответственности. Это одинаково негативно влияет на правоприменительную практику, поскольку субъекты могут стремиться уклониться от ответственности при применении правовых лакун [1, с. 2112].

Дополнительные аспекты регулирования трансграничной передачи данных

Необходимо учитывать, что трансграничную передачу данных нельзя рассматривать изолированно, это один из видов взаимодействия с персональными данными, который должен содержать обязательные компоненты: соблюдение процедуры получения согласия на это в рамках заключения договора, а также обязательное осуществление оценки рисков. DPDP Act предусмотрел новые требования к согласию (Раздел 6), в связи с чем многие субъекты, в том числе, банки, были обязаны пересмотреть положения соглашения на обработку и использование персональных данных. В частности, оно должно стать более точным и ясным, необходимо было перевести его на несколько языков, используемых в Индии, а также добавить графы, в которых физические лица могли бы прямо указать своё согласие на совершение отдельных действий помимо подписи как общего согласия на условия документа, в частности, возможно отдельно выделить согласие на передачу данных в зарубежные юрисдикции. Наиболее удобно реализовать данные изменения возможно при применении так называемых платформ управления согласием, которые позволяют применять несколько языков и добавлять отдельные графы для согласия в зависимости от условий основного договора с банком. Также возможно создать специальные порталы для отзыва согласия и получения дополнительных согласий от клиентов по запросам на доступ к данным [3, с. 23].

В части регулирования процедуры передачи данных необходимо учитывать положения DPDP Rules, которые напрямую не регулируют трансграничную передачу данных, однако содержат требования, которые следует соблюдать при осуществлении данной процедуры. Во-первых, Правило 6 предусматривает ряд мер безопасности при работе с данными, в том числе осуществление шифрования, контроля доступа, маскировки, мониторинга и резервного копирования.

Во-вторых, Правило 7 закрепляет обязанность по уведомлению в случае нарушения законодательства, в том числе в случае неправомерных действий иностранных субъектов, взаимодействующих с данными из Индии. Тогда необходимо осуществлять двойное уведомление, то есть уведомление как собственника данных, так и Совет по защите данных. В-третьих, к данным, переданным за рубеж, применяются положения о хранении и удалении, установленные в Правиле 8. В-четвёртых, передача данных не отменяет права владельцев данных из Правила 14, в том числе права на доступ, исправление и удаление, то есть при непрерывном цикле использования данных в иностранной юрисдикции. В дополнение необходимо учитывать, что в силу Правила 23 Правительство вправе запрашивать информацию относительно обрабатываемых данных у соответствующих субъектов, в связи с чем даже при трансграничной передаче данных передающие субъекты обязаны продумывать механизм оперативного получения необходимой информации.

Соответственно, обязанности субъектов, передающих данные, содержащиеся в ряде положений DPDP Rules, следует учитывать и при осуществлении трансграничной передачи данных. Такое широкое регулирование, характерное для Индии, приводит к обязанности субъектов самостоятельно разрабатывать точные стандарты работы с данными с учётом особенностей взаимодействия с иностранной юрисдикцией. В банковской сфере это имеет особое значение, поскольку на банки-SDF возложена особая ответственность за защиту особо значимых данных.

Заключение

Таким образом, административно-правовое регулирование трансграничной передачи данных в банковской сфере в Индии осуществляется именно на основе положений DPDP Act, но не исключительно его нормами. Значимую роль играют акты Резервного банка Индии, положения DPDP Rules, а также акты Правительства по установлению ограничений на передачу данных в определённые юрисдикции или на передачу конкретных видов данных, которые будут приняты в дальнейшем – это составляет уникальную систему контроля трансграничной передачи данных, основанных на подходе “негативного списка”. В связи с этим при трансграничной передаче данных обеспечивается двойная проверка уровня защиты данных в иностранной юрисдикции как Правительством, так и передающим субъектом, который обязан учитывать как вероятность введения ограничений при несоблюдении требований в конкретной юрисдикции, так и наличие высокой ответственности за причинение ущерба пользователям в связи с угрозой безопасности их данных. Важный аспект локализации данных именно в банковской сфере регулируется актами Резервного банка Индии как специальными нормами в данной сфере. Наличие подобных требований также отличает индийское регулирование, однако такое строгое регулирование обеспечивает повышенный уровень защиты данных, что особенно важно в банковской среде, требует дополнительных затрат, но и стимулирует привлечение инвестиций в юрисдикцию с высокими стандартами защиты данных. Ещё одной особенностью режима данных в Индии является выделение субъектов, ответственных за обработку особо значимых данных, тогда как институт совместных субъектов, обрабатывающих данные, отсутствует. Это создаёт повышенные обязанности по защите данных для субъектов, получивших первый статус, и образует правовые лакуны в случае совместной работы с данными при отсутствии второго. Ряд общих требований, содержащихся в DPDP Act и DPDP Rules, также налагают дополнительные обязанности на банки в особенности при осуществлении трансграничной передачи данных.

Уникальный режим защиты данных в Индии обладает гибкостью, необходимой в быстро меняющихся условиях цифровой экономики, распределяет обязанности по контролю за стандартами обработки данных в иностранной юрисдикции между Правительством и передающим субъектом, что повышает степень защиты. Однако само регулирование является недостаточно детализированным, стабильным и проработанным, что стимулирует законодателей на его улучшение.

Список литературы:

[1] Ganga V. (2025) Cross-border data transfers and data localization under India‘s DPDPA 2023 – A comparative analysis with EU-GDPR // Indian Journal of Law and Legal Research. V. VII I. I. P. 2106 - 2120.

[2] Kashyap P. K. (2023) Digital Personal Data Protection Act, 2023: A new light into the data protection and privacy law in India. ICREP Journal of Interdisciplinary Studies. V. 2 I. I. P. 1-12.

[3] Katkuri S. (2025) A critical analysis of the Digital Personal Data Protection Act, 2023 // International Journal of Law. № 11. P. 22-24.

[4] Kermina M. P. (2023) The 2023 Digital Personal Data Protection Act: Evaluating its Strength in Protecting Citizen Data // Jus Corpus Law Journal. V. 4, I. 1. P. 112-119.

[5] Singh R. K. (2024) Analysing personal data protection (DPDP) bill, 2023 // International Journal of advanced legal research.V. 4, I. 3 . P. 1-19.

[6] Tandon U., Gupta, N.K. (2025) International Privacy in the Age of Artificial Intelligence: Critical Analysis of India‘s DPDP Act 2023 // Legal Issues in the Digital Age. V. 6. № 2. P. 87–117.

References:

[1] Ganga V. (2025) Cross-border data transfers and data localization under India’s DPDPA 2023 – A comparative analysis with EU-GDPR // Indian Journal of Law and Legal Research. V. VII I. I. P. 2106 - 2120.

[2] Kashyap P. K. (2023) Digital Personal Data Protection Act, 2023: A new light into the data protection and privacy law in India. ICREP Journal of Interdisciplinary Studies. V. 2 I. I. P. 1-12.

[3] Katkuri S. (2025) A critical analysis of the Digital Personal Data Protection Act, 2023 // International Journal of Law. № 11. P. 22-24.

[4] Kermina M. P. (2023) The 2023 Digital Personal Data Protection Act: Evaluating its Strength in Protecting Citizen Data // Jus Corpus Law Journal. V. 4, I. 1. P. 112-119.

[5] Singh R. K. (2024) Analysing personal data protection (DPDP) bill, 2023 // International Journal of advanced legal research.V. 4, I. 3 . P. 1-19.

[6] Tandon U., Gupta, N.K. (2025) International Privacy in the Age of Artificial Intelligence: Critical Analysis of India’s DPDP Act 2023 // Legal Issues in the Digital Age. V. 6. № 2. P. 87–117.