

СЕРДЮК Алевтина Леонидовна,
кандидат юридических наук, доцент,
доцент кафедры гражданского права
Санкт-Петербургского института (филиала)
ФГБОУ ВО «Всероссийский государственный
университет юстиции (РПА Минюста России)»,
e-mail: alevtinaserdyuk@yandex.ru

СОГЛАСИЕ СУБЪЕКТА ДАННЫХ КАК ОСНОВАНИЕ ТРАНСГРАНИЧНОЙ ПЕРЕДАЧИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Аннотация. В статье исследуется согласие субъекта данных как одно из правовых оснований трансграничной передачи персональных данных. Актуальность темы обусловлена тем, что цифровая экономика объективно зависит от международных потоков данных, тогда как государства одновременно усиливают требования к локализации, трансграничной передаче и защите персональных данных. Ограничения на потоки данных нередко принимают форму правового или фактического протекционизма, повышают транзакционные издержки и создают неопределенность для субъектов, осуществляющих предпринимательскую деятельность.

Ключевые слова: персональные данные, информация, согласие, трансграничная передача данных, защита персональных данных, локализация персональных данных.

SERDYUK Alevtina Leonidovna,
Candidate of Legal Sciences,
Associate Professor Associate Professor,
Department of Civil Law Saint Petersburg Institute
(Branch) of the All-Russian State University of Justice

CONSENT OF THE DATA SUBJECT AS A GROUND FOR THE CROSS-BORDER TRANSFER OF PERSONAL DATA

Annotation. The article examines the consent of the data subject as one of the legal grounds for the cross-border transfer of personal data. The relevance of the topic lies in the fact that the digital economy objectively depends on international data flows, while states are simultaneously strengthening requirements for data localization, cross-border transfer, and personal data protection. Restrictions on data flows often take the form of legal or de facto protectionism, increase transaction costs, and create uncertainty for business entities.

Key words: personal data, information, consent, cross-border data transfer, personal data protection, personal data localization.

Введение

Современная цифровая экономика основана на постоянном трансграничном движении информации: такие потоки необходимы для облачных сервисов, электронной коммерции, финансовых услуг, логистики, исследований и платформенных бизнес-моделей. В книге В. Меркуріо подчеркивается, что ограничение потоков данных создает форму торгового протекционизма, увеличивает издержки компаний и особенно чувствительно для субъектов малого и среднего предпринимательства; при этом с 2017

по 2021 год число стран, введивших барьеры локализации данных, заметно выросло [1, с. 24–25].

Одновременно именно в сфере трансграничной передачи проявляется слабость традиционной конструкции согласия: субъект формально выражает волю, но практически не контролирует ни юрисдикцию получателя, ни последующие передачи, ни доступ государственных органов третьей страны к его данным. Осложняется это и тем, что особенностью трансграничной передачи персональных данных является множественность

субъектного состава [2, с. 68]. Поэтому вопрос состоит не в том, может ли согласие использоваться вообще, а в том, в каких пределах оно допустимо и какими дополнительными гарантиями должно сопровождаться.

Методология

Методологическую основу статьи составляют:

- формально-юридический метод – для анализа правовых оснований трансграничной передачи;
- сравнительно-правовой метод – для сопоставления Европейского союза (далее – ЕС), Гонконга и Ассоциация государств Юго-Восточной Азии (далее – ASEAN);
- функциональный метод – для оценки того, насколько согласие реально защищает субъекта данных в трансграничных сценариях.

Обсуждение

Как отмечают F. Deane, E. Woolmer, S. Cao и K. Tranter, потоки данных составляют «сердце и душу цифрового оборота» [3, с. 157], что подчеркивает их системообразующее значение для цифровой экономики. Вывод персональной информации за рубеж по своей правовой природе относится к предоставлению персональной информации внешним субъектам.

В классической модели защиты персональных данных согласие рассматривается как выражение информационной автономии субъекта права. В этом смысле оно позволяет сделать законной обработку и последующую передачу данных при условии добровольности, информированности, конкретности и однозначности. Однако в сфере международных передач его роль закономерно сужается: чем выше правовой и технологический риск, тем менее оправдано возлагать защиту субъекта исключительно на его волеизъявление. Эту идею подтверждает европейская модель, где передача в третьи страны структурирована по иерархии: адекватность, надлежащие гарантии, и лишь затем – отдельные изъятия для специфических случаев, включая явное согласие.

В Гонконге конструкция согласия также встроена в систему трансграничной передачи: раздел 33 Personal Data (Privacy) Ordinance (PDPO) (раздел 33 не действовал, так как не был включён в действие с момента принятия закона в 1996 году) предусматривает письменное согласие субъекта данных как одно из условий допустимости передачи за пределы юрисдикции [1, с. 51]. Одновременно В. Меркуріо отмечает, что правовые системы, строящие передачу на чрезмерно сложных процедурах согласия, разрешений и

локального хранения, могут фактически подталкивать компании к локализации данных и росту комплаенс-издержек [1, с. 24, 34].

В Китае регулирование трансграничной передачи персональной информации строится вокруг трех основных комплаенс-механизмов:

- оценка безопасности;
- стандартный договор;
- профессиональная сертификация [4].

«В США сам факт предоставления пользователем своих персональных данных, необходимых для заключения и исполнения договора, который он добровольно подписывает (или принимает условия онлайн), рассматривается как подразумеваемое согласие» [5, с. 103].

Следовательно, согласие в контексте трансграничной передачи выполняет двойственную функцию: оно служит инструментом легитимации передачи, но при неудачной регуляторной конструкции либо становится фикцией, либо превращается в один из триггеров де-факто локализации. Именно эта двойственность и образует ядро исследуемой проблемы.

Даже если субъект дает согласие, он редко способен оценить правовой режим страны-импортера, риск доступа иностранных государственных органов, цепочку последующих получателей, различия в судебной защите и реальные последствия отзыва согласия после передачи. Европейская комиссия прямо указывает, что при отсутствии решения об адекватности и надлежащих гарантий согласие возможно только после предоставления субъекту всей необходимой информации о рисках такой передачи. Это уже показывает, что согласие в международном контексте не является достаточным основанием: оно предполагает повышенный стандарт раскрытия рисков.

European Data Protection Board (EDPB) в руководстве по derogациям статьи 49 General Data Protection Regulation (GDPR) рассматривает основания этой статьи как исключения, а не как стандартный маршрут для регулярных и масштабных потоков данных. Для ЕС системно предпочтительны решения об адекватности, стандартные договорные положения (SCC), обязательные корпоративные правила (BCR) и иные гарантии статьи 46; согласие же допускается как механизм для специфических ситуаций. Такой подход важен концептуально: право ЕС тем самым признает, что личная автономия не может компенсировать структурные риски чужой юрисдикции. EDPB подчеркивает, что derogации статьи 49 являются исключениями из общего принципа, поэтому должны толковаться ограничительно; экспортер данных должен сначала попытаться использовать механизмы статей 45 и 46.

Согласие теоретически может быть отозвано, но после трансграничной передачи реализация этого права осложняется множественностью участников обработки, различием процессуальных режимов и фактической утратой контроля над копиями данных. В такой ситуации согласие начинает работать преимущественно как формальный документ комплаенса, а не как эффективный способ управления риском. На это косвенно указывает и гонконгский подход: рекомендуется организациям использовать модельные договорные условия и иные управленческие меры, не полагаясь только на волеизъявление субъекта (Guidance on Recommended Model Contractual Clauses for Cross-border Transfer of Personal Data). Гонконг движется не в сторону абсолютного приоритета согласия, а в сторону комбинации общих принципов PDPO, мягкого права и договорных гарантий.

ЕС строит передачу данных в третьи страны по принципу приоритета институциональных гарантий. Европейская комиссия разъясняет, что при наличии решения об адекватности дополнительные гарантии не требуются; при его отсутствии применяются SCC, BCR, коды поведения и сертификация; только если эти инструменты отсутствуют, возможны дерогации, включая явное согласие после информирования о рисках. В настоящее время Европейская комиссия также продолжает признавать механизм EU-U.S. Data Privacy Framework как основание свободной передачи данных в сертифицированные американские компании, что еще раз показывает, что ЕС стремится опираться не на массовое согласие субъектов, а на институционализированные механизмы.

Эту же тенденцию фиксирует исследование трансграничных потоков данных и управления данными: международные соглашения, решения об адекватности, стандартные договорные положения и иные институциональные инструменты становятся ключевыми в поддержании законных потоков данных в условиях фрагментации правовых порядков [6, с. 56-57, 79-80].

ASEAN предлагает иной тип решения: не иерархию «запрет – исключение», а механизм региональной совместимости через ASEAN Data Management Framework, Implementing Guidelines и ASEAN Model Contractual Clauses (ASEAN MCC). Совместное руководство ASEAN и ЕС прямо ориентировано на повышение интероперабельности ASEAN MCC и EU SCC. Это принципиально важно, потому что ASEAN-подход демонстрирует, что устойчивость трансграничной передачи обеспечивается прежде всего не индивидуальным согласием, а стандартизированными обязательствами получателя, организационной подотчет-

ностью и едиными практиками управления данными.

Проблема согласия как основания трансграничной передачи состоит в том, что оно:

- индивидуализирует системный риск, перекладывая на субъекта оценку чужой юрисдикции;
- формализует защиту, но не гарантирует реального контроля после передачи;
- не покрывает последующие передачи и множественность обработчиков;
- не устраняет дисбаланс сил между субъектом и цифровой платформой;
- может усиливать правовую неопределенность, если используется вместе с непрозрачными процедурами согласования и решений.

Комбинация жестких требований к передаче, специального согласия и неопределенности способна вести к де-факто локализации данных (1, с. 24, 34), а фрагментарная политика создает риск для бизнеса и инвестиций (1, с. 52, 60-61).

Как отмечает А.Д. Курсова, согласие персональных данных отвечает ряду требований и принципов, которые должны быть согласованы между собой и, вместе с тем, данное согласие одному оператору должно гарантировать, что субъект сможет осуществлять свои права по отношению и к другим операторам, которые задействованы в обработке персональных данных [7, с. 192].

Иными словами, согласие не должно быть центром трансграничного режима. Оно может оставаться элементом системы, но не ее опорой. Для устойчивого баланса между свободой потоков данных и защитой личности требуется более сложная архитектура правовых, организационных и технических гарантий. В этом смысле согласие субъекта данных не может рассматриваться как самодостаточная гарантия, поскольку общая цель режима международной передачи состоит в недопущении снижения уровня защиты после вывоза данных за пределы юрисдикции ЕС [8].

Основные результаты

В случаях международного обмена данными представляется обоснованным закрепить в рамках правового регулирования и в правоприменении следующую модель:

- первый уровень – должны использоваться решения об адекватности и иные межюрисдикционные механизмы признания эквивалентности режима защиты;
- второй уровень – надлежащие гарантии: SCC, BCR, модельные контрактные положения, сертификация и коды поведения;

- третий уровень – исключительные derogации, включая согласие, применимые только тогда, когда передача носит эпизодический, ограниченный и действительно понятный субъекту характер. Такая архитектура соответствует логике GDPR и одновременно совместима с развитием гонконгских и ASEAN-механизмов.

Считаем, что только согласие не может быть достаточным основанием для трансграничной обработки данных, но возможно только при одновременном наличии следующих условий:

- передача не носит массового и постоянного характера;
- субъекту сообщены конкретные риски иностранной юрисдикции;
- отсутствует более надежный механизм передачи;
- субъект может отказаться без утраты базового доступа к услуге, если передача не является объективно необходимой;
- для чувствительных данных применяются дополнительные технические и договорные меры. Такой подход следует из европейских разъяснений по статье 49 и из общей логики EDPB о вспомогательном характере derogаций.

Даже когда передача основана на договорных условиях, экспортер должен проводить оценку режима доступа публичных органов, исполнимость договорных обязательств, доступные средства правовой защиты и вероятность последующих передач. Такая оценка особенно важна после решения Суда юстиции Европейского Союза (CJEU), принятое 16 июля 2020 года (Schrems II) и отражена в европейских и британских рекомендациях по международным передачам.

Наиболее перспективный вектор развития – это переход от модели «субъект все разрешил» к модели «оператор доказал наличие устойчивых, проверяемых и исполнимых гарантий». Такой подход лучше соответствует реальной сложности цифровой инфраструктуры и глобальных цепочек поставок данных. [6, с. 79-80]

В. Меркурיו отдельно акцентирует чувствительность трансграничного регулирования для малого и среднего бизнеса [1, с. 24, 52]. Соглашаясь с анализом и предложениями ученого, считаем, что регулятору следует разработать:

- типовые договоры;
- чек-листы оценки передачи;
- матрицы странового риска;
- безопасные отраслевые профили передачи данных;
- упрощенные шаблоны уведомлений субъектов.

Такой подход уменьшает риск того, что сложность регулирования будет толкать бизнес либо к формальному согласию, либо к избыточной локализации данных.

В российском праве альтернативы согласию уже существуют на уровне общих оснований обработки.

Применительно к российской правовой действительности Зюбанов К.А. отмечает, что «согласие на обработку персональных данных, ввиду своей специфики как с точки зрения правоотношений, регулируемых законодательством в области персональных данных, так и с точки зрения механики функционирования этого инструмента, имеющего основной целью обеспечение прав субъектов персональных данных, имеет двойственную природу, частно- и публично-правовые аспекты» [9, с. 631]. Вместе с тем, именно в подходах российского законодателя находит отражение то, что необходимо различать основание обработки персональных данных и условия допустимости их трансграничной передачи. Основания обработки перечислены в статье 6 Федерального закона 27.07.2006 № 152-ФЗ «О персональных данных» это не только согласие, но и исполнение закона, договора, защита жизненно важных интересов, законные интересы оператора или третьих лиц, научные и статистические цели и др.

Следовательно, трансграничная передача в российском праве не сводится к согласию как к единственному юридическому титулу; согласие – лишь один из возможных общих режимов правовой обработки.

Заключение

Согласие субъекта данных сохраняет значение в системе трансграничной передачи персональных данных, однако его роль должна быть строго ограниченной. В международном контексте оно не способно само по себе обеспечить эквивалентность правовой защиты, как это наблюдается в национальных правовых режимах, нейтрализовать риски иностранной юрисдикции, гарантировать контроль над последующей обработкой и компенсировать фактическое неравенство сторон. Поэтому согласие следует понимать не как универсальное основание, а как исключительную derogацию, применимую лишь в узких и прозрачных случаях.

Сравнительный анализ показывает, что наиболее жизнеспособные модели смещают центр тяжести с индивидуального согласия на институциональные гарантии: решения об адекватности, стандартные договорные условия, корпоративные правила, оценку рисков передачи и дополнительные технические меры. Для государств и

регуляторов это означает, что задача состоит не в умножении форм согласия, а в создании согласованной и предсказуемой архитектуры трансграничной передачи данных, это позволит обеспечить создание целостной и согласованной политики в сфере трансграничных потоков данных, о необходимости которой говорят и зарубежные исследователи [1, с. 60-61].

Список литературы:

[1] Mercurio B., Yu R. *Regulating Cross-Border Data Flows – Issues, Challenges and Impact*. – London : Anthem Press, 2022. – 94 p.

[2] Гатиятуллина Э. М. Правовое регулирование трансграничной передачи персональных данных в цифровой экономике // Основные тенденции развития современного права: проблемы теории и практики : материалы IX Национальной научно-практической конференции. В 2-х частях, Казань, 27–28 февраля 2025 года. – Казань : Университет управления «ТИСБИ», 2025. – С. 67–73.

[3] Deane F., Woolmer E., Cao S., Tranter K. *Trade in the Digital Age: Agreements to Mitigate Fragmentation* // *Asian Journal of International Law*. – 2024. – Vol. 14. – P. 154–179. – DOI: 10.1017/S204425132300036X.

[4] Ren Ya., Cai S. *Balance of Efficiency and Security: Improvement of China's Personal Information Exit Compliance Path* // *Economic Problems and Legal Practice*. – 2023. – Vol. 19, No. 1. – P. 108–113. – DOI: 10.33693/2541-8025-2023-19-1-108-113.

[5] Левашенко А., Синельников-Мурылев С. Персональные данные: экономические проблемы и правовое регулирование // *Экономическая политика*. – 2025. – Т. 20, № 6. – С. 96–119. – DOI: 10.18288/1994-5124-2025-6-96-119.

[6] Восс У. Г. Трансграничные потоки данных, общий регламент защиты персональных данных и управление данными // *Вестник международных организаций*. – 2022. – Т. 17, № 1. – С. 56–95. – DOI: 10.17323/1996-7845-2022-01-03.

[7] Курсова А. Д. Согласие как правовое основание обработки персональных данных // *Седьмые цивилистические чтения памяти профессора М. Г. Прониной : сборник материалов*, Минск, 03 апреля 2025 года. – Минск : Академия управления при Президенте Республики Беларусь, 2025. – С. 188–193.

[8] Marelli M. *Transferring personal data to international organizations under the GDPR: an analysis of the transfer mechanisms* // *International Data Privacy Law*. – 2024. – Vol. 14, No. 1. – P. 19–36. – DOI: 10.1093/idpl/ipad022.

[9] Зюбанов К. А. Согласие на обработку персональных данных – sui generis действие // *Вестник Российского университета дружбы народов. Серия: Юридические науки*. – 2024. – Т. 28, № 3. – С. 622–633. – DOI: 10.22363/2313-2337-2024-28-3-622-633.

References:

[1] Mercurio B., Yu R. *Regulating Cross-Border Data Flows – Issues, Challenges and Impact*. – London : Anthem Press, 2022. – 94 p.

[2] Gatiyatullina E. M. *Legal regulation of cross-border transfer of personal data in the digital economy//Main trends in the development of modern law: problems of theory and practice: materials of the IX National Scientific and Practical Conference*. In 2 parts, Kazan, February 27-28, 2025. – Kazan: University of Management "TISBI," 2025. – S. 67-73.

[3] Deane F., Woolmer E., Cao S., Tranter K. *Trade in the Digital Age: Agreements to Mitigate Fragmentation* // *Asian Journal of International Law*. – 2024. – Vol. 14. – P. 154–179. – DOI: 10.1017/S204425132300036X.

[4] Ren Ya., Cai S. *Balance of Efficiency and Security: Improvement of China's Personal Information Exit Compliance Path* // *Economic Problems and Legal Practice*. – 2023. – Vol. 19, No. 1. – P. 108–113. – DOI: 10.33693/2541-8025-2023-19-1-108-113.

[5] Levashenko A., Sinelnikov-Murylev S. *Personal data: economic problems and legal regulation// Economic policy*. – 2025. – T. 20, NO. 6. – S. 96-119. – DOI: 10.18288/1994-5124-2025-6-96-119.

[6] Voss U. G. *Cross-Border Data Flows, General Regulation on Personal Data Protection and Data Management//Bulletin of International Organizations*. – 2022. – T. 17, NO. 1. – S. 56-95. – DOI: 10.17323/1996-7845-2022-01-03.

[7] Kursova A.D. *Consent as a legal basis for the processing of personal data//Seventh civil readings in memory of Professor M.G. Pronina: a collection of materials*, Minsk, April 03, 2025. – Minsk: Academy of Management under the President of the Republic of Belarus, 2025. – S. 188-193.

[8] Marelli M. *Transferring personal data to international organizations under the GDPR: an analysis of the transfer mechanisms* // *International Data Privacy Law*. – 2024. – Vol. 14, No. 1. – P. 19–36. – DOI: 10.1093/idpl/ipad022.

[9] Zyubanova K. A. *Consent to the processing of personal data - sui generis action//Bulletin of the Peoples' Friendship University of Russia. Series: Legal Sciences*. – 2024. – T. 28, NO. 3. – S. 622-633. – DOI: 10.22363/2313-2337-2024-28-3-622-633.

