Национальное регулирование вопросов трансграничной передачи данных

Ольга Исмагилова, Карина Кудакаева

Цифровизация влечет за собой беспрецедентный рост объемов и темпов сбора, обработки, передачи и хранения данных за счет оптимизации процессов на всех этапах. По данным ОЭСР, с 2012 г. количество изобретений в области передачи данных, запатентованных пятью странами — мировыми лидерами[1] по интеллектуальной собственности в данной сфере, в среднем росло на 19% в год.

Сбор и передача данных служит источником создания стоимости — данные используются не только непосредственно для предоставления пользователям товаров и услуг, но также для аналитики и создания новых предложений для потребителей.

Национальное регулирование вопросов передачи данных обусловлено необходимостью защиты конфиденциальности[2] и обеспечения информационной безопасности при трансграничной передаче персональных и других чувствительных категорий данных. При этом барьеры, связанные с ограничением свободного трансграничного перемещения потоков данных, увеличивают время и расходы компаний на осуществление внешнеэкономической деятельности (как экспорта, так и импорта), и могут препятствовать развитию новых технологий (таких как интернет вещей, искусственный интеллект и другие).

Можно выделить 3 подхода к вопросам трансграничной передачи данных на уровне национального регулирования (см. рисунок):

1. Передача данных запрещена.
2. Передача данных разрешена при выполнении определенных законодательных требований.
3. Передача данных разрешена во все страны без необходимости соблюдения каких-либо дополнительных законодательных требований.

Полный запрет на трансграничную передачу данных является наиболее жесткой мерой защиты и применяется лишь небольшим числом стран. Например, в Саудовской Аравии конфиденциальные данные государственных органов и потребительские данные частных фирм не могут передаваться за пределы страны ни по какой причине. В Индонезии существует запрет на передачу данных, связанных с предоставлением населению услуг (к примеру, финансовых), в том числе частными фирмами. В Китае не разрешена передача за рубеж персональной информации, собираемой коммерческими банками. При этом другие типы персональных данных могут передаваться за границу при соблюдении необходимых требований.

Какие-либо ограничения на трансграничную передачу персональных данных применяются многими странами (см. рисунок) и могут быть связаны с:

— Необходимостью получения разрешения ответственных органов власти и / или согласия субъекта персональных данных.
— Дополнительными требованиями по локализации (хранению определенных данных на территории страны)[3].
— Ограничением числа стран, в которые можно передавать персональные данные.

Ограничения на передачу данных чаще всего носят комплексный характер и представляют собой сочетание 2–3 из указанных выше мер. В Китае локализационные требования сочетаются с необходимостью получения разрешения на передачу данных в каждом конкретном случае после прохождения необходимых проверок в области безопасности[4] — это касается персональных данных и важной информации, собираемой операторами критической информационной инфраструктуры. Зачастую для разных категорий данных применяются разные требования.

В отдельных случаях национальное законодательство предусматривает альтернативные меры защиты данных при их трансграничной передаче. Так, во многих странах (см. рисунок на стр. 10) передача данных возможна лишь в страны с «адекватным» уровнем защиты[5]. В некоторых случаях возможна передача данных и в страны, не обеспечивающие уровень защиты аналогичный национальному.

[1] США, Япония, Южная Корея, Китай и Тайвань.

[2] О международной практике регулирования вопросов защиты данных мы писали в Мониторинге №33.

[3] Подробнее существующие ограничения, связанные с локализацией данных, будут рассмотрены в следующем выпуске Мониторинга.

[4] Проверка исходящей информации осуществляется в отношении рисков для безопасности национальной обороны и политической системы, экономики, науки и технологий.

[5] К примеру, ЕС признает 12 стран, где обеспечивается уровень защиты данных, аналогичный европейскому — Андорра, Аргентина, Канада, Швейцария, Израиль, Новая Зеландия, США, Уругвай, Фарерские острова; острова Гернси, Мэн и Джерси.

Например, в России, Аргентине, Турции, Австралии, Колумбии, Мексике, Израиле, ЕС и Перу для этого необходимо получить разрешение субъекта персональных данных. В ЮАР в таком случае помимо согласия субъекта требуется специальное разрешение регулирующих органов. Во многих странах также существует обширный список исключений, обеспечивающих свободу передачи данных. Например, согласно условиям контракта, обязательствам по международным соглашениям или в случае обеспечения жизненно важных интересов субъекта персональных данных при невозможности получения его согласия.

Интересен пример Тайваня, законодательство которого запрещает передачу персональных данных лишь на территорию материкового Китая.

Требования по локализации не всегда влекут за собой запрет на передачу данных. Так, согласно российскому законодательству, персональные данные граждан можно передавать за рубеж при соблюдении условия их хранения на территории России. А в США существуют требования по локализации отдельных видов данных. Кроме того, в отдельных штатах ограничена передача данных, связанных с оказанием государственных услуг населению. В то же время национальное регулирование предполагает, что трансграничное перемещение данных может осуществляться свободно во все страны без необходимости получения какого-либо разрешения органов власти либо согласия субъекта, что позволяет отнести США к последнему блоку — странам без барьеров в области передачи данных. При этом, в случае нарушения общих требований законодательства к обеспечению хранения данных или в случае их неправомерного использования компании привлекаются к ответственности (например, налагается внушительный штраф).

Различия в подходах стран к трансграничной передаче данных

* Для отдельных категорий данных

** Требование может не выполняться при соблюдении других (альтернативных) мер защиты