Проблемы регулирования трансграничных потоков данных в мировой экономике

УДК 339.5(100) + 004.65
ББК 65.428(0) + 32
А-900
DOI: 10.24411/2072-8042-2021-1-51-59

Анна Викторовна АСАДУЛЛИНА,
кандидат экономических наук,
Всероссийская академия внешней торговли
(119285, Москва, Воробьевское шоссе, 6а),
кафедра мировой и национальной экономики - доцент,
e-mail: aasadullina@vavt.ru

Аннотация

В настоящее время потоки цифровых данных через границы являются центральной частью глобальных цепочек создания стоимости и ключевым условием функционирования широкого круга отраслей промышленности и сферы услуг.

Повсеместный обмен данными через границы вызывает обеспокоенность правительств и приводит к появлению новых регуляторных правил по их защите, продиктованных, в том числе, желанием стран использовать базы данных для поощрения внутреннего развития цифровых секторов, что является по сути новой формой протекционизма. Требования к локальному хранению данных могут ухудшать условия торговли и производства, закрыв доступ к более дешевым глобальным цифровым услугам.

Организация на постоянной основе межстранового диалога по созданию системы функциональной совместимости между национальными системами защиты персональных данных позволит поддержать развитие международной торговли и не допустить «разорванности» мирового цифрового пространства.

Ключевые слова: Трансграничные потоки данных, запрет на передачу данных, требования о локальном хранении, конфиденциальность и безопасность, Общий регламент по защите данных ЕС, международная торговля, протекционизм.

Issues of Cross-Border Data Flows Regulations in the World Economy

Anna Victorovna ASADULLINA,
Candidate of Economic Sciences,
Russian Foreign Trade Academy (119285, Moscow, Vorob'evskoe shosse, 6A),
Department of World and National Economy - Associate Professor,
e-mail: aasadullina@vavt.ru

Abstract

Nowadays cross-border data flows play a critical role in the global value chains and a broad range of manufacturing and services industries.

Worldwide cross-border data flows are a source of concern for the governments that prompts them to adopt new data protection regulations as countries encourage the use of databases to promote their domestic digital industries, which is in effect a new form of protectionism. The local data storing requirements may affect adversely the trade and production by preventing access to cheaper global digital services.

A permanent cross-border dialogue for interoperability of the national personal data protection systems might facilitate global trade and avoid the so-called digital fragmentation.

Keywords: Cross-border data flows, prohibit the transfer of data abroad, local storage requirements, consumer and security, General Data Protection Regulation, international trade, protectionism.

В настоящее время потоки данных через границы являются центральной частью глобальных цепочек создания стоимости и основным требованием для функционирования широкого круга отраслей обрабатывающей промышленности и сферы услуг. Стратегическое развитие бизнеса зависит от способности анализировать большие наборы данных; потоки данных являются неотъемлемой частью современных логистических систем и электронных таможенных процедур.

Однако повсеместный обмен данными через границы вызывает обеспокоенность правительств и граждан по поводу некоторых негативных побочных эффектов, связанных со сбором, передачей и использованием такого большого количества информации, в частности, личных данных или идентифицирующей личность информации, часто без ведома тех лиц, к которым относятся данные. В некоторых странах проблемы, связанные с конфиденциальностью и/или национальной безопасностью, привели к растущим призывам к более глубокому и более широкому регулированию Интернета и основополагающих потоков данных. В результате правительства обновляют правила, связанные с данными, и все чаще обуславливают передачу данных через границы или вводят требования о локальном хранении.

Нам представляется целесообразным первоначально в статье представить таксономию понятия передача данных.

В основе Интернета лежит глобальная сеть компьютеров, имеющих персональные идентификационные устройства – IP-адреса. Когда файл (поисковый запрос, запрос сайта, запрос видео и пр.) отправляется с определенного компьютера одной страны получателю из другой страны, он разбивается на небольшие пакеты информации, которые потом повторно собираются в пункте назначения. Небольшие пакеты информации следуют в пункт назначения по разным маршрутам, находящимся часто в разных странах (или даже континентах). Маршрутизаторы направляют информационные пакеты по сетям, выбирая самые короткие и

наименее загруженные маршруты. Такой характер передачи априорно затрудняет определение географической принадлежности потоков данных; причем данная задача становится еще более сложной с учетом того, что для повышения скорости потока и надежности передачи фирмы используют «зеркала», расположенные в разных странах и реплицирующие веб-страницы. Например, если пользователь хочет получить доступ к британской газете из Франции, то маршрутизаторы ведут пакеты информации по сетям трех стран: Франции, США и Польши, минуя Великобританию. А абсолютно внутренний информационный запрос в Париже доступа к электронной библиотеке ОЭСР будет проходить через сервер в США, являясь, тем самым, трансграничным.

Важным является и то, что ценность передаваемых данных не тождественна их объему. Однако в отличие от цены, например поставки оборудования, сложно определить внутреннюю стоимость данных: в основе оценки внутренней ценности должен лежать не объем, а способ их применения. Бесспорно то, что передаваемый файл Excel, содержащий в себе сто персональных записей покупок индивида в онлайн-магазине и занимающий тот же объем памяти, что и файл со ста записями в картах медицинских учреждений, будет менее ценен исходя из последствий потери (кражи) последних. Кроме того, ценность данных может также увеличиться, когда объединение станет больше, чем сумма его частей. Например, записи о покупках, связанные с медицинскими записями, могут помочь таргетировать рекламные объявления. Еще одной отличительной характеристикой данных является то, что кроме внутренней ценности они имеют и потенциальную ценность: неиспользуемая сегодня информация может стать ценной завтра с изменением динамики бизнеса или в сочетании с другими данными, которые еще не стали доступны.

Понимание все более важной роли и ценности передачи данных обращает пристальное внимание регулирующих органов как на национальном, так и на наднациональном уровне. Для целей международной торговли товарами и услугами проблема регулирования обмена и трансграничного перемещения данных особенно актуальна и должна решаться дифференцировано, в зависимости от типа данных, которые можно представить в виде следующих групп:

- персональные данные или информация, идентифицирующая личность[1];
- данные по отдельным секторам экономики;
- «важные (критические) данные», определяемые как данные, относящиеся к национальной безопасности, экономическому развитию и общественным интересам.

ОЭСР определяет персональные данные как любую информацию, касающуюся идентифицированного или идентифицируемого лица, что предполагает, что если один аспект набора данных может быть связан с конкретным человеком, тогда все эти данные могут стать личными. Более того, с изменениями в технологии деидентифицированные данные могут быть повторно идентифицированы и то, что сегодня считается неличными, может стать персональными данными завтра.

Если рассматривать регуляторные правила по защите данных, которые существуют в настоящее время на национальных уровнях, то можно все правила разделить на 2 группы:

1. Ограничения на трансграничные потоки данных;

2. Локальные требования к хранению данных.

Ориентировочная таксономия подходов к трансграничным потокам данных может быть представлена следующим образом[2]:

1. Первый подход – назовем его либеральным – характеризуется свободной передачей данных – свободным потоком, и предполагает отсутствие запретов на трансграничную передачу данных и требования выполнения каких-либо конкретных условий для перемещения данных через границы, однако предусматривается постотчетность экспортера данных, если личные данные, отправленные за границу, используются не по назначению.

2. Передача данных в зависимости от предоставляемых гарантий – поток, обусловленный защитой, – трансграничная передача данных разрешается только в том случае, если соблюдаются условия адекватности или эквивалентности, которые могут оцениваться самим экспортером и/или специально уполномоченным государственным органом.

3. Ограничительный поток, подлежащий авторизации – переводы данных являются каждый раз предметом рассмотрения соответствующих государственных органов.

Вторая большая группа правил касается норм хранения данных и, как и в случае трансграничного регулирования потоков данных, даже в пределах одной страны могут существовать разные правила хранения и обработки к разным типам данных. Требования по хранению и обработке данных могут носить личный характер, секторальный характер (чаще всего с указанием на сектор здравоохранения, банковский сектор, страхование и картографирование), указывать на критически важную инфраструктуру. Требования к локальному хранению данных варьируются в диапазоне от отсутствия требований до требований к хранению и обработке с ограничением потока.

Первая категория – отсутствие требований для локального хранения данных по умолчанию, является довольно распространенной по странам, учитывая, что количество страновых требований по локальному хранилищу данных небольшое (и чаще направлено только на определённые сектора).

Вторая категория – это подход, в соответствии с которым устанавливаются требования по сохранению копии целевых данных во внутренних вычислительных средствах компаний (метаданные электросвязи и финансовые данные предприятий); либо подход, по которому обработка данных может происходить за границей, но при постобработке данные должны быть возвращены на родину для хранения. И последняя категория правил предполагает, чтобы данные хранились только локально.

Анализируя опыт отдельных стран в политике регулирования потоков трансграничных данных, можно заметить, что этот опыт в основной своей массе отражает основные предпочтения граждан в области защиты личной жизни:

Таблица 1

Ключевые элементы регулирования трансграничного потока данных в ряде стран мира (2020)

	Наименование законодательного акта	*Основное содержание*
1.	КНР - Закон о кибербезопасности Китайской Народной Республики/ The People's Republic of China Cyber Security Law (CSL)[3], 2017 г.	Рамочный закон, руководящие принципы которого применяются к личным данным, определяемым как информация, которая может использоваться для определения личности физического лица; и к «критическим» данным, определяемым как данные, относящиеся к национальной безопасности, экономическому развитию и общественным интересам. Обязательства по передаче данных возлагаются на сетевых операторов (любой компании, работающей через компьютерную сеть); операторов критически важной информационной инфраструктуры (СПО). К СПО предъявляют более строгие требования, включая требования к локальному хранению данных. Для международной передачи персональных данных требуется четкое требование «уведомление-согласие» при любых обстоятельствах.
2.	Австралия - Закон о конфиденциальности 1988 года (с изменениями и дополнениями) / Privacy Act 1988, Privacy Regulation 2013, Amendment (Notifiable Data Breaches) Act 2017.	Устанавливаются 13 принципов конфиденциальности (APP) - стандарты сбора, использования, раскрытия, качества и безопасности личной информации. Закон применяется к «субъектам APP», включая правительственные учреждения, организации частного сектора с годовым оборотом в 3 млн. долл США и более, а также к некоторым более мелким организациям, где они имеют непосредственное отношение к личной информации (поставщики медицинских услуг частного сектора, органы кредитной отчетности, кредитные организации).

	Наименование законодательного акта	*Основное содержание*
3.	Япония - Закон о защите личной информации/ The Act on the Protection of Personal Information (APPI), 2017.	Регулирует вопросы защиты частной жизни в Японии, устанавливает в качества надзорной правительственной организации по вопросам защиты конфиденциальности Комиссию по защите личной информации (PPC). Вводит как общие требования по передаче данных третьей стороне, так и трансграничные требования. Предписывает обязанность получать предварительно согласие субъектов данных для передачи их содержания третьим сторонам в страны, не включенные в белый список APPI или третьим сторонам, не установившим аналогичные APPI адекватные стандарты защиты конфиденциальности. В настоящее время страны ЕС определены как страны из белого списка на основании решения об адекватности от 23 января 2019 года. Согласно руководящим принципам для морских перевозок, одним из примеров приемлемой международной структуры является система CBPR АТЭС.
4.	Европейский союз - Общий регламент по защите данных/ General Data Protection Regulation (вступил в силу 25.05.2018) [4]	Регламент имеет экстерриториальный характер: распространяется и на компании из стран, не входящих в Евросоюз. Разрешает трансграничную передачу данных в случаях: • принятия адекватного решения в отношении системы защиты данных страны-получателя на основе критериев, содержащихся в «Справочнике адекватности» (к примеру, двустороннее соглашение с Японией об адекватности); • присутствуют специальные меры предосторожности в виде обязательных корпоративных правил или стандартных договорных положений или публичных соглашений между правоохранительными органами.

	Наименование законодательного акта	*Основное содержание*
5.	Россия[5]- Закон о персональных данных/ Федеральный закон от 21 июля 2014 г. N 242-ФЗ	Согласно закону операторы данных, собирающие персональные данные о гражданах России, должны записывать, систематизировать, накапливать, хранить, изменять, обновлять и извлекать данные, используя базы данных, физически расположенные в России. Эти персональные данные могут быть переданы, но только после того, как они будут впервые сохранены в России. Локализации данных для телекоммуникационных данных. Российский подход гораздо шире, чем требования к хранению данных телекоммуникаций других стран, поскольку он требует от компаний хранить фактическое содержимое сообщений пользователей в течение шести месяцев, таких как голосовые данные, текстовые сообщения, изображения, звуки и видео, а не только метаданные (кто, когда и как долго сообщения). Во-вторых, он требует, чтобы телекоммуникационные компании и интернет-провайдеры сокращали услуги для пользователей, если они не отвечают на запрос правоохранительных органов о подтверждении их личности (что вызывает ряд вопросов конфиденциальности).

Источник: составлено автором.

Россия относится к группе стран, где действует наиболее жесткий подход к защите персональных данных ее граждан – требования о локальном их хранении: согласно закону о персональных данных, операторы данных, собирающие персональные данные о гражданах России, должны «записывать, систематизировать, накапливать, хранить, изменять, обновлять и извлекать» данные, используя базы данных, физически расположенные в России. Эти персональные данные могут быть переданы, но только после того, как они будут впервые сохранены в России.

Несмотря на вступление в силу в Европейском союзе Общего регламента по защите данных, вопрос о локализации данных до сих пор является спорным. Так, Франция и Германия не поддерживают введение запрета на локализацию данных; Швеция и Великобритания требуют свободного их перемещения через границы.

Причины, по которым национальные правительства ограничивают трансграничные потоки данных, могут состоять в следующем:

- в разной степени существующая на национальном уровне обеспокоенность по поводу конфиденциальности идентифицирующей личность информации;

• стремление к доступности данных для целей аудита в отдельных специфичных отраслях, поддержанное нормативными требованиями государств (телекоммуникационная, банковская и пр. сферы);

• обеспечение национальной безопасности как в плане защиты информации, которая считается конфиденциальной, так и в отношении возможности служб национальной безопасности государства получать и просматривать данные. Последнее, в частности, может быть очень широким по своей природе, обеспечивая широкий диапазон доступа к любой форме данных.

Кроме того, обуславливание трансграничных потоков данных и необходимость локального хранения может быть продиктовано желанием стран использовать базы данных для поощрения внутреннего развития цифровых секторов, что является по сути новой формой промышленной политики[6].

В виду того что использование трансграничных данных широко распространено не только в сфере ИКТ и услуг, но и на всех этапах проектирования, производства, доставки и продажи товаров компаний, занимающихся производственной деятельностью, новые условия регулирования данных вызывают у бизнес-сообщества все большую озабоченность.

Действительно, меры, обуславливающие доступ к цифровому потоку данных и его использование, оказывают влияние на эффективность отдельных стадий и жизнеспособность цепочек создания стоимости для современного производства.

Так, например, требования к локальному хранению данных, являющиеся по сути аналогом традиционной стратегии импортозамещения, могут ухудшать условия торговли и производства в силу того, что заставят фирмы переключиться на потенциально менее надежных и эффективных, и более дорогих местных поставщиков, и закроют доступ к глобальным цифровым услугам или международным решениям на основе аутсорсинга[7].

Преодоление «разорванности» цифрового пространства и обеспечение прозрачности, недискриминационного характера правил регулирования потоков трансграничных данных для поддержания международной торговли делает, таким образом, необходимой организацию на постоянной основе межстранового диалога, который бы позволил достичь большей функциональной совместимости между национальными системами защиты персональных данных.

ПРИМЕЧАНИЯ:

[1] The OECD Privacy Framework. Электронный ресурс. Режим доступа: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

[2] Casalini F., González J. López (2019-01-23), "Trade and Cross-Border Data Flows", OECD Trade Policy Papers, No. 220, OECD Publishing, Paris. Электронный ресурс: http://dx.doi.org/10.1787/b2023a47-en

[3] The People's Republic of China Cyber Security Law. Электронный ресурс.: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/

[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. [Электронный ресурс]. Режим доступа: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016R0679-20160504

[5] Федеральный закон от 21 июля 2014 г. N 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях». [Электронный ресурс]. Режим доступа: http://base.garant.ru/70700506/#ixzz6Ll46sj3G

[6] Casalini F., González J. López (2019-01-23), "Trade and Cross-Border Data Flows", OECD Trade Policy Papers, No. 220, OECD Publishing, Paris. Электронный ресурс: http://dx.doi.org/10.1787/b2023a47-en

[7] National Board of Trade (2015), "No Transfer, No Production – a Report on Cross-Border Data Transfers, Global Value Chains, and the Production of Goods", Kommerskollegium, Stockholm. Электронный ресурс: https://unctad.org/system/files/non-official-document/dtl_ict4d2016c02_Kommerskollegium_en.pdf

БИБЛИОГРАФИЯ:

1. Федеральный закон от 21 июля 2014 г. N 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях». [Электронный ресурс]. Режим доступа: http://base.garant.ru/70700506/#ixzz6Ll46sj3G (Federal`ny`j zakon ot 21 iyulya 2014 g. N 242-FZ «O vnesenii izmenenij v otdel`ny`e zakonodatel`ny`e akty` Rossijskoj Federacii v chasti utochneniya poryadka obrabotki personal`ny`x danny`x v informacionno-telekommunikacionny`x setyax». [E`lektronny`j resurs]. Rezhim dostupa)

2. The Act on the Protection of Personal Information (APPI), 2017. [Электронный ресурс]. Режим доступа: https://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf

3. Casalini F., González J. López, "Trade and Cross-Border Data Flows", OECD Trade Policy Papers, No. 220, 2019. - OECD Publishing, Paris. Электронный ресурс: http://dx.doi.org/10.1787/b2023a47-en

4. No Transfer, No Production – a Report on Cross-Border Data Transfers, Global Value Chains, and the Production of Goods/ Kommerskollegium, Stockholm - 2015. Электронный ресурс: https://unctad.org/system/files/non-official-document/dtl_ict4d2016c02_Kommerskollegium_en.pdf

5. The OECD Privacy Framework. Электронный ресурс. Режим доступа: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

6. Privacy regulation 2013, Amendment (Notifiable Data Breaches) Act 2017. [Электронный ресурс]. Режим доступа: https://www.oaic.gov.au/privacy/notifiable-data-breaches/

7. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. [Электронный ресурс]. Режим доступа: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016R0679-20160504