Экономическая политика. 2020. Т. 15. № 3. С. 152–175 DOI: 10.18288/1994-5124-2020-3-152-175

Цифровая экономика

МИРОВОЙ ОПЫТ РЕГУЛИРОВАНИЯ ЗАЩИТЫ, ПЕРЕДАЧИ И ХРАНЕНИЯ ДАННЫХ

Ольга ИСМАГИЛОВА, Каринэ ХАДЖИ

Ольга Дмитриевна Исмагилова — научный сотрудник Института международной экономики и финансов, Всероссийская академия внешней торговли (РФ, 119285, Москва, Воробьевское ш., 6А); Российский центр исследований АТЭС, РАНХиГС (РФ, 119034, Москва, Пречистенская наб., 11).
E-mail: oibrishim@gmail.com

Каринэ Рафаэлевна Хаджи — научный сотрудник Института международной экономики и финансов, Всероссийская академия внешней торговли (РФ, 119285, Москва, Воробьевское ш., 6А); Российский центр исследований АТЭС, РАНХиГС (РФ, 119034, Москва, Пречистенская наб., 11).
E-mail: k.khadzhi@vavt.ru

Аннотация

Регулирование трансграничных потоков данных и защиты конфиденциальности информации играет значимую роль в международных переговорах по развитию цифровой экономики в связи с беспрецедентным ростом объемов и темпов сбора, обработки, хранения и передачи данных. Несмотря на высокую актуальность темы и серьезное влияние регулирования этой сферы деятельности на все предприятия, относящиеся к цифровой экономике, в России проведено не так много исследований, в которых систематизируется информация о подходах, применяемых различными странами. В статье приводится обзор существующих подходов к национальному регулированию защиты, передачи (в том числе трансграничной) и хранения данных; проведен анализ влияния выбранных подходов к регулированию на международные торговые потоки; выработаны предложения по возможным мерам, способствующим снижению издержек компаний в цифровую эпоху. Сегодня большинство стран занимается регулированием потоков персональных и других категорий «чувствительных» данных посредством либо принятия отдельного закона, либо внесения соответствующих положений в секторальные законы. Подходы к регулированию трансграничной передачи данных варьируются от полного запрета на передачу всех или определенных типов персональных данных за рубеж до полной либерализации законодательства в этой сфере. Наиболее распространено применение одного или нескольких требований в отношении передачи данных за пределы страны: например, локализация данных, ограничение числа стран, в которые можно свободно передавать «чувствительные» данные без дополнительных условий, получение согласия субъекта персональных данных и/или разрешения ответственных государственных органов. Результаты исследования могут быть использованы ФОИВ для разработки государственной политики в области регулирования трансграничных потоков данных и обеспечения защиты конфиденциальности информации, в том числе с учетом опыта и лучших практик других государств, а также для выработки российской позиции для участия в мероприятиях различных международных площадок.

Ключевые слова: персональные данные, «чувствительные» данные, защита данных, трансграничная передача данных, локализация данных, электронная коммерция.
JEL: F02, K24.

Введение

Цифровизация влечет за собой беспрецедентный рост объемов и темпов сбора, обработки, хранения и передачи данных (в том числе при взаимодействии на международном уровне) за счет повсеместного внедрения цифровых технологий и оптимизации процессов на всех этапах. Сегодня практически каждая компания (независимо от сферы деятельности) сталкивается с необходимостью сбора, обработки, хранения и передачи данных. Значимость передачи (в том числе трансграничной) данных в последние годы заметно возросла — в особенности это касается международной торговли и взаимодействия в рамках глобальных цепочек поставок.

Потребительская ценность товаров и услуг со временем существенно трансформировалась. Раньше она основывалась на функциональности продукта и была результатом повышения производительности труда. Теперь всё большую ценность приобретают эффективные логистические и цифровые решения, включенные в продукт[1]. Практически все виды трансграничных транзакций сегодня имеют цифровую составляющую, которая обеспечивается за счет онлайн-платформ для предоставления связи компаний и клиентов в любой точке мира, осуществления заказов, оплаты и отслеживания передвижения товаров, в том числе с использованием различных электронных кодов.

Около 12% глобальной торговли товарами уже приходится на долю электронной коммерции[2]. И если раньше она была представлена в основном такими виртуальными товарами, как электронные книги, приложения, онлайн-игры, музыкальные файлы MP3, потоковые сервисы, программное обеспечение и услуги облачных вычислений, то 3D-печать со временем может привести к включению в сферу электронной коммерции новых категорий товаров. Потоки данных позволяют осуществлять экспорт услуг в цифровом формате, а также обеспечивают новые возможности для передвижения людей и прямых иностранных инвестиций за счет платформ для осуществления коммуникаций и цифровых транзакций.

За последнее десятилетие потоки данных увеличили мировой ВВП по меньшей мере на 10%. В ценовом отношении это составило 7,8 трлн долл. только в 2014 году[3]. Международная торговая

---

[1] No Transfer, No Production — A Report on Cross-Border Data Transfers, Global Value Chains, and the Production of Goods. The National Board of Trade. 2015. https://unctad.org/meetings/en/Contribution/dtl_ict4d2016c02_Kommerskollegium_en.pdf.

[2] McKinsey Global Institute. Digital Globalization: The New Era of Global Flows. 2016. February. https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows.

[3] Ibid.

палата (ICC) сообщает, что развитие Интернета и увеличение потоков данных способствовало ускорению роста ВВП большинства стран, в том числе и развивающихся, на 15–20%[4].

С 2005 года по 2018-й количество абонентов фиксированного широкополосного Интернета в мире увеличилось в пять раз, превысив отметку в 1 млрд чел. В то же время в период с 2007 года по 2018-й число пользователей мобильного Интернета в мире (показатель рассчитывается как количество абонентов на 100 чел.) увеличилось с 4 до 69,3. Таким образом, аудитория мобильного Интернета увеличилась с 268 млн чел. в 2007 году до 5,3 млрд в 2018-м, показав рост почти в двадцать раз. При этом потенциал роста не исчерпан.

Пропускная способность трансграничных каналов передачи данных увеличилась примерно в сорок пять раз с 2005 года по 2015-й[5], а в период с 2015-го по 2019-й она выросла еще в три раза (с 153 282 Кбит/сек. до 485 662 Кбит/сек.)[6].

Быстрыми темпами растут и объемы потребляемого трафика. Так, объем потребляемого фиксированного широкополосного интернет-трафика вырос с 502 до 833 эксабайтов в период с 2015 года по 2017-й, а объем мобильного интернет-трафика увеличился за этот же период больше чем в три раза, достигнув значения в 130 эксабайт в 2017 году. Основной объем потребляемого трафика приходится на страны Азиатско-Тихоокеанского региона: в 2017 году более 60 эксабайт мобильного интернет-трафика (рост в два раза по сравнению с 2016-м) и почти 350 эксабайт фиксированного широкополосного интернет-трафика. Именно в этом регионе наиболее активно ведется дискуссия о необходимости определить правила обращения с данными (в том числе персональными).

Интерес к вопросам регулирования потоков данных всё больше растет в развивающихся странах. Одна из возможных причин — значительный рост потребления интернет-трафика в данной группе государств, где его объем превышает показатели развитых стран. Этим может быть обусловлена и заинтересованность компаний в выходе на развивающиеся рынки. Если в 2015 году на развитые и развивающиеся страны приходились примерно равные доли потребляемого интернет-трафика, то в уже в 2017 году доля последних выросла почти в два раза.

---

[4] International Chamber of Commerce (ICC). Trade in the Digital Economy: A Primer on Global Data Flows for Policymakers. 2016. https://iccwbo.org/content/uploads/sites/3/2016/09/Trade-in-the-digital-economy-A-primer-on-global-data-flows-for-policymakers.pdf.

[5] McKinsey Global Institute…

[6] International Telecommunications Union (ITU). Key ICT Indicators for Developed and Developing Countries and the World (Totals and Penetration Rates). 2019. https://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2019/ITU_Key_2005-2019_ICT_data_with%20LDCs_28Oct2019_Final.xls.

В странах Содружества независимых государств потребляют относительно небольшой объем интернет-трафика: в 2017 году менее 50 эксабайт фиксированного широкополосного интернет-трафика (около 6% от общемирового показателя) и менее 10 эксабайт мобильного интернет-трафика (менее 8% от общемирового показателя)[7]. Однако потенциал роста рынка реализован не полностью.

Данные занимают всё более значимую роль в вопросах государственного управления. Во многих странах мира происходит формирование «открытого» цифрового правительства путем увеличения количества и видов государственных услуг, предоставляемых в электронной и мобильной форме, а также развития национальной инфраструктуры пространственных данных.

Всё острее встает вопрос права владения данными, поскольку доступ к ним расширяется не только у государства, но и у крупных национальных и иностранных (в том числе трансграничных) компаний. Так, согласно исследованию экспертов Оксфордского университета, проведенному на основе данных 1 млн мобильных приложений, скачанных в интернет-магазинах Google Play в США и Великобритании, 88% мобильных приложений передавали данные пользователей компаниям, связанным с *Alphabet*, около 43% — компании *Facebook*, 34% — *Twitter*, 26% — *Verizon*, 23% — *Microsoft* и 18% — *Amazon*. При этом около 100 тыс. приложений передавали данные более чем в одну юрисдикцию [Binns et al., 2018].

Стоит отметить, что часто передаваемые в приложениях персональные данные носят конфиденциальный характер (например, это могут быть данные о физической активности, сердечном ритме или женском здоровье), и пользователи рассчитывают на их конфиденциальность[8].

В результате технологического развития цифровые компании получают доступ к колоссальным ресурсам, подчас превышающим ресурсы отдельных государств. Так, выручка пяти крупнейших цифровых компаний мира (*Google, Amazon, Facebook, Apple* и *Microsoft*) в 2018 году составила 802 млрд долл., что превышает, например, общий ВВП Саудовской Аравии (684 млрд долл.), а их общая стоимость (3,5 трлн долл.) уступает только ВВП каждой из четырех лидирующих по этому показателю стран мира (США, Китая, Японии и Германии). При этом численность потребителей услуг этих компаний значительно превышает население самых крупных стран. Так, например, аудитория *Facebook* насчитывала 2,4 млрд пользователей в 2018 году. Такое положение позволяет цифровым корпора-

[7] International Telecommunications Union (ITU). Measuring the Information Society Report. Vol. 1. 2018. https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2018/MISR-2018-Vol-1-E.pdf.

[8] *Делюкин Е.* WSJ: 11 популярных приложений отправляли в Facebook медицинские, финансовые и другие личные данные пользователей // Vc.ru. 2019. 27 февраля. https://vc.ru/services/59617-wsj-11-populyarnyh-prilozheniy-otpravlyali-v-facebook-medicinskie-finansovye-i-drugie-lichnye-dannye-polzovateley.

циям укреплять естественную монополию и оказывать влияние на общественное мнение в интересах тех или иных социальных, экономических или политических групп[9]. Правительства разных стран задаются вопросом о взаимосвязи сбора данных компаниями и их доминирующего положения на рынке. Так, в 2019 году антимонопольными органами ЕС было инициировано расследование о практиках сбора данных компанией *Google*[10].

Вопросы регулирования трансграничных потоков данных и обеспечения защиты конфиденциальности играют значимую роль в международной цифровой повестке и привлекают особое внимание в связи с увеличением случаев утечки персональных и других категорий «чувствительных» данных, а также различных видов киберпреступлений и/или использования данных в социальной инженерии[11]. *InfoWatch* сообщает, что за первое полугодие 2019 года в мире произошло 1276 случаев утечки данных (на 22% больше аналогичного показателя 2018 года). Среднее число утерянных записей за один случай — 6,85 млн. Общее количество скомпрометированных данных достигло 8,74 млрд (в 3,6 раза больше по сравнению с аналогичным периодом 2018 года). 97% данных были скомпрометированы в результате мегаутечек. Из-за них теряется по меньшей мере 10 млн записей за один раз. Всего за первое полугодие 2019-го произошла 41 мегаутечка данных, что превышает аналогичный показатель за первое полугодие 2018-го (21 случай) почти в два раза[12].

Главной задачей повышения эффективности действующего национального регулирования в области защиты данных и конфиденциальности информации является сохранение баланса интересов потребителей (гражданского общества), бизнеса и органов власти для обеспечения достаточного уровня безопасности и конкуренции при одновременном снижении излишних ограничений для коммерческой деятельности.

Основная часть проведенных исследований в России касается анализа национального законодательства в данной сфере, например [Проскурякова, 2016], в том числе в контексте регулирования персональных данных в различных секторах [Журавлев, 2016; Лопаткина, Муслов, 2015], а также в сравнении с некоторыми другими странами [Евсеева и др., 2016; Емуранова, 2016], или анализа подходов США и ЕС к регулированию этого вопроса в контексте

---

[9] *Жданов С.* Эпоха цифровых государств: как Facebook, Google и Amazon выигрывают войну с правительством США // Нож. 2019. 28 мая. https://knife.media/corporations-vs-state/.

[10] *Chee F. Y.* Exclusive: EU Antitrust Regulators Say They Are Investigating Google's Data Collection // Reuters. 2019. December 1. https://www.reuters.com/article/us-eu-alphabet-antitrust-exclusive/exclusive-eu-antitrust-regulators-say-they-are-investigating-googles-data-collection-idUSKBN1Y40NX.

[11] Социальная инженерия — это метод несанкционированного доступа к информации или системам хранения данных без использования технических средств.

[12] InfoWatch. Глобальное исследование утечек конфиденциальной информации в первом полугодии 2019 года. https://www.infowatch.ru/resources/analytics/reports/17376.

обеспечения свободы слова и прав человека в онлайн-среде [Бирюков, 2015; Determann, 2019]. Примечательно, что в большей части работ предметом исследований является соблюдение права на конфиденциальность в интернете с позиции защиты основных прав и свобод человека, в том числе права на неприкосновенность частной жизни и свободы слова, при соблюдении надлежащего уровня безопасности.

Предметом исследования настоящей статьи являются подходы разных государств к регулированию потоков данных и возможное влияние такого регулирования на порядок ведения бизнеса в той или иной стране. Представлен их сравнительный анализ и даны рекомендации относительно возможных мер по снижению издержек компаний в цифровую эпоху. Необходимо отметить, что повестка международных организаций в области регулирования трансграничной передачи данных является предметом отдельного рассмотрения; в связи с широким кругом включенных в нее задач и вопросов она не будет анализироваться в статье.

1. Национальное регулирование защиты данных

Национальное регулирование защиты данных является одним из ключевых элементов обеспечения информационной безопасности как составной части национальной безопасности. Основные вопросы регулирования касаются того, кто будет владеть данными (персональными, государственными и корпоративными) и как обеспечить их безопасный сбор, хранение, обработку и удаление, сохранив необходимую степень конфиденциальности, а также возможность их использования для дальнейшей оптимизации всех процессов[13]. Наибольшее внимание на этом этапе привлекает защита персональных данных различных категорий, современные правовые основы которой будут рассмотрены в разделе.

ЮНКТАД выделил восемь основных принципов защиты персональных данных, характерных для всех стран.

1. Открытость: организации должны предоставлять открытый доступ к информации, имеющей отношение к политике сбора и использования персональных данных.
2. Ограничения сбора: сбор персональных данных должен быть ограниченным, законным и справедливым, осуществляться с оповещением и/или с согласия субъекта персональных данных.

[13] The United Nations Conference on Trade and Development (UNCTAD). Policy Brief: Making Digital Platforms Work for Development. No 73. 2019. March. https://unctad.org/en/PublicationsLibrary/presspb2019d2_en.pdf.

3. Указание цели: цели сбора и разглашения персональных данных должны быть четко обозначены в момент их сбора.
4. Ограничения использования: использование или раскрытие персональных данных должно быть ограничено либо тесно связано с конкретными целями.
5. Безопасность: персональные данные должны быть обеспечены надлежащей степенью защиты.
6. Качество данных: персональные данные должны быть актуальными, точными и вовремя обновляться.
7. Доступ и возможность корректировки: субъекты персональных данных должны иметь достаточно прав для получения доступа к своим персональным данным и внесения изменений в них.
8. Ответственность: операторы обработки персональных данных обязаны соблюдать принципы защиты данных[14].

Механизмы обработки персональных и других типов данных должны одновременно обеспечивать их защиту и способствовать техническому прогрессу и инновациям (посредством предоставления легитимного доступа к данным для развития таких технологий, как большие данные, искусственный интеллект, интернет вещей, робототехника, электроника с открытым исходным кодом, облачные технологии и др.). Например, ОЭСР приняла рекомендации Совета по искусственному интеллекту[15], которые затем легли в основу текста приложения к заявлению министров торговли и цифровой экономики Группы двадцати от 8–9 июня 2019 года[16]. В рекомендациях отмечена необходимость создания открытых баз данных (с привлечением государственных и частных инвестиций) и фондов данных для развития искусственного интеллекта при условии обеспечения защиты персональных данных и требований информационной (цифровой) безопасности, с тем чтобы новые технологии не навредили человеку и не создавали угроз его безопасности.

В 1990-х годах в мире насчитывалось лишь около двадцати стран, регулирующих потоки персональных данных в рамках национального законодательства, однако уже к 2015 году их количество превысило сто. И это число растет из года в год [Durou, 2015].

На сегодня большинство стран занимается регулированием потоков персональных и других категорий «чувствительных» данных. Регулирование может осуществляться тремя способами (рис. 1).

---

[14] The United Nations Conference on Trade and Development (UNCTAD). Data Protection Regulations and International Data Flows: Implications for Trade and Development. 2016. https://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf.

[15] Organization for Economic Co-operation and Development (OECD). Recommendation of the Council on Artificial Intelligence. https://tuac.org/wp-content/uploads/2019/05/OECD_AI-Recommendation.pdf.

[16] G20 Ministerial Statement on Trade and Digital Economy. 2019. https://www.ranepa.ru/images/News_ciir/Project/Ministerial_Statement_on_Trade_and_Digital_Economy.pdf.

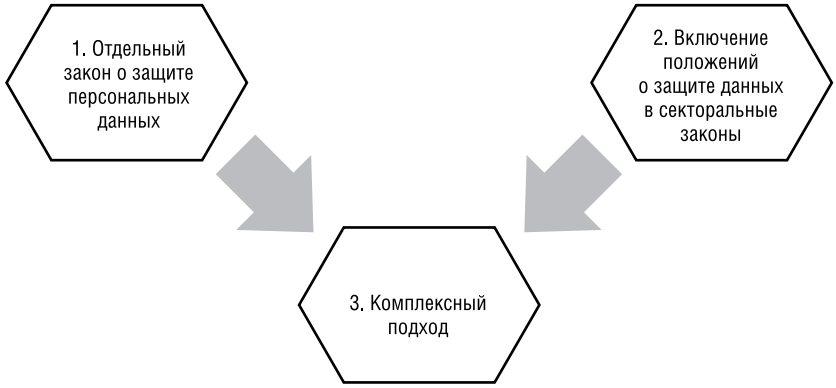


Рис. 1. **Подходы стран к регулированию защиты данных**

Рассмотрим каждый из существующих подходов к регулированию защиты данных на национальном уровне.

1. *Принятие отдельного закона о защите персональных данных*. Практика характерна для Европейского союза, который является примером для многих стран. В ЕС действует «Общий регламент защиты персональных данных» (GDPR), но при этом вопросы локализации данных остаются в компетенции национального регулирования каждой страны союза.

Отдельный закон о защите персональных данных действует и в других странах, например в России, Азербайджане, Армении, Израиле, Казахстане, Киргизии, Малайзии, Мексике, Молдавии, Сингапуре, Турции, Узбекистане, Украине, Южной Корее и Японии.

2. *Внесение положений о защите персональных данных в соответствующие секторальные законы*, например в законы об информационной безопасности, телекоммуникациях, электронной коммерции. При этом отдельный закон о защите персональных данных не принимается.

Единый секторальный подход на всей территории страны действует, например, в Брунее-Даруссаламе, Вьетнаме, Индонезии[17], Иране, Нигерии и Чили. В Бразилии в настоящее время применяется секторальный подход, однако с 15 августа 2020 года начнет действовать «Общий закон о защите данных» (LGPD) — аналог GDPR, утвержденный президентом Бразилии в июле 2019 года.

В некоторых странах, придерживающихся секторального подхода, требования по защите данных различаются в зависимости от территориальной единицы (штата, региона, эмирата и др. — с учетом особенностей административно-территориального устройства государства). Так, положения по защите персональных данных, включенные в секторальные законы, различаются, например, в Ин-

[17] Обсуждается возможность принятия единого закона о защите персональных данных.

дии[17] (по штатам), Китае (особое законодательство действует в Гонконге и на Тайване), Объединенных Арабских Эмиратах (отдельное законодательство применяется в свободных экономических зонах).

В США (при отсутствии соответствующего федерального закона)[17] защита данных обеспечивается следующими регулирующими документами:

- федеральным законом «О неприкосновенности частной жизни»;
- отдельными законами штатов (так, только в Калифорнии принято более двадцати пяти законов в этой области);
- секторальными законами (например, о финансовой и медицинской информации);
- отдельными руководствами для бизнеса (например, «Рекомендациями для бизнеса и регуляторов о защите персональных данных потребителей в эпоху быстрых изменений» Комиссии США по торговле).

3. *Комплексный подход* предполагает, что принимается отдельный закон о защите персональных данных, а также вносятся соответствующие изменения в секторальные законы.

Примерами стран, использующих такой подход, являются Австралия и Канада. Так, в Канаде помимо всеобщего закона о защите конфиденциальности данных и электронных документах (PIPEDA) в провинциях Альберта, Британская Колумбия и Квебек действует отдельное регулирование, связанное с защитой данных и содержащее дополнительные требования к операторам данных.

При этом передача отдельных видов данных (финансовой, медицинской и бухгалтерской информации, а также корпоративных данных), как правило, регулируется отдельными секторальными нормативно-правовыми актами независимо от указанного подхода страны к регулированию вопросов защиты данных.

2. Национальное регулирование трансграничной передачи данных

По данным ОЭСР, с 2012 года количество изобретений, запатентованных пятью экономиками — мировыми лидерами по интеллектуальной собственности в сфере передачи данных (Китаем, Китайским Тайбэем, США, Южной Кореей и Японией), в среднем росло на 19% в год. Сбор и передача данных служат источником создания стоимости: данные используются не только непосредственно для предоставления пользователям товаров и услуг (в том

числе посредством интернет-торговли), но также для аналитики и создания новых предложений для потребителей[18].

Национальное регулирование трансграничной передачи персональных и других категорий «чувствительных» данных обусловлено необходимостью защиты их конфиденциальности и обеспечения информационной безопасности. Как и в случае с указанными механизмами защиты данных, барьеры, связанные с ограничением свободного трансграничного перемещения потоков данных, увеличивают время и расходы компаний на осуществление внешнеэкономической деятельности (экспорта и импорта услуг) и могут создавать дополнительные сложности для развития новых видов предпринимательства, основанных на использовании больших массивов данных [Ferracane, Marel, 2018]. Согласно «Индексу ограничений для торговли услугами в секторе телекоммуникаций» ОЭСР, 38 стран применяют более строгое законодательство в области передачи персональных данных по сравнению с «Рекомендациями ОЭСР по защите конфиденциальности и трансграничным потокам персональных данных»[19].

Регулирование трансграничной передачи данных в рамках национального законодательства предполагает один из трех подходов (рис. 2), при этом для разных категорий данных могут применяться разные требования и подходы.

Рассмотрим более подробно каждый из существующих подходов к регулированию трансграничной передачи данных на национальном уровне.

1. Полный запрет на передачу данных за пределы страны

Этот подход 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[20]. В Индонезии существует запрет на передачу данных, связанных с предоставлением населению услуг (к примеру, финансовых), в том числе частными фирмами[21]. В Китае запрещена передача за пределы страны (в том

---

[18] Organization for Economic Co-operation and Development (OECD). Measuring the Digital Transformation: A Roadmap for the Future. https://www.oecd-ilibrary.org/docserver/9789264311992-en.pdf?expires=1589353357&id=id&accname=guest&checksum=29F82DA4A5517C3DD1E626E53BE80515.

[19] Organization for Economic Co-operation and Development (OECD). STRI Sector Brief: Telecommunications. 2018. https://www.oecd.org/trade/topics/services-trade/documents/oecd-stri-sector-note-telecommunications.pdf.

[20] *Tymburski K., Balouziyeh J., Kirkham K. M.* Saudi Arabia: New Cloud Computing Regulatory Framework // Mondaq. 2018. April 5. http://www.mondaq.com/saudiarabia/x/689306/new+technology/Saudi+Arabia+new+Cloud+Computing+Regulatory+Framework.

[21] Министерство коммуникаций и информатики Республики Индонезия. Закон об информации и электронных трансакциях от 21.04.2008 № 11. https://jdih.kominfo.go.id/produk_hukum/view/id/167/t/undangundang+nomor+11+tahun+2008+tanggal+21+april++2008.

Рис. 2. **Подходы стран к регулированию трансграничной передачи данных**

числе оффшорным компаниям) любых персональных финансовых[22] и медицинских данных[23]. При этом другие типы персональных данных могут передаваться за границу при соблюдении необходимых требований.

2. Передача данных разрешена во все страны без необходимости соблюдения каких-либо дополнительных законодательных ограничений (барьеры отсутствуют на национальном уровне)

Полная либерализация законодательства по передаче данных, как и полный запрет на передачу данных встречаются редко. Так, никаких ограничений в отношении трансграничной передачи персональных данных в любую другую юрисдикцию пока не существует в Боливии, Зимбабве, Мозамбике, Намибии и на Филиппинах[24].

Интересен пример США, где согласно национальному регулированию трансграничное перемещение данных может осуществляться свободно во все страны без необходимости получения какого-либо разрешения органов власти либо согласия субъекта. В то же время в США существуют требования по локализации отдельных видов данных[25]. Например, согласно «Руководству по безопасности налоговой информации для федеральных служб,

---

[22] Notice by the People's Bank of China Regarding the Effective Protection of Personal Financial Information by Banking Institutions. http://www.lawinfochina.com/display.aspx?lib=law&id=8837&CGid=.

[23] Interpretation on Population Health Information Management Measures (Trial Implementation). https://www.chinadaily.com.cn/m/chinahealth/2014-06/15/content_17588400.htm.

[24] Data Protection Laws of the World. https://www.dlapiperdataprotection.com/index.html?t=transfer&c=AO.

[25] См. подробнее: *Cory N.* Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost? // Information Technology & Innovation Foundation. 2017. May. https://www.researchgate.net/publication/333292633_Cross-Border_Data_Flows_Where_Are_the_Barriers_and_What_Do_They_Cost.

а также служб штатов и административных единиц» № 1075 информационные системы, задействованные в получении, обработке, хранении или передаче федеральных налоговых данных, обязаны располагаться на территории США, а также посольств США или военных баз США[26]. Следует подчеркнуть, что отсутствие дополнительных требований к обеспечению защиты персональных данных при их трансграничной передаче не означает отсутствия общих требований к защите персональных данных (подход США к регулированию защиты персональных данных был представлен в разделе 1). В случае нарушения общих требований законодательства к обеспечению хранения данных или в случае их неправомерного использования компании привлекаются к ответственности, например на них налагаются внушительные штрафы, являющиеся на практике одними из самых крупных штрафов в мире (рис. 3). Таким образом, США используют принцип ex-post регулирования трансграничной передачи данных, в то время как абсолютное большинство стран придерживаются подхода ex-ante.

3. Трансграничная передача данных возможна при соблюдении определенных законодательных требований

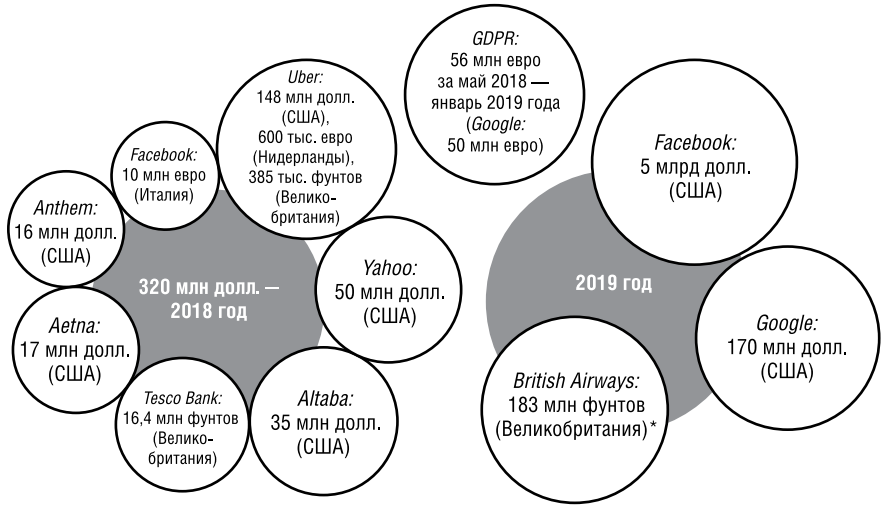
Подход, предполагающий существование определенных законодательных требований к передаче данных, является наиболее распространенным в мире. При этом указанные ниже ограничения могут применяться странами как по отдельности, так и комплексно (сочетая две-три различные меры).

Приведем примеры существующих ограничений на трансграничную передачу данных.

- *Необходимость получения разрешения ответственных органов власти.* Например, в Испании трансграничная передача данных, подпадающих под действие типовых контрактов или обязательных корпоративных правил, возможна лишь после получения соответствующего разрешения директора Испанского управления по защите данных[27].
- *Необходимость получения согласия субъекта персональных данных.* Согласие субъекта персональных данных для их трансграничной передачи требуется во многих странах, например в Брунее-Даруссаламе, Индии, Коста-Рике, Румынии, Сингапуре, Чили, Южной Корее и Японии. В Индонезии передавать персональные данные пользователей электронных систем можно лишь с письменного разрешения субъекта персональных данных. В Малайзии согласие субъекта

[26] Publication 1075: Tax Information Security Guidelines for Federal, State and Local Agencies, Safeguards for Protecting Federal Tax Returns and Return Information. 2016. https://www.irs.gov/pub/irs-pdf/p1075.pdf.

[27] *Burgos C., Pehlivan C.* Data Protected—Spain. 2018. https://www.linklaters.com/en/insights/data-protected/data-protected---spain.



* Итоговое решение в отношении British Airways пока не принято. См.: Information Commissioner's Office (ICO). Intention to Fine British Airways £183.39m Under GDPR for Data Breach. 2019. July 8. https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/.

Источники: European Data Protection Board. First Overview on the Implementation of the GDPR and the Roles and Means of the National Supervisory Authorities. https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2019/02-25/9_EDPB_report_EN.pdf; Federal Trade Commission. Stipulated Order for Civil Penalty, Monetary Judgment, and Injunctive Relief. https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_order_filed_7-24-19.pdf; *Corfield G.* UK Data Watchdog Kicks £280m British Airways and Marriott GDPR Fines into Legal Long Grass. https://www.theregister.com/2020/01/13/ico_british_airways_marriott_fines_delayed/; Federal Trade Commission. Stipulated Order for Permanent Injunction and Civil Penalty Judgment. https://www.ftc.gov/system/files/documents/cases/172_3083_youtube_coppa_consent_order.pdf; InfoWatch. Штрафы за утечки данных: мировая картина. https://www.infowatch.ru/sites/default/files/report/analytics/russ/infowatch_fines_leak_2018.pdf?rel=1.

Рис. 3. **Наиболее крупные штрафы за утечки данных, 2018–2019 годы, и общая сумма штрафов за нарушение GDPR, 2018 год**

персональных данных является достаточным условием для получения возможности их трансграничной передачи наряду с другими дополнительными условиями[28].

- *Передача персональных данных может осуществляться только в определенные страны.* Ограничения по количеству стран, в которые разрешена трансграничная передача данных, также варьируются в различных юрисдикциях.

  К примеру, законодательство Китайского Тайбэя разрешает передачу персональных данных во все страны, кроме территории материкового Китая[29]. В отдельных странах (например, в Аргентине, Пакистане, России, Турции, Чили, а также в ЕС)

[28] Laws of Malaysia. Personal Data Protection Act 2010. No 709. 2016. https://www.kkmm.gov.my/pdf/Personal%20Data%20Protection%20Act%202010.pdf.

[29] *Chen C., Fahey M. R.* Data Protection in Taiwan: Overview. 2018. https://uk.practicallaw.thomsonreuters.com/5-578-3485?__lrTS=20190902135743837&transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1.

передавать данные можно лишь в определенные государства согласно соответствующему законодательно закрепленному перечню. Так, ЕС признает тринадцать стран и территорий, где обеспечивается уровень защиты данных, аналогичный европейскому: Андорра, Аргентина, Израиль, Канада (только коммерческие организации), коронные земли — острова Гернси, Джерси и Мэн, Новая Зеландия, США (только для участников программы сертификации EU—US Privacy Shield), Уругвай, Фарерские острова, Швейцария и Япония. Ведутся переговоры по включению в этот перечень Южной Кореи[30].

Согласно регулированию других экономик, передача данных разрешена в любую страну, обеспечившую эквивалентный уровень защиты. Таким образом, список государств официально не закреплен и выбор страны, куда будет осуществляться трансграничная передача данных, определяется тем, гарантирует ли она адекватный уровень защиты данных. Такой подход применяют, например, Австралия, Бруней-Даруссалам, Израиль, Индия, Канада, Китайский Тайбэй, Колумбия, Малайзия, Мексика, Новая Зеландия, Перу, Сингапур, ЮАР и Япония.

Национальное законодательство в отдельных случаях также предусматривает альтернативные меры защиты данных при их трансграничной передаче. Так, в некоторых странах возможна передача данных и в страны, не обеспечивающие уровень защиты, аналогичный национальному (в обход соответствующего требования). Например, в России, Австралии, Аргентине, Израиле, Колумбии, Малайзии, Мексике, Перу, Турции, а также странах ЕС для этого необходимо получить разрешение субъекта персональных данных. В ЮАР в таком случае помимо согласия субъекта требуется специальное разрешение регулирующих органов[31].

- *Дополнительные требования по локализации*[32]. Приведенный выше пример полного запрета на передачу данных в другие страны, применяемый отдельными странами, фактически представляет собой пример безусловной локализации. Подобное ограничение влечет за собой значительные издержки для бизнеса, осуществляющего внешнеэкономическую деятельность, особенно обременительные для малого бизнеса.

[30] Adequacy Decisions. How the EU Determines if a Non-EU Country Has an Adequate Level of Data Protection. 2019. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

[31] Government Gazette. Act No 4 of 2013: Protection of Personal Information Act, 2013. https://www.justice.gov.za/legislation/acts/2013-004.pdf.

[32] Локализация представляет собой законодательное требование по хранению данных, передаваемых в электронном или другом виде, на территории страны.

Издержки связаны с ограничением выбора поставщиков, иногда более конкурентных по цене и/или качеству услуг хранения данных, в других странах и дополнительными расходами на организацию хранения копий данных в стране.

При этом локализация может и не препятствовать трансграничной передаче данных при условии соблюдения законодательного требования о хранении копии данных на территории страны и других требований по передаче данных. К примеру, согласно российскому законодательству персональные данные граждан можно передавать за рубеж при соблюдении условий их трансграничной передачи, при этом необходимость хранения данных на территории России является отдельным требованием ко всем операторам данных независимо от наличия или отсутствия необходимости их трансграничной передачи. Таким образом, указанные требования являются независимыми друг от друга[33].

Кроме того, локализация не всегда представляет собой законодательное требование о хранении копии данных на территории страны. Так, например, в Малайзии нет открытого требования по локализации персональных данных, однако необходимо получить разрешение правительственных органов на трансграничную передачу персональных данных граждан, и, соответственно, некоторые исследователи рассматривают этот пример как фактическую локализацию данных[34].

3. Национальное регулирование локализации данных

На международных площадках ведутся активные дискуссии о целесообразности локализации отдельных категорий данных, а также других мер регулирования трансграничных потоков данных в контексте возможных ограничений для бизнеса в цифровую эпоху. ОЭСР[35] и Европейский центр международной политической экономии (ECIPE)[36] относят локализацию к барьерам для цифровой торговли.

США и Япония выступали на площадке ВТО с предложением о введении запрета требований локализации на многостороннем уровне. Они полагают, что подобные ограничения препятствуют быстрому и эффективному развитию цифровой экономики и цифровой торговли.

---

[33] Обработка и хранение персональных данных в РФ. Изменения с 1 сентября 2015 года. https://digital.gov.ru/ru/personaldata/.

[34] *Cory N.* Cross-Border Data Flows…

[35] Organization for Economic Co-operation and Development (OECD). Digital Services Trade Restrictiveness Index Regulatory Database.

[36] The European Centre for International Political Economy (ECIPE). Digital Trade Estimates Report 2018. https://ecipe.org/dte/dte-report/.

Потенциальный протекционистский характер локализационных мер связан с тем, что они могут приводить к перераспределению торговли в некоторых сферах в пользу национальных компаний. В частности, расчеты показывают, что существует положительная корреляция между требованиями по локализации данных и уровнем нетарифных барьеров в некоторых секторах услуг[37].

Согласно исследованию ECIPE, число локализационных ограничений, применяемых различными странами мира, значительно выросло за последнее время: в 2000 году их было 19, а в 2016-м стало уже 84 (в 64 странах). Среди стран, не применяющих требования по локализации, Австрия, Венгрия, Израиль, Ирландия, Исландия, Испания, Италия, Коста-Рика, Латвия, Литва, Норвегия, Португалия, Словакия, Словения, Чехия, Чили, Швейцария, Эстония и ЮАР.

Локализационные ограничения применяются к различным категориям данных (рис. 4).

Наиболее широкий массив информации, подпадающий под локализацию, — персональные данные граждан, включающие информацию, собранную как государственными органами страны, так и частным сектором. Локализационные требования по хранению операторами копий всех персональных данных на серверах внутри страны применяются, например, в России, Казахстане и Вьетнаме.

Личные данные граждан, обрабатываемые (отдельными либо всеми) государственными органами, учебными заведениями, государственными банками, больницами и другими государственными институтами (в том числе в рамках предоставления госуслуг), подлежат локализационным ограничениям в Германии, Индии, в отдельных провинциях Канады, Китайском Тайбэе, Нидерландах, Сингапуре, в отдельных штатах США и в Швеции. Данные, собранные в национальном реестре физических лиц Бельгии, должны храниться только на территории страны.

Другие локализационные требования применяются к отдельным («чувствительным») данным и чаще всего касаются телекоммуникационного сектора, финансовых, медицинских данных либо деловой документации.

В Китае требования по локализации действуют в отношении достаточно большого объема данных — персональной и другой информации, собираемой критически важными объектами информационной инфраструктуры и операторами сетей. Фактически к этой категории относятся данные, собранные госорганами и компаниями ключевых секторов (включая телекоммуникации,

---

[37] *Гущин Е., Исмагилова О., Кнобель А., Кудакаева К., Кутовая А., Латыпова Ю., Прока К., Пыжиков Н., Флегонтова Т.* Возможности и риски от снижения цифровых барьеров. Мониторинг актуальных событий в области международной торговли. 2019. № 33. 17 июля. https://www.vavt-imef.ru/wp-content/uploads/2019/07/Monitoring_33-1.pdf.

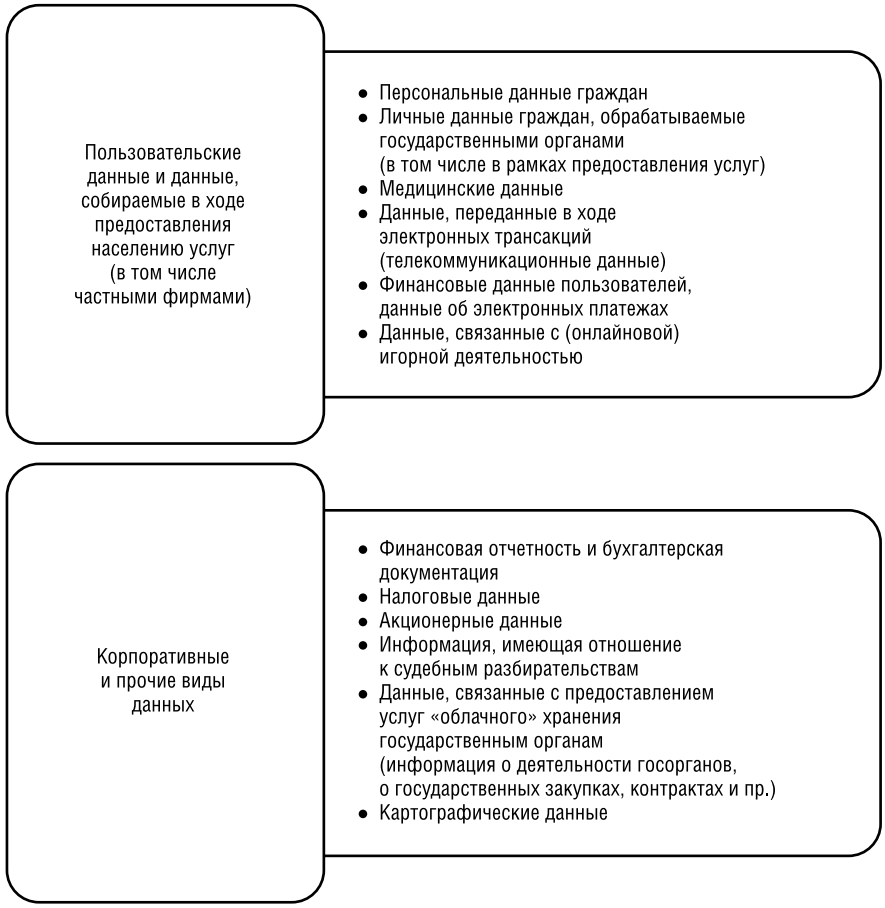


Рис. 4. **Типы данных, подпадающих под локализационные требования в различных странах**

энергетику, транспорт, систему ирригации и др.)[38]. Требования по локализации в Китае сочетаются с необходимостью получения разрешения на передачу данных в каждом конкретном случае после прохождения необходимых проверок в области безопасности (пример сочетания нескольких ограничений на трансграничную передачу данных). Проверка исходящей информации осуществляется в отношении рисков для безопасности национальной обороны и политической системы, экономики, науки и технологий[39].

Локализация медицинских данных применяется в Австралии, Великобритании и Дании.

---

[38] *Ning S., Wu H.* China: Data Protection 2019. https://iclg.com/practice-areas/data-protection-laws-and-regulations/china.

[39] Уведомление о публичном запросе информации Национального информационного бюро сети Интернет в отношении подхода к оценке безопасности при трансграничной передаче персональных и важных данных (проект запроса комментариев). 2017. https://www.chinalawtranslate.com/en/2016-cybersecurity-law/.

Во Вьетнаме все компании, предоставляющие интернет-услуги, должны иметь хотя бы один сервер с базами данных на территории страны. В случае наличия требований к серверной системе, расположенной во Вьетнаме, вся серверная система, расположенная за его пределами, должна отвечать этим требованиям[40].

В Иране все данные пользователей мессенджеров необходимо хранить на территории страны.

Локализация данных, переданных в ходе электронных транзакций, применяется в России, Бразилии, Германии, Казахстане, Мексике и Нигерии.

Локализация телекоммуникационных данных помимо требования о наличии серверов для хранения информации на территории страны (с тем чтобы была возможность предоставить ее компетентным органам по запросу и предотвратить неконтролируемую передачу персональных и других типов данных компетентным органам других стран) обычно сопровождается законодательно установленными сроками, в течение которых вся передаваемая информация (не только данные о пользователях, но и непосредственно данные, передаваемые пользователями) должна храниться операторами. В России такие сроки прописаны в так называемом законе Яровой. В других странах сроки, как правило, указаны в тексте основного закона о защите персональных или других типов данных или же в соответствующих подзаконных актах.

Согласно новому государственному регулированию электронных систем и транзакций в Индонезии центры обработки данных операторов электронных систем для государственного сектора должны находиться на территории страны[41].

В Бразилии, Дании, Нигерии, Франции, Швеции, Южной Корее и Японии все провайдеры облачных услуг, предоставляющие услуги хранения данных государственным учреждениям, должны иметь центры обработки данных, расположенные в пределах страны.

В России, Венесуэле, Индии, Индонезии и Турции существует требование по хранению и обработке на территории страны всех данных, связанных с электронными платежами.

Финансовые учреждения Бразилии и Люксембурга обязаны обрабатывать свои данные внутри страны. Шведским поставщикам финансовых услуг де-факто необходимо хранить всю свою документацию в пределах национальной юрисдикции для предоставления надзорным органам немедленного доступа к серверам.

---

[40] Аналитический обзор международного опыта по локализации баз данных, содержащих персональные данные граждан. 2018. https://pd.rkn.gov.ru/docs/Obzor_po_lokalizacii.docx.

[41] *Hutagalung F., Kriyasa M. I., Rajab G. V., Afiandari W.* Highlights in the New Government Regulation on Electronic Systems and Transactions. 2019. https://dentons.hprplawyers.com/en/insights/articles/2019/november/19/highlights-in-the-new-government-regulation-on-electronic-systems-and-transactions.

В Бразилии, Великобритании, Германии, Дании, Индии, Индонезии и Швеции финансовая (и другая годовая) отчетность и бухгалтерская документация компаний должны храниться на территории страны в течение определенного времени. Согласно закону о бухгалтерском учете Финляндии бухгалтерская отчетность должна храниться на территории страны либо в другой стране ЕС, если гарантируется доступ к данным в режиме реального времени. В Бельгии и Новой Зеландии налоговые данные компаний должны храниться в центрах обработки данных, физически расположенных на территории страны.

В Болгарии, Польше и Румынии все данные, связанные с предоставлением услуг на рынке азартных игр, включая данные о ставках, участниках и выплатах, должны храниться с использованием оборудования (серверов для хранения данных), расположенного на территории страны.

Южная Корея — единственная страна, которая внедрила требование по локализации картографических данных с целью ограничения доступа к коммерческим спутниковым изображениям высокого разрешения[42].

Требования по локализации данных применяются многими странами для обеспечения суверенитета (в том числе права определять, какие типы данных могут покидать пределы национальной юрисдикции), национальной безопасности, а также защиты частной жизни граждан. Помимо этого, некоторые авторы говорят о необходимости локализации в целях улучшения условий для национальных поставщиков на начальных этапах развития, находящихся априори в неравном положении по сравнению с крупными трансграничными компаниями[43].

В то же время сама по себе локализация не является гарантией обеспечения необходимого уровня защиты данных — он зависит от наличия в стране передовых технологий в области информационной безопасности. Кроме того, в случае с безусловной локализацией высок риск потери всех данных при возникновении какой-либо чрезвычайной ситуации (соответствующие условия определяются архитектурой хранения данных, существующей в стране).

Таким образом, несмотря на многочисленные дискуссии об обоснованности локализации, на практике она широко применяется в мире наряду с другими ограничениями по передаче данных за рубеж.

---

[42] Korea Law. Act on the Establishment, Management, etc. of Spatial Data. 2019. http://elaw.klri.re.kr/eng_service/lawView.do?hseq=32771&lang=ENG.

[43] The United Nations Conference on Trade and Development (UNCTAD). Trade and Development Report 2018: Power, Platforms and the Free Trade Delusion, 2018. https://unctad.org/en/PublicationsLibrary/tdr2018_en.pdf.

Кроме того, во многих странах существует обширный перечень исключений, обеспечивающих свободу передачи данных, таких как исполнение условий контракта, обязательства по международным соглашениям или обеспечение жизненно важных интересов субъекта персональных данных при невозможности получить его согласие, как, например, в России.

Заключение

Формирование требований к политике защиты и трансграничной передачи персональных и других категорий «чувствительных» данных может создавать компаниям сложности для торговли в цифровую эпоху. Эти сложности определяются следующими обстоятельствами:

- различиями в национальном регулировании стран мира, влекущими за собой (помимо расходов на исполнение законодательных норм) административные издержки, связанные с необходимостью поиска информации о существующих требованиях и отслеживания происходящих изменений;
- отсутствием регулирования защиты данных на территории некоторых стран или недостаточной степенью его проработанности, что создает повышенные риски утечки данных;
- непрозрачностью и разрозненностью нормативно-правовой базы отдельных стран (особенно в случае секторального подхода и региональных различий в регулировании защиты данных);
- высокой стоимостью сертификации компаний с целью подтверждения соответствия политики обработки персональных данных требованиям законодательства;
- высокой стоимостью мер по обеспечению соблюдения законодательства по защите данных (например, для выполнения требований GDPR, согласно расчетам *Ernst&Young*, 500 крупнейших компаний мира должны будут потратить 7,8 млрд долл.)[44];
- высокими штрафными санкциями в случае несоблюдения необходимых мер защиты данных и отсутствием досудебного порядка разрешения возникших разногласий и споров. Например, самый крупный штраф за утечку персональных данных в 2018 году, по данным СМИ, был выписан в США: *Uber* согласилась выплатить 148 млн долл. В общей сложно-

[44] *Kahn J., Bodoni S., Nicola S.* It'll Cost Billions for Companies to Comply with Europe's New Data Law // Bloomberg Businessweek. 2018. March 22. https://www.bloomberg.com/news/articles/2018-03-22/it-ll-cost-billions-for-companies-to-comply-with-europe-s-new-data-law.

сти, по данным мониторинга СМИ, в 2018 году компании во всем мире были оштрафованы на 320 млн долл. В основном штрафные санкции применяются к компаниям в Великобритании, Италии, Сингапуре, США и Франции[45]. Согласно отчетности Европейского совета по персональным данным (EDPB), за первые девять месяцев действия GDPR (май 2018 — январь 2019 года) в ЕС компании обязали выплатить штрафы на общую сумму около 56 млн евро (из них штраф в размере 50 млн евро был назначен к выплате *Google*)[46]. Крупнейшие штрафы в 2019 году побили рекорды 2018 года. Так, компания *Facebook* была оштрафована в США на рекордные 5 млрд долл., *Equifax* — на 275 млн долл.[47], не считая компенсации пострадавшим пользователям в размере до 425 млн долл.[48], а *Google* — на 170 млн долл.[49] В то же время *British Airways* грозит штраф в 183 млн фунтов стерлингов (рис. 3). Несоблюдение требований бразильского LGPD в будущем также может повлечь за собой значительные административные санкции, а именно штраф в размере 2% от валового объема продаж компании (или группы компаний) либо не более 50 млн реалов (около 12,9 млн долл.) за нарушение[50].

Согласно исследованию *IBM*, проведенному среди 507 компаний, столкнувшихся с последствиями утечки данных в 2018 году[51], средняя стоимость их расходов в результате утечек персональных данных по всему миру составила 3,92 млн долл. Показатели разнятся в зависимости от стран, в которых компании ведут свою деятельность. Самые высокие у США — 8,19 млн долл. Они включают расходы на мониторинг утечек, оповещение о произошедших утечках, меры по преодолению последствий (в том числе оплату штрафов и выплату компенсаций) и ущерб от потери клиентской базы.

---

[45] InfoWatch. Глобальное исследование утечек конфиденциальной информации в 2018 году. https://www.infowatch.ru/resources/analytics/reports/report2018.

[46] European Data Protection Board (EDPB). First Overview on the Implementation of the GDPR and the Roles and Means of the National Supervisory Authorities. https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2019/02-25/9_EDPB_report_EN.pdf.

[47] Federal Trade Commission (FTC). FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook. 2029. July 24. https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions.

[48] Federal Trade Commission (FTC). Equifax Data Breach Settlement. 2019. September. https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement.

[49] Federal Trade Commission (FTC). Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law. 2019. September 4. https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations.

[50] What Is the Brazil General Data Protection Law (LGPD)? 2018. July 20. https://www.onetrust.com/what-is-the-brazil-general-data-protection-law-lgpd.

[51] Опрос проводился в шестнадцати странах и региональных единицах: в Австралии, АСЕАН (Вьетнаме, Индонезии, Малайзии, Сингапуре, Таиланде и Филиппинах), на Ближнем Востоке (в ОАЭ и Саудовской Аравии), в Бразилии, Великобритании, Германии, Индии, Италии, Канаде, скандинавских странах, в США, Турции, Франции, ЮАР, Южной Корее и Японии.

Снижению издержек компаний на мировом рынке могли бы способствовать следующие меры.

- Формирование на международном уровне общих принципов защиты и трансграничной передачи данных в зависимости от их категории.
- Выработка единых мировых стандартов обеспечения защиты данных при их сборе, хранении, обработке, передаче и удалении, а также обеспечение надлежащего качества соответствующих услуг.
- Продвижение международных инициатив по гармонизации и взаимному признанию законодательства в области защиты персональных и других категорий данных (например, «Конвенция 108+» Совета Европы или двухсторонние и многосторонние соглашения о взаимном признании).
- Повышение транспарентности законодательства стран, обмен опытом и лучшими практиками в области защиты и трансграничной передачи данных.
- Координация действий стран для предотвращения утечки данных.
- Внедрение мер по снижению стоимости услуг по обеспечению защиты и хранения данных.

Литература

1. *Бирюков М. М.* Актуальные аспекты правовой защиты персональных данных в Европейском союзе, США и России // Московский журнал международного права. 2015. № 3. С. 197–208.
2. *Евсеева А. А., Калуцкий И. В., Спеваков А. Г.* Сравнительный анализ российского и китайского законодательства в области обработки и защиты персональных данных // Известия Юго-Западного государственного университета. Серия «Управление, вычислительная техника, информатика, медицинское приборостроение». 2016. Т. 20. № 3. С. 78–84.
3. *Емуранова О. А.* Сравнительный анализ правового регулирования защиты персональных данных граждан России и стран БРИКС // В мире науки и инноваций: сб. стат. Междунар. науч.-практ. конф. (25 декабря 2016 года, Пермь): в 8 ч. Ч. 8. Уфа: Аэтерна, 2016. С. 159–164.
4. *Журавлев М. С.* Защита персональных данных в телемедицине // Право. Журнал ВШЭ. 2016. № 3. С. 72–84.
5. *Лопаткина Н. В., Муслов Б. В.* Правовое регулирование врачебной тайны и защиты персональных данных как фактор обеспечения безопасности личности, общества, государства // Право. Безопасность. Чрезвычайные ситуации. 2015. № 2(27). С. 17–23.
6. *Проскурякова М. И.* Конституционно-правовые рамки защиты персональных данных в России // Вестник Санкт-Петербургского университета. Право. 2016. № 2. С. 12–27.
7. *Binns R., Lyngs U., Van Kleek M., Zhao J., Libert T., Shadbolt N.* Third Party Tracking in the Mobile Ecosystem. Proceedings of the 10th ACM Conference on Web Science. Amsterdam, May 27–30, 2018. P. 23–31.
8. *Determann L.* Privacy and Data Protection // Moscow Journal of International Law. 2019. No 1. P. 18–26.

9. *Durou E.* Big Data. Mining a National Resource // A Middle East Point of View. 2015. Fall. P. 22–29. https://www2.deloitte.com/content/dam/Deloitte/xe/Documents/About-Deloitte/mepovdocuments/mepov18/mepov18_fall-2015.pdf.
10. *Ferracane M. F., Marel E. van der.* Do Data Policy Restrictions Inhibit Trade in Services? The European Centre for International Political Economy. Digital Trade Estimates Working Paper. 2018. https://ecipe.org/publications/do-data-policy-restrictions-inhibit-trade-in-services/.

Ekonomicheskaya Politika, 2020, vol. 15, no. 3, pp. 152-175

Olga D. ISMAGILOVA. Institute for International Economics and Finance, Russian Foreign Trade Academy (4A, Pudovkina ul., Moscow, 119285, Russian Federation); Russian APEC Study Center, Russian Presidential Academy of National Economy and Public Administration (11, Prechistenskaya nab., Moscow, 119034, Russian Federation).
E-mail: oibrishim@gmail.com

Karine R. KHADZHI. Institute for International Economics and Finance, Russian Foreign Trade Academy (4A, Pudovkina ul., Moscow, 119285, Russian Federation); Russian APEC Study Center, Russian Presidential Academy of National Economy and Public Administration (11, Prechistenskaya nab., Moscow, 119034, Russian Federation).
E-mail: k.khadzhi@vavt.ru

Global Experience in Regulating Data Protection, Transfer and Storage

Abstract

Cross-border data flows management and privacy protection are placed high in the international digital agenda due to unprecedented growth in the volume and pace of data collection, processing, storage and transfer globally. Despite the high importance of data flows regulation and its serious influence on all enterprises involved in digital economy, there is little research conducted in Russia and systemizing the national strategies in this sphere of regulation. The article provides an overview of the existing approaches of different countries to data protection, transfer (cross-border included) and storage, analyses the impact of regulation on international trade flows, and develops proposals for possible measures to reduce costs for companies in the digital age. The research discovers that today most countries of the world regulate personal data and other categories of sensitive data flows through the introduction of either a separate law or data protection provisions in the relevant sectoral laws. The countries' approaches range from a complete ban on the cross-border transfer of all or certain categories of data to foreign countries to complete liberalization in this area. The most common approach is the introduction of one or several restrictions from the set of measures related to cross-border data transfers: data localization requirement; limitations on the number or type of countries to which sensitive data can be transferred without additional requirements; and the requirement of the personal data subject's consent or responsible public authorities' permission.
Keywords: personal data, sensitive data, data protection, cross-border data flows, data localization, e-commerce.
JEL: F02, K24.

References

1. Birukov M. M. Aktual'nye aspekty pravovoy zashchity personal'nykh dannykh v Yevropeyskom soyuze, SSHA i Rossii [Topical Aspects of the Legal Protection of Personal Data in the European Union, the United States and Russia]. *Moskovskiy zhurnal mezhdunarodnogo prava [Moscow Journal of International Law]*, 2015, no. 3, pp. 197-208.
2. Evseeva A. A., Kalutsky I. V., Spevakov A. G. Sravnitel'nyy analiz rossiyskogo i kitayskogo zakonodatel'stva v oblasti obrabotki i zashchity personal'nykh dannykh [Comparative Analysis of Russian and Chinese Legislation in the Area of Processing and Protection of Personal Data]. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta [Proceedings of the Southwest State University]*, 2016, vol. 20, no. 3, pp. 78-84.
3. Emuranova O. A. Sravnitel'nyy analiz pravovogo regulirovaniya zashchity personal'nykh dannykh grazhdan Rossii i stran BRIKS [Comparative Analysis of Legal Regulation of Personal Data Protection of the Citizens in Russia and BRICS Countries]. In: *V mire nauki i innovatsiy: sb. stat. st. Mezhdunar. nauch.-prakt. konf. (25 dekabrya 2016 goda, Perm) [In the World of Science and Innovations: Collection of Articles of the International Workshop and Conference, 25 December 2016, Perm]*, in 8 vols., vol. 8. Ufa, Aeterna, 2016, pp. 159-164.
4. Zhuravlev M. S. Zashchita personal'nykh dannykh v telemeditsine [Personal Data Protection in Telemedicine]. *Pravo. Zhurnal VShE [Law. HSE Journal],* 2016, no. 3, pp. 72-84.
5. Lopatkina N. V., Muslov B. V. Pravovoe regulirovanie vrachebnoy tayny i zashchity personal'nykh dannykh kak faktor obespecheniya bezopasnosti lichnosti, obshchestva, gosudarstva [Legal Regulation of Medical Confidentiality and Personal Data Protection as a Factor of Safety of the Individual, Society and State]. *Pravo. Bezopasnost'. Chrezvychaynye situatsii [Law. Safety. Emergency Situations]*, 2015, no. 2(27), pp. 17-23.
6. Proskuryakova M. I. Konstitutsionno-pravovye ramki zashchity personal'nykh dannykh v Rossii [Constitutional Framework for the Protection of Personal Data in Russia]. *Vestnik Sankt-Peterburgskogo universiteta [Vestnik of Saint Petersburg University]*, 2016, no. 2, pp. 12-27.
7. Binns R., Lyngs U., Van Kleek M., Zhao J., Libert T., Shadbolt N. Third Party Tracking in the Mobile Ecosystem. In: *Proceedings of the 10th ACM Conference on Web Science.* Amsterdam, 2018, May 27-30, pp. 23-31.
8. Determann L. Privacy and Data Protection. *Moscow Journal of International Law,* 2019, no. 1, pp. 18-26.
9. Durou E. Big Data. Mining a National Resource. *A Middle East Point of View*, 2015, Fall, pp. 22-29. https://www2.deloitte.com/content/dam/Deloitte/xe/Documents/About-Deloitte/mepovdocuments/mepov18/mepov18_fall-2015.pdf.
10. Ferracane M. F., Marel E. van der. Do Data Policy Restrictions Inhibit Trade in Services? *The European Centre for International Political Economy*, Digital Trade Estimates Working Paper, 2018. https://ecipe.org/publications/do-data-policy-restrictions-inhibit-trade-in-services/.