Экономическая политика. 2022. Т. 17. № 4. С. 76–99 DOI: 10.18288/1994-5124-2022-4-76-99

Цифровая экономика

Доступ к данным в цифровой экономике: рекомендации, инициативы, перспективы

Александра Александровна Коваль

ORCID ID: 0000-0002-0431-1725

Научный сотрудник Центра
Россия — ОЭСР, РАНХиГС
(РФ, 119571, Москва, пр. Вернадского, 82).
E-mail: koval-aa@ranepa.ru

Антонина Давидовна Левашенко

ORCID ID: 0000-0003-2029-3667

Руководитель Центра
Россия — ОЭСР, РАНХиГС
(РФ, 119571, Москва, пр. Вернадского, 82).
E-mail: levashenko@ranepa.ru

Ольга Сергеевна Магомедова

ORCID ID: 0000-0003-0593-3101

Аналитик Центра ответственного ведения бизнеса, Всероссийская академия внешней торговли Министерства экономического развития Российской Федерации
(РФ, 119285, Москва,
Воробьевское шоссе, 6а).
E-mail: o.magomedova.96@vavt.ru

Аннотация

Цель настоящей статьи — дать оценку правовому режиму данных в России с точки зрения возможности имплементации международных стандартов и лучших зарубежных практик. Для развития цифровой экономики данные являются ключевым ресурсом, поэтому условия доступа к ним и обмена ими становятся факторами благосостояния современного информационного общества и качественного развития конкурентных цифровых рынков. В статье проводится правовой анализ Рекомендации ОЭСР по улучшению доступа к данным и обмену ими 2021 года. Базовая рекомендация по развитию доступности данных заключается в установлении доверия среди участников оборота данных. Основой для доверия служат надежные правовые режимы защиты соответствующих данных. Поэтому международные эксперты поддерживают государства в обеспечении сбалансированных мер развития доступа к данным и обмену ими, которые давали бы больше свободы для оборота данных при сохранении правовых гарантий соответствующих режимов данных. В качестве примера зарубежных практик по регулированию данных для содействия цифровой экономике исследователи приводят положения Регламента ЕС об управлении данными. Опыт ЕС включает разработку трех механизмов улучшения доступа к данным: механизма повторного использования защищаемых данных в публичном секторе, института посредника в передаче данных и института альтруистичного управления данными (data-альтруизма). Для выявления препятствий к имплементации исследованных стандартов и практик рассматриваются основные пробелы и недостатки российского законодательства в области персональных данных. В результате анализа формулируются выводы о необходимости внесения определенных изменений в ФЗ-152 «О персональных данных» в части расширения возможностей субъектов персональных данных управлять ими как непременного условия для становления надежного оборота данных.

Ключевые слова: обмен данными, персональные данные, управление данными, передача данных, ОЭСР, ЕС, data-альтруизм, владельцы данных, пользователи данных.
JEL: M15, O19, L86.

Статья подготовлена в рамках выполнения научно-исследовательской работы государственного задания РАНХиГС.

Статья поступила в редакцию в июне 2022 года

Ekonomicheskaya Politika, 2022, vol. 17, no. 4, pp. 76–99 DOI: 10.18288/1994-5124-2022-4-76-99

Digital Economy

Access to Data in the Digital Economy: Recommendations, Initiatives, Prospects

Alexandra A. Koval

ORCID ID: 0000-0002-0431-1725

Researcher, Center Russia—OECD, Russian Presidential Academy of National Economy and Public Administration,[a] koval-aa@ranepa.ru

Antonina D. Levashenko

ORCID ID: 0000-0003-2029-3667

Head, Center Russia—OECD, Russian Presidential Academy of National Economy and Public Administration,[a] levashenko@ranepa.ru

Olga S. Magomedova

ORCID ID: 0000-0003-0593-3101

Analytic, Center of Responsible Business Conduct, Russian Foreign Trade Academy of the Ministry of Economic Development of Russian Federation,[b] o.magomedova.96@vavt.ru

[a] 82, Vernadskogo pr., 119571, Moscow, Russian Federation

[b] 6a, Vorobevskoe sh., 119285, Moscow, Russian Federation

Abstract

This article assesses how compatible Russia's legal regime for digital data is with the implementation of international standards and best practices. Data is a key resource for developing a digital economy, and therefore the conditions provided for access to data and data sharing become factors in the well-being of an information society and in the qualitative development of competitive digital markets. As an illustration of the applicable international standards, the article provides legal analysis of the OECD Recommendation on Enhancing Access to and Sharing of Data from 2021, which is concerned primarily with ensuring the trustworthiness of the data ecosystem; and the essential element for that is a reliable legal regime protecting data. Governments should therefore provide balanced measures for facilitating both access to and sharing of data in order to allow more freedom for data to circulate while maintaining the legal guarantees of the data regimes. As an illustration of the best international regulatory practices, the article analyzes the recently adopted EU Data Governance Act, which addresses three main topics: the reuse of protected data in the public sector, the configuration of providers of data sharing services, and the introduction of what is termed data altruism. The authors examine the main gaps and shortcomings in Russian legislation pertaining to personal data in order to identify ways in which implementation of international standards and practices might be hindered. The article concludes with the authors' argument that amendments to Federal Law No. 152 "On Personal Data" are necessary to improve the ability of personal data subjects to manage their data, as this is an essential condition for the development of a trustworthy data ecosystem in Russia.

Keywords: data sharing, personal data, data management, data transfer, OECD, EU, data altruism, data owners, data users.

JEL: M15, O19, L86.

Acknowledgements

The article has been prepared as part of a research program commissioned by the state from the RANEPA.

Article submitted June 2022

Введение

На новом витке развития цифровых прав больше внимания необходимо уделять правам на доступ к информации и обмену данными. Прежде всего это обусловлено тенденцией датафикации (*datafication*) многих областей жизни, когда деятельность человека, его личностные характеристики и позиции преобразуются в данные, которые получают экономическую ценность в условиях цифровой экономики. Например, реализация гражданских прав стала зависеть от возможности доступа к инструментам открытого правительства (*open government*), передачи своих данных, обмена информацией [Graef, Prüfer, 2021]. В цифровой экономике право на доступ к информации получает новую коннотацию: речь идет уже о доступе не столько к сведениям, сколько к возможностям и преимуществам цифровой экономики, связанным с данными, к технологиям, основанным на данных (технологиям алгоритмической обработки данных, таким как искусственный интеллект, интернет вещей (IoT), большие данные, блокчейн и др.), к публичным услугам в режиме онлайн и т. д.

В этом отношении стимулирование доступа к информации и создание условий для обмена данными находятся в общей парадигме инклюзивного устойчивого развития. По оценкам международных экспертов, доступ к данным и обмен способны генерировать добавочную стоимость в размере от 0,1 до 1,5% внутреннего валового продукта какого-либо государства для публичного сектора и от 1 до 2,5% — для частного сектора[1]. Еще до бума цифровизации многих областей мировой экономики на фоне пандемии аналитики *International Data Corporation (IDC)* прогнозировали ежегодный рост объема данных до 61% с достижением к 2025 году объема в 175 зеттабайт [Reinsel et al., 2018]. Несмотря на рост оборота данных в мире, публичные институты, компании и физические лица по-прежнему сталкиваются с барьерами в доступе к данным и обмену данными. Эксперты Организации экономического сотрудничества и развития (ОЭСР) выделяют три группы проблем в этой области.

Во-первых, повышение открытости данных сопряжено с рисками нарушения прав, связанных с соответствующей информацией (например, сведения о производственных операциях хотя и представляют интерес для бизнеса, но подпадают под режим коммерческой тайны). Это значит, что расширение доступа к данным со специальными режимами защиты ограничено правовыми гаран-

[1] Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies. 2019. https://www.oecd.org/publications/enhancing-access-to-and-sharing-of-data-276aaca8-en.htm.

тиями сохранения соответствующего режима. Тем не менее такая задача решаема, если пользователи и владельцы данных смогут определить оптимальные условия оборота данных на основе риск-ориентированного подхода.

Во-вторых, для оборота данных необходимо выстраивать доверие между его участниками, прежде всего со стороны носителей данных (применительно к персональным данным) и владельцев данных (применительно к данным, связанным с правами интеллектуальной собственности, данным в режиме коммерческой тайны и т. д.). Поэтому эксперты отмечают необходимость поддержки активного участия заинтересованных лиц в вопросах управления данными, включая создание партнерств владельцев и пользователей данных. Вместе с тем следует учитывать, что партнерства между пользователями и владельцами данных не должны ограничивать доступ к обороту для новых лиц или для лиц из других юрисдикций, чтобы не создавать антиконкурентные эффекты на глобальных рынках цифровых услуг.

В-третьих, доступ к данным должен обеспечиваться посредством специальных механизмов и устойчивых бизнес-моделей, которые учитывают необходимые правовые гарантии. Важно сокращать правовые пробелы и неопределенности режима владения данными, а также содействовать укреплению в цифровой экономике принципа свободы договора в B2B-отношениях (в деловых отношениях между коммерческими организациями) с учетом характера данных, составляющих объект сделок.

В решении обозначенных групп задач неприемлемы управленческие шаблоны (то, что зарубежные эксперты называют *one-size-fits-all solutions*). Каждый цифровой сегмент уникален, каждый тип данных имеет свои особенности, главное же в том, что рынки цифровых услуг развиваются на базе различных законодательных и регуляторных подходов в отношении данных.

В настоящей статье проводится детальный разбор Рекомендации ОЭСР по улучшению доступа к данным и обмену ими, которая представляет собой уникальную систему международных стандартов, применимых при формировании государствами национальных подходов к управлению данными. Авторы настоящей статьи принимали непосредственное участие в качестве экспертов в составе российской делегации в разработке Рекомендации в рамках деятельности Комитета ОЭСР по политике в области цифровой экономики (*Committee on Digital Economy Policy, CDEP*) в 2019–2021 годах. Ярким примером имплементации международных стандартов служит Регламент ЕС об управлении данными, предлагающий несколько новых механизмов. Авторы проводят обзор пробелов российского законодательства, препятствующих

имплементации международных рекомендаций или заимствованию успешного зарубежного опыта. В заключение представлены правовые рекомендации для улучшения доступа к данным и оборота данных в России.

2. Правовой анализ Рекомендации ОЭСР по улучшению доступа к данным и обмену ими

На международных площадках разрабатываются рекомендации и стандарты для повышения доступности данных. В разработку вопросов этой области и цифровой экономики в целом большой вклад вносит ОЭСР.

В октябре 2021 года советом министров ОЭСР была утверждена Рекомендация ОЭСР по улучшению доступа к данным и обмену ими (OECD Recommendation on Enhancing Access to and Sharing of Data, далее — Рекомендация EASD)[2]. Этот документ стал первым согласованным на международном уровне многоотраслевым инструментом повышения доступности данных для национальных правительств. Следует отметить, что разработка Рекомендации основывалась на опыте принятия организацией секторальных инструментов улучшения доступа к данным, таких как Рекомендация по управлению данными о здоровье 2016 года[3]. Рекомендация EASD включает принципы и указания для регуляторных решений по максимизации преимуществ использования всех типов данных (персональных, неперсональных, открытых, служебных, публичных и частных) в различных отраслях. Таким образом, положения Рекомендации разработаны для универсального применения по отраслям и типам данных. Следует проанализировать содержание и правовое значение каждой из рекомендаций в отдельности.

1. *Первая и базовая рекомендация* заключается в укреплении надежности систем данных (*trustworthiness of the data ecosystem*). Вопрос обеспечения надежности систем данных является основным для развития цифровой экономики и информационного общества в целом. Надежность подразумевает не только (и не столько) кибербезопасность, сколько готовность управлять рисками, с которыми сопряжено повышение открытости данных. Так, эксперты Комитета ОЭСР по политике в области цифровой экономики выделяют такие риски открытости данных, как нарушение безопасности персональных данных, этические нарушения их обработки, нарушение правового режима данных, связанных с правами интеллектуальной собственности, нарушение режима конфиденциальности данных (включая утечку и несанкциониро-

[2] https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0463.
[3] https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0433.

ванный доступ к ним), утрата контроля обработки данных их носителями или законными владельцами, низкий уровень доверия к институтам публичного и частного секторов[4].

Для повышения надежности экосистем данных рекомендуется прежде всего обеспечить участие заинтересованных лиц в открытом и инклюзивном процессе консультаций при разработке, имплементации и мониторинге политик управления данными в части повышения доступа к ним. Такая мера необходима для повышения доверия к экосистемам данных и современным информационным технологиям их обработки [Hansen, 2016]. В частности, рекомендуется создавать публично-частные партнерства по обмену данными. Как указывает ОЭСР, обмен между публичным и частным секторами может иметь социально ценные эффекты (*additional value for society*), включая конкретные экономические выгоды[5]. Основным условием для публично-частного взаимодействия является приверженность системе открытого правительства и публичным интересам.

Следует отметить, что, как и другие рекомендации ОЭСР, Рекомендация EASD строится на принципе инклюзивного управления, поэтому многие положения мотивируют национальных управленцев к большему вовлечению в регуляторные процессы заинтересованных лиц. Практики вовлечения заинтересованных лиц в регуляторный процесс пользуются большой популярностью в странах ОЭСР и поддержкой международных организаций ввиду легитимирующего эффекта. Речь идет об общественном восприятии регуляторных решений как справедливых и правомерных. Однако, как уточняют зарубежные исследователи, выполнение процедуры привлечения заинтересованных лиц само по себе не легитимирует принятые в результате регуляторные решения [Busuioc, Jeynaker, 2022]. Легитимирующий эффект возникает только с учетом таких факторов, как условия участия заинтересованных лиц в процедурах взаимодействия (консультациях, сборе мнений), порядок организации процедур взаимодействия с точки зрения прозрачности и равного доступа [Braun, Busuioc, 2020]. Поэтому формальное включение процедур взаимодействия с заинтересованными лицами без действительного использования этих ресурсов (наблюдений, рекомендаций, замечаний) не решает задачи инклюзивного управления данными. Важно, что международные практики вовлечения заинтересованных лиц не ограничиваются опытом стран с классической моделью гражданского общества, проявляющего активность в вопросах публично-

[4] https://www.oecd-ilibrary.org/science-and-technology/mapping-data-portability-initiatives-opportunities-and-challenges_a6edfab2-en.

[5] http://theodi.org/wp-content/uploads/2021/03/RPT_Trust-in-data-ecosystems-23.02.21-STC-final-report.pdf.

го управления. Например, канадские юристы, разрабатывающие предложения для Национальной стратегии по данным Канады, апеллируют к успешному опыту Бразилии в проведении публичных консультаций по закону о правах в интернете, известному как Marco Civil da Internet [Tusikov, Haggart, 2020].

Для установления доверия к цифровым решениям правительствам рекомендовано также повышать транспарентность условий доступа к данным и обмена информацией, имплементируя практики ответственного управления данными на всех циклах работы с ними (*data value cycle*). Подчеркивается, что практики управления данными должны соответствовать применимым, признанным и широко принятым техническим, организационным и правовым стандартам, включая кодексы поведения, этические принципы[6]. Отдельно оговаривается, что для баз персональных данных условия их обработки должны охватывать регулирование субъектов, которым обеспечивается доступ, субъектов, которым передаются данные, условий, на которых возможен обмен ими.

2. Вторая рекомендация касается принятия правительствами единого подхода к вопросу обеспечения доступа к данным на всех уровнях и областях управления, так называемого *strategic whole-of-government approach*. На практике такой подход включает несколько компонентов. Во-первых, необходимо сделать вопросы доступа к данным и обмена ими приоритетными при принятии решений. Это значит, что решения принимаются только с учетом их преимуществ и недостатков относительно цели обеспечения доступа к данным. Во-вторых, регуляторные решения могут приниматься на основе единых правил, применимых для различных уровней управления (*scalable data governance frameworks*). Формат масштабируемых основ (*scalable frameworks*) отличается от привычных инструментов работы, применяемых в иерархической структуре органов, когда, например, вышестоящий орган формирует рекомендации для подведомственных институтов. Такой формат предполагает горизонтальное применение единых рамок работы независимо от уровня компетенций [Lovelock, 2018]. Единый вектор в регуляторной политике может задаваться и путем принятия национальных стратегий по управлению данными (*national data strategies*), которые охватывали бы экономические, социальные,

[6] Кодексы поведения в обработке данных могут разрабатываться профильными ведомствами или экспертными организациями в области управления данными, например: European Commission. Ethics and Data Protection, 2021. https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-and-data-protection_he_en.pdf; European Data Protection Board. Codes of Conduct, 2019–2022. https://edpb.europa.eu/our-work-tools/our-documents/topic/code-conduct_en. Кроме того, кодексы поведения в обработке данных принимаются на отраслевом уровне, например: Asociación para la Autorregulacion de la Comunicación Comercial. Code of Conduct in Data Processing in Advertising Activities. https://edpb.europa.eu/system/files/2021-04/code_of_conduct_data_processing_in_advertising_activities_en.pdf.

культурные, технические и правовые аспекты. Например, проект такой стратегии рассматривается в Канаде в контексте инициатив по трансформации публичных сервисов[7]. Проект пользуется значительной поддержкой гражданского общества и независимых специалистов[8]. Хотя универсальная стратегия не была принята, Канада в октябре 2019 года успешно представила Стратегию по данным о здоровье как наиболее чувствительной категории. В-третьих, необходимо обеспечить возможность координации институтов при принятии решений. В-четвертых, следует создать правовой режим доступа к данным, не связанный с конкретными технологическими решениями и способный применяться одинаково для всех информационных технологий и технологических операций (*technology-neutral regulatory environment*) [Koops, 2006].

3. Третья рекомендация касается чувствительной темы соблюдения баланса между стремлением к облегчению доступа к данным и необходимостью соблюдения связанных с ними публичных и частных прав. Такая сложная юридическая задача была дословно зафиксирована в рекомендации: «Обеспечивать условия доступа к данным и обмена ими, гарантируя, что данные настолько открыты, насколько возможно для того, чтобы максимизировать извлекаемые из них преимущества, и что данные настолько закрыты, насколько это необходимо для защиты публичных и частных интересов»[9]. Речь идет о конкретных интересах, включая национальную безопасность, правоприменение, защиту неприкосновенности частной жизни (защиту персональных данных), прав интеллектуальной собственности, а также о таких этических ценностях, как добросовестность, человеческое достоинство, защита от предвзятых решений и дискриминации в отношении отдельных лиц или социальных групп. В связи со сложностью вопроса стоит обратить внимание на юридическую технику формулирования рекомендаций. Для защиты публичных и частных интересов как условия доступа к данным и обмена ими рекомендуется принимать именно «соразмерные шаги» (*proportionate steps*), то есть шаги, сбалансированные с шагами по обеспечению доступа к данным.

Кроме того, сами участники оборота должны нести ответственность за качество данных, которые они предоставляют, и за имплементацию мер управления рисками на протяжении всего цикла обработки данных, включая меры, необходимые для защи-

---

[7] Centre for International Governance Innovation. A National Data Strategy for Canada. Key Elements and Policy Considerations. https://www.cigionline.org/static/documents/documents/Paper%20no.160_3.pdf.

[8] *Scassa T.* Canada's Data Plan: We Need a Data Strategy that Supports Our Values and Encourages Innovation. 2019. https://apo.org.au/sites/default/files/resource-files/2019-01/apo-nid216561.pdf.

[9] Recommendation of the Council on Enhancing Access to and Sharing of Data. 6 October 2021. Item V (a). https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0463.

ты их конфиденциальности и безопасности. В связи с этим государствам рекомендуется содействовать в имплементации оценки воздействия и проведения аудита в операциях управления данными. Безусловно, такие меры требуют строгой организации, поэтому компании, работающие с данными, также нуждаются в грамотной кадровой политике в части распределения функций, зон ответственности при принятии решений, в использовании консультационных механизмов, в предотвращении рисков.

Баланс между доступностью данных и соблюдением публичных и частных интересов достигается путем взаимных ограничений в каждой области: если меры для защиты прав — то соразмерные, если доступ к данным — то при определенных условиях (*conditioned data access*). Специалисты международной организации прямо рекомендуют стимулировать имплементацию механизмов контроля доступа к данным и технологиям их повышенной защиты.

4. Развитие доступа к данным происходит в рамках цифровой экономики. Поэтому следующая, *четвертая рекомендация* касается развития рыночных аспектов доступа к данным, прежде всего поддержки конкурентных условий их получения. При должном соблюдении прав потребителей, прав интеллектуальной собственности и прав на защиту персональных данных субъекты должны иметь возможность контролировать свои данные и управлять ими. Злоупотребление со стороны компаний законно полученными данными недопустимо, включая практики их использования для расширения влияния на рынке. Возможные гибкие решения в обеспечении здоровой конкурентной среды в цифровой экономике — это кодексы поведения, руководства, соглашения по доступу к данным и обмену ими. Для этой цели также немаловажное значение имеет и доступ к капиталу. Поэтому для государств важно поддерживать долгосрочные инвестиции в технические решения для доступа к данным и обмену ими, в том числе путем поддержки новых бизнес-моделей, инноваций, проектов масштабирования бизнеса.

5. Доступ к данным должен обеспечиваться независимо от юрисдикции расположения пользователя, владельца информационной системы, серверов облачного провайдера и т. д., то есть должен быть трансграничным. Однако многие государства, включая Россию, связывают вопрос трансграничной передачи данных с проблемами национальной информационной безопасности. Международный документ ОЭСР не стимулирует государства к пересмотру своих позиций, но рекомендует «оценивать и по мере возможного минимизировать ограничения на трансграничный доступ к данным

и трансграничный обмен данными»[10]. Те ограничения, которые государства всё же устанавливают на свое усмотрение, должны применяться на недискриминационной основе, быть транспарентными, *необходимыми* и *соразмерными* уровню рисков. Необходимость мер, ограничивающих доступ к данным, целесообразно оценивать по таким критериям, как чувствительность данных, цель и контекст доступа, обмена и использования [Бембеева, 2018].

6. Доступ к данным определяется также техническими характеристиками их формата и выполняемых с ними операций. Поэтому Рекомендация EASD ОЭСР направлена на поддержку поисковой доступности, интероперабельности данных, а также возможности их многократного использования организациями как публичного, так и частного секторов. На техническом уровне доступность данных обеспечивается, если они передаются со всеми необходимыми метаданными (сведениями о технических характеристиках информации или о содержании, например IP-адрес владельца информации, формат данных и др.), в том числе с помощью Application Programming Interface, программных интерфейсов приложений.

7. Наконец, доступ к данным зависит от способностей самих субъектов их использовать. Поэтому государствам рекомендовано принимать меры по повышению сознательности субъектов в использовании данных, в том числе в части понимания преимуществ и рисков их использования, по развитию компетенций и навыков для работы с ними. Государствам следует обеспечивать доступ к устойчивым, открытым, безопасным, масштабируемым объектам информационной инфраструктуры для сбора, обработки и хранения данных.

Таким образом, семь рекомендаций в международном документе ОЭСР задают для государства ключевые направления работы и принципы развития в этих направлениях. Обозначенные направления составляют необходимые аспекты полноценного режима обеспечения доступа к данным. Государства могут в различной мере прилагать усилия по имплементации отдельных направлений, однако асимметрия усилий препятствует получению положительных результатов. Например, если государство не способно обеспечить технические условия защиты персональных данных от их несанкционированного использования, то ему будет сложно справиться с базовой задачей установления доверия пользователей. Следовательно, оно не может эффективно реализовывать политику обеспечения открытых публичных данных или другие мероприятия по

[10] Recommendation of the Council on Enhancing Access to and Sharing of Data. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0463.

развитию доступа к данным и обмена ими. Поэтому Рекомендация ОЭСР должна имплементироваться планомерно.

3. Пример зарубежного опыта совершенствования доступа к данным: Регламент ЕС об управлении данными

Международные рекомендации формируются в ответ на реальные вызовы и трудности, с которыми сталкиваются государства. Нередко рекомендации основываются на уже полученном удачном опыте решения тех или иных задач или на интересных проектах в соответствующей области. В этом отношении большой исследовательский и практический интерес представляет Регламент ЕС об управлении данными, принятый Европейским парламентом в апреле 2022 года (Data Governance Act, далее — регламент, DGA)[11]. Проект регламента был представлен Еврокомиссией в ноябре 2020 года и получил преимущественно положительные оценки на публичных консультациях, завершившихся в сентябре 2021-го[12]. Регламент вступит в силу спустя пятнадцать месяцев с момента принятия, в июле 2023 года[13]. Основная задача регламента — обеспечить надежные механизмы для многократного использования некоторых категорий защищенных данных как в публичном, так и в частном секторе с помощью создания института посредников информационных услуг и стимулирования практик добровольного предоставления данных для многократного пользования. Появление регламента не спонтанно: содействие обороту данных в ЕС входит в число задач Стратегии ЕС по данным (European Strategy for Data) и продолжает серию шагов по обеспечению правовых инструментов для развития цифровой экономики. Ранее в ЕС были приняты Регламент о свободной передаче неперсональных данных 2018 года (Regulation on the Free Flow of Non-Personal Data, FFD)[14], Акт ЕС о кибербезопасности (Cybersecurity Act)[15], Директива об открытых данных (Open Data Directive)[16]. Кроме того, в ЕС уже приняты отраслевые акты регулирования доступа к данным и их передачи, например в сфере платежных услуг, электрических систем, умных транспортных систем, систем учета ресурсов. Теперь юристы ЕС приступили к реализации проекта универсального значения[17].

---

[11] https://europarl.europa.eu/doceo/document/TA-9-2022-0111_EN.html.
[12] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767.
[13] https://ec.europa.eu/commission/presscorner/detail/en/ip_21_6428.
[14] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1807.
[15] https://eur-lex.europa.eu/eli/reg/2019/881/oj.
[16] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019L1024.
[17] *Horjak S.* Promoting Data Sharing: Presidency Reaches deal with Parliament on Data Governance Act. 2021. December 1. https://slovenian-presidency.consilium.europa.eu/en/news/promoting-data-sharing-presidency-reaches-deal-with-parliament-on-data-governance-act/.

Регламент представляет три значительные инициативы.

Во-первых, он создает механизм для безопасного многократного использования некоторых категорий данных в публичном секторе (глава II: «Повторное использование некоторых категорий защищенных данных органами в публичном секторе», ст. 3–8). Речь идет о таких категориях собранных для целей ведения статистики данных, как персональные, составляющие коммерческую тайну, защищающие право интеллектуальной собственности. В этом отношении Регламент DGA дополняет Директиву по открытым данным 2019 года, которая не касалась перечисленных видов данных[18]. Регламент прямо устанавливает запрет предоставления исключительных прав на повторное использование защищаемых данных в публичном пользовании или иных практик, ограничивающих доступ к таким правам (п. 1 ст. 4). Публичные органы должны определить условия доступа к неоднократному использованию защищенных данных: условия должны быть недискриминационными, пропорциональными, объективно обоснованными и публично доступными для ознакомления (п. 1, 2 ст. 5). Публичные органы должны иметь надлежащие технические условия, для того чтобы обеспечить сохранение режима защиты данных (п. 5 ст. 5). В требованиях беспрепятственного доступа к повторному использованию данных существуют исключения, связанные с выполнением цели общественного интереса. Если достижение общественной цели невозможно без предоставления исключительного права на повторное использование данных ограниченному кругу лиц, то такое предоставление осуществляется на основе принципов транспарентности, равного обращения и недискриминации (п. 4 ст. 4). Это значит, что сам факт предоставления исключительных прав конкретным лицам должен быть открытым. Однако период пользования исключительными правами не может превышать трех лет (п. 5 ст. 4). Еврокомиссия планирует установить единую точку доступа с электронной поисковой системой по данным в публичном секторе (п. 1 ст. 8). Предоставление доступа для повторного использования данных не означает, что они выкладываются в открытый доступ или предоставляются по любому запросу. Доступ может быть платным, но плата устанавливается исключительно для того, чтобы покрывать затраты на обработку данных и администрирование запросов (п. 5 ст. 6).

Во-вторых, регламент создает условия для осуществления новой бизнес-модели в посредничестве данных — *data sharing services* (глава III: «Требования, применимые для услуг передачи данных»,

---

[18] *Baloup J., Lalova-Spinks T.* CiTiP White Paper on the Data Governance Act. 2021. August 3. https://www.law.kuleuven.be/citip/blog/citip-white-paper-on-the-data-governance-act/.

ст. 9–14). Главная задача механизма — обеспечить безопасную среду для обмена данными среди компаний и частных лиц. Примечательно, что механизмом могут пользоваться как компании, так и физические лица. Так, согласно п. 1 ст. 9 под услугами передачи данных понимаются услуги посредничества между владельцами данных (*data holders*), являющимися юридическими лицами, и потенциальными пользователями (*data users*), между субъектами, намеренными обеспечить доступ к своим персональным данным, и потенциальными пользователями. Причем такие посреднические услуги сопровождаются предоставлением соответствующих технических средств. Обмен данными может осуществляться с помощью цифровых платформ, которые обеспечивают условия для выполнения обязательств по их обмену. С использованием этих сервисов становится возможным делиться своими данными, не опасаясь их неправомерного использования или утраты. Ведь в случае компаний данные — это не только операционный ресурс для деятельности, но и ресурс с экономической ценностью, обеспечивающий конкурентное преимущество в цифровой экономике[19].

Специальные сервисы для обмена данными актуальны и для частных лиц, которым необходима поддержка в реализации своих прав как субъектов персональных данных. Использование посреднических услуг для обмена данными обеспечивает их носителям полный контроль над своими данными и позволяет делиться ими с теми компаниями, которым носители доверяют. Контроль может осуществляться с помощью таких инструментов управления личной информацией, как цифровое пространство личных данных (*data spaces / data wallets*). Эти инструменты представляют собой приложения, через которые носители данных могут обмениваться ими на основании согласия на их обработку и хранение.

Поставщики посреднических услуг в передаче данных должны задекларировать свою деятельность через национальный компетентный орган по управлению данными, что служит гарантией добросовестности посредника (цифровой платформы) для пользователей. Регистрация осуществляется в уведомительном порядке, путем направления уведомления о намерении предоставлять услуги обмена данными в компетентный орган (п. 1 ст. 10). Требования к содержанию уведомления также фиксируются в п. 6 ст. 10. Компетентный орган в течение недели издает декларацию о факте получения надлежащего уведомления об оказании посреднических услуг (п. 7 ст. 10). Основное правило в деятельности посред-

[19] *Morgan Ch. S., Langlois Fr., Lan J.* A Canadian Perspective on the EU's Proposed Data Governance Act. 2022. February 8. https://www.mccarthy.ca/en/insights/blogs/techlex/canadian-perspective-eus-proposed-data-governance-act.

ников заключается в ограничении использования данных, попадающих в распоряжение посредника, в иных целях, чем те, для которых данные были переданы (п. 1 ст. 11). Посредники не могут извлекать из полученных данных собственную выгоду, например путем их продажи. Посредник может извлекать выгоду, только взимая плату за транзакции, которые он выполняет. Задачи посредника заключаются в обеспечении обмена данными, включая их прием от владельца в определенном формате и конвертацию в иной формат по запросу пользователя для повышения межотраслевой интероперабельности данных (п. 4 ст. 11). Посредник обеспечивает безопасность данных, принимая меры для предотвращения злоупотребления доступом к ним со стороны потенциальных пользователей, технические, правовые, организационные меры для недопущения незаконного доступа к данным, меры для повышения уровня безопасности их хранения и передачи (п. 5, 7, 8 ст. 11).

В-третьих, Регламент ЕС вводит институт альтруизма в управлении данными (глава IV: "Data Altruism"). Понятие *data-альтруизм* означает добровольное обеспечение носителем данных доступа к ним для общего блага или общих интересов. Практики data-альтруизма доступны как физическим, так и юридическим лицам. Например, компании, намеренные собирать данные для целей, представляющих общий интерес, могут быть включены в национальный реестр организаций, официально занимающихся альтруизмом в управлении данными (п. 2 ст. 15). Стоит обратить внимание, что статус организации-альтруиста в управлении данными (*data altruism organization*) доступен только юридическим лицам, которые учреждены для достижения общих интересов и функционируют на некоммерческой основе, причем независимо от какой-либо коммерческой компании. Правило позволяет разграничить управление данными в коммерческих целях и данными, собранными для некоммерческих целей, а главное — предотвращает риски использования данных, предназначенных для data-альтруизма, в коммерческих целях, в том числе риски самовольного утверждения исключительных прав на обработку таких данных. Однако некоторые исследователи полагают, что проведение подобного различия, напротив, ограничивает юридические лица, которые уже практикуют альтруистичное управление данными с соблюдением всех требований европейского права в области персональных данных. В таком случае результат может быть противоположным: не деятельность выходит из серой зоны, а лица перестают осуществлять урегулированную деятельность [Veil, 2022].

Статус *data altruism organization* является общеевропейским: зарегистрированные в одной стране организации могут законно

заниматься альтруистичным управлением данными в остальных юрисдикциях ЕС. Такой статус доступен и для зарубежных компаний: постоянное представительство иностранной организации, намеренной собирать в ЕС данные на основе процедур, предусмотренных для data-альтруизма, может зарегистрироваться в одном из государств — членов ЕС (п. 3 ст. 17). Регистрацию должен осуществлять специально уполномоченный для этих целей национальный орган (п. 1 ст. 15). Главное правило в осуществлении альтруистичного управления данными — это обеспечение полной транспарентности деятельности. Поэтому зарегистрированные организации обязуются вести полные и точные записи сведений о том, какие физические и юридические лица осуществляют обработку данных во владении организации, даты и длительность обработки, декларируемые цели обработки и сведения о расходах на нее (п. 1 ст. 18). Кроме того, зарегистрированные организации несут обязательство ежегодно отчитываться о своей деятельности (п. 2 ст. 18). Раскрытию подлежат сведения о порядке сбора данных для целей общего интереса, перечень лиц, получивших к ним доступ, информация о результатах их использования, об источниках доходов и расходах компании, связанных с управлением данными. Во взаимодействии с владельцами данных зарегистрированная организация должна обязательно информировать о целях общественного значения, для которых она допускает обработку данных, а также о любых условиях их обработки за пределами стран ЕС (п. 1 ст. 19). Раскрытие сведений о территориальных условиях сопряжено с необходимостью обеспечения обработки и передачи данных в соответствии с правом ЕС.

Создание института альтруистичного управления поощряет частных лиц и компании передавать данные таким организациям, которые будут их использовать для общественного блага. В особенности такую инициативу поддерживают научные европейские сообщества [Shabani, 2021]. Участие в альтруистичных практиках доступно физическим лицам. Субъекты персональных данных могут предоставлять их с помощью специальной формы согласия на обработку, где вместо привычных положений о целях обработки приводятся указания, что согласие предоставляется на многократное использование данных для общезначимых целей (п. 1 ст. 22). Форма будет разрабатываться Еврокомиссией. Положения формы должны быть модульными; предполагается, что они будут легко адаптироваться к специфике отдельных отраслей и целей (п. 2 ст. 22). Следует подчеркнуть, что предоставление персональных данных для альтруистичных целей не лишает субъектов данных права управления ими, поэтому субъекты персональных

данных могут отзывать свое согласие, предоставленное по специальной форме, в соответствии с общей процедурой отзыва согласия, установленной положениями Регламента ЕС о защите персональных данных.

Введение нового формата практики управления данными требует определенного уровня контроля развития новых практик. Поэтому в отношении соблюдения зарегистрированными организациями обязательств по альтруистичному управлению данными компетентные национальные органы проводят мониторинг (п. 1 ст. 21). Каких-либо материальных санкций за выявленные нарушения регламент не предусматривает, преследуя цель поддержать интерес организаций к новой практике. Тем не менее в качестве крайней меры со стороны регулирующих органов указывается возможность исключения организации из реестра зарегистрированных.

Предложенные механизмы пользуются значительным вниманием компаний и организаций в области управления данными — ведь такие механизмы затрагивают сразу множество аспектов, таких как использование данных, защищаемых частными правами, в публичном секторе, обеспечение доступа к ним и их использование в B2B-отношениях, создание условий развития более конкурентных рынков облачных технологий и минимальных гарантий безопасности для оборота неперсональных данных в трансграничном контексте[20].

4. Развитие доступа к данным в России

В России тематика доступа к данным также стоит в повестке профильных государственных ведомств. Например, с 2014 года разрабатывается концепция открытых данных, в частности идея создания государственной информационной системы сбора, хранения и управления публичными данными, размещаемыми в интернете государственными органами власти и местного самоуправления (www.data.gov.ru)[21]. Но реализация проекта открытых данных в России пока малорезультативна ввиду низкого качества самих данных, как отмечают специалисты Минэкономразвития[22]. Представители отрасли также указывают на проблему дисбаланса между доступностью данных по экономическим показателям и открытостью данных по качеству жизни, например данных о преступности, уровне образования, успешных медицинских опера-

[20] https://privacylaws.com/media/3506/inception-impact-assessment.pdf.

[21] Министерство экономического сотрудничества и развития. Открытый дайджест PRO данные. 2021. Июль. https://economy.gov.ru/material/file/f8e7119514ee3e6c1dc13c35aa29ff37/open_data.pdf.

[22] Там же.

циях, заболевших определенным вирусом[23]. Для развития бизнеса наиболее значимы именно данные по качеству жизни, поскольку они позволяют правильно оценивать потребительский рынок и другие факторы[24]. Следует отметить, что вопрос открытости данных, интересных для частного сектора, а тем более генерируемых внутри него, остается проблематичным не только в России. По оценкам экспертов ОЭСР, только 15% публичных инициатив по управлению данными в странах ОЭСР направлены на содействие обороту в частном секторе[25].

В правовом режиме данных имеются и другие пробелы, препятствующие эффективной имплементации в России международных рекомендаций и лучших практик. Так, выполнение базовой рекомендации надежности и доверия ограничено тем, что положения ФЗ-152 «О персональных данных» не обеспечивают субъектов персональных данных правом в полной мере распоряжаться ими [Мамыкина, 2020]. Прежде всего можно видеть ряд пробелов в порядке получения согласия на обработку персональных данных. В условиях не закреплено требование об их обработке для цели, строго определенной в форме получения такого согласия (ст. 6 ФЗ-152). Кроме того, в условиях действительности согласия устанавливается, что «согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом» (п. 1 ст. 9 ФЗ-152)[26]. Такая формулировка в российском законодательстве допускает возможность выводить наличие согласия субъекта персональных данных на сбор и обработку его данных из его конклюдентных действий. Например, когда интернет-пользователь регулярно совершает какие-либо операции на цифровой платформе, его действия могут негласно фиксироваться на платформе. Собранные таким образом данные потенциально подвержены анализу с помощью алгоритмических технологий для формирования теневого цифрового профиля пользователя [Гадельшин, Степанов, 2021]. Проблема несанкционированного формирования цифровых профилей пользователей (как совокупности данных о предпочтениях, алгоритмах действий и иных характеристик пользователей) заключается в потенциальном риске использования данных против интересов пользователя вплоть

---

[23] Министерство экономического сотрудничества и развития. Открытый дайджест...

[24] Количество открытых данных в России растет, а их качество — нет // CNEWS. 2021. 14 июля. https://cnews.ru/news/top/2021-07-14_kolichestvo_otkrytyh_dannyh.

[25] Enhancing Access to and Sharing of Data… https://www.oecd.org/publications/enhancing-access-to-and-sharing-of-data-276aaca8-en.htm.

[26] http://www.consultant.ru/document/cons_doc_LAW_61801/6c94959bc017ac80140621762d2ac59f6006b08c/.

до цифровой дискриминации, например демонстрации товаров на маркетплейсе в зависимости от предпочитаемой потребителем ценовой категории товаров. В результате в России субъекты персональных данных не пользуются теми необходимыми гарантиями соблюдения их свободного целевого согласия на обработку данных, которые обеспечивали бы доверие носителей данных к возможностям их оборота, согласно рекомендации I в документе ОЭСР (Рекомендации EASD).

Проблема неясного режима прав субъектов персональных данных отражается и на определении прав и обязательств операторов данных. Так, в российском законодательстве не закреплено обязательство последних уведомлять субъектов персональных данных о нарушении безопасности данных. Ввиду интенсификации оборота данных, увеличения числа лиц, способных получить доступ к ним, и иных факторов цифровизации, повышающих вероятность рисков нарушения персональных данных, субъектам данных нужны гарантии, что они будут уведомлены о любых инцидентах, которые нарушают доступность, целостность или конфиденциальность данных и информационных систем [Петренко, Суховей, 2012]. Обязательство уведомления о нарушении уже закреплено в Регламенте ЕС о защите персональных данных (ст. 33), в Гражданском кодексе штата Калифорния (ст. 1798.29) и других документах. Пробелы в правовом режиме базовых участников оборота данных, носителя данных и оператора данных препятствуют введению новых категорий участников, таких как хранилища или банки данных (*data repositories*), брокеры данных (*data brokers*), рынки данных (*data marketplaces*), и других, оказывающих посреднические и сопроводительные услуги владельцам и носителям данных. К этой категории относятся и поставщики посреднических услуг по смыслу Регламента ЕС об управлении данными (*providers of data sharing services*). Ясное разграничение прав и обязательств участников оборота данных, включая посредников, составляет необходимое условие для реализации Рекомендации ОЭСР о развитии рыночных аспектов доступа к данным.

В российском законе о персональных данных прямо не закреплено право субъекта персональных данных на их перенос, рекомендуемое к закреплению в национальном праве в Рекомендации EASD. Переносимость данных (*data portability*) означает возможность передачи данных, собранных и обрабатываемых одним оператором, другому оператору по воле субъекта этих персональных данных. Право на перенос данных представляет один из элементов контроля субъекта персональных данных над своими данными, предоставленными для обработки [Абрамова, 2020]. Такое право имеет большое экономическое значение. Для субъекта это право

означает облегчение доступа к получению цифровых услуг от различных поставщиков. Для поставщиков цифровых услуг — доступ к данным большего числа пользователей. В этом отношении право на перенос данных рассматривается как фактор развития более конкурентного рынка цифровых услуг. По мнению международных экспертов, отсутствие законодательного регулирования такого права может тормозить развитие цифровой экономики[27]. Поэтому страны ОЭСР, в которых еще не установлено такое право, стремятся вносить в национальное законодательство необходимые поправки. Например, в 2021 году Южная Корея внесла поправки в закон о персональной информации 2011 года, закрепившие ряд дополнительных прав и гарантий субъектам персональных данных, включая право на перенос данных [Park, Kang, 2021].

От качества регулирования зависит развитие практик ответственного и осознанного управления данными на уровне частных лиц, а соответственно, и возможность для организаций более эффективно взаимодействовать с субъектами данных по вопросам их передачи или предоставления к ним доступа для конкретных целей, в том числе общественно значимых (научных, журналистских, статистических). Сегодня в России регулирование доступа к персональным данным для научных и иных значимых целей не дает ясного понимания, каким образом упрощается доступ к данным и упрощается ли вообще. Дело в том, что Федеральным законом «О персональных данных» (ФЗ-152) устанавливается, что «обработка персональных данных осуществляется в статистических или иных исследовательских целях при условии обязательного обезличивания персональных данных» (п. 9 ст. 9). Однако в зависимости от цели исследования может быть необходим полный комплекс данных о человеке. Кроме того, согласно п. 8 ст. 9 ФЗ-152 обработка персональных данных для профессиональной деятельности журналиста, научной, литературной или иной творческой деятельности возможна «при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных». На практике это значит, что институты, собирающие данные для научных и других названных целей, не освобождаются от традиционного обязательства получения полноценного согласия на обработку персональных данных. В связи с этим для научных институтов и других организаций в России тем более была бы ценна имплементация практик альтруистичного управления данными, когда сами носители данных предоставляют возможность использовать их на законных основаниях для публично значимых целей.

---

[27] Enhancing Access to and Sharing of Data… https://www.oecd.org/publications/enhancing-access-to-and-sharing-of-data-276aaca8-en.htm.

Реализации Рекомендации ОЭСР о беспрепятственном доступе к данным независимо от юрисдикции в российском праве может препятствовать требование локализации данных[28]. Хотя международные эксперты допускают необходимость применения государством требования локализации данных из соображений информационной безопасности страны или отдельных секторов экономики, подчеркиваются негативные экономические эффекты такой меры, например ограничение доступа на рынок обработки данных иностранных поставщиков и как следствие — снижение конкуренции и высокие тарифы [Ursic et al., 2018].

В настоящее время в России требование локализации не сопряжено с дополнительными ограничениями на трансграничную передачу данных. Однако рассматриваются варианты введения иных ограничений на потоки данных «в целях защиты прав российских граждан». Так, в марте 2021 года Роскомнадзор сообщал о планах предложить законодательно ограничить передачу персональных данных путем введения определенных правил их трансграничной передачи. По мнению регулирующего органа, такое решение позволило бы обеспечить необходимый уровень защиты персональных данных на иностранных цифровых площадках без специальных соглашений регулирующих органов об экстерриториальном действии российского правового режима данных[29]. Но дальше публичной декларации дело не пошло, соответствующий законопроект о поправках в ФЗ-152 подготовлен не был. Ввиду действующего требования локализации данных иностранные провайдеры в России вынуждены пользоваться услугами российских центров обработки данных. Представляется более целесообразным уточнить требование локализации данных — например, установить его для персональных данных более высокого класса защищенности или чувствительных данных, таких как биометрические.

Для повышения доступности данных в частном секторе российским регуляторам следует рассмотреть несколько рекомендаций международных экспертов ОЭСР.

Во-первых, публичные институты могут разрабатывать руководства по договорам об обработке и передаче данных (*contract guidelines*). Так, японское Министерство экономики, торговли и промышленности в 2018 году выпустило Руководство по договорам об использовании данных и технологий искусственного интеллекта[30]. Государственное ведомство определяет оптималь-

---

[28] Mapping Approaches to Data and Data Flows. Report for the G20 Digital Economy Task Force. 2020. https://www.oecd.org/sti/mapping-approaches-to-data-and-data-flows.pdf.

[29] *Черноусов И.* Роскомнадзор предлагает расширить действие закона о персональных данных // Российская Газета. 2021. 23 марта. https://rg.ru/2021/03/23/roskomnadzor-predlagaet-rasshirit-dejstvie-zakona-o-personalnyh-dannyh.html.

[30] https://www.meti.go.jp/english/press/2019/0404_001.html.

ные параметры оборота данных, позволяя участникам корректировать условия [Shimpo, 2018]. Но такие руководства могут создаваться и на уровне бизнес-инициатив, например инициатива модельных соглашений по обмену данными среди нидерландских компаний (Dare 2 Share Cooperation Agreement)[31].

Во-вторых, необходимо создавать партнерства для обмена данными, включая публично-частные партнерства (*data sharing partnerships*). Такие партнерства могут реализовываться и в формате цифровых платформ, подлежащих сертификации на соответствие условиям безопасности обмена данными. Например, в Японии разработана своя система сертификации платформ для обмена данными, предусматривающая процедуру запроса со стороны компаний данных от государственных ведомств (*data request system*)[32].

В-третьих, важно определять категории частных данных, представляющих публичный интерес (*private sector data for public interest purposes*). Например, во Франции закон цифровой республики (*Loi pour une République numérique*) включил в данные публичного интереса данные частного сектора, связанные с публичными услугами, такими как коммунальные и транспортные, а также данные, необходимые для национальной статистики[33]. Подобные инициативы уже реализованы в Австралии, Финляндии и других странах ОЭСР.

Большой интерес к таким инструментам обусловлен их доступностью для реализации. К тому же подобные инициативы органично вписываются в систему международных стандартов, отраженных в рекомендации ОЭСР 2021 года. Однако важно понимать, что использование тех или иных инициатив возможно только при соответствующем уровне регулирования самих данных. Поэтому решение задачи повышения доступа к данным и совершенствования передачи данных в России следует начинать с устранения выявленных пробелов в режиме их регулирования.

Заключение

Задача улучшения регулирования данных в России стоит в повестке российских профильных ведомств (Роскомнадзора, Минцифры) в рамках работы по развитию цифровой экономики страны. Однако для принятия эффективных мер повышения до-

---

[31] Ministry of Economic Affairs and Climate Policy. Dutch Digitalisation Strategy. Dutch Vision on Data Sharing between Businesses. February 2019. P. 24. https://www.permanentrepresentations.nl/documents/publications/2020/01/06/dutch-vision-on-data-sharing-between-businesses.

[32] Enhancing Access to and Sharing of Data… https://www.oecd.org/publications/enhancing-access-to-and-sharing-of-data-276aaca8-en.htm.

[33] *Paggi F.* Ce que la loi "Lemaire" change pour les collectivités territoriales. Analyse Juridique. 2017. 8 Mai. https://www.seban-associes.avocat.fr/wp-content/uploads/2017/05/Ce_que_la_loi_Lemaire_change_pour_les_collectivites_territoriales.pdf. (In Franc.)

ступа к данным и их передачи в соответствии с международными стандартами, такими как Рекомендация EASD 2021 года, или зарубежными практиками, такими как механизмы, представленные в Регламенте ЕС об управлении данными, необходимо обеспечить базовые условия защиты данных и правовой режим участников их обмена. Для развития надежной экосистемы данных следует укрепить права субъектов персональных данных путем внесения соответствующих поправок в ФЗ-152 «О персональных данных», прежде всего в части уточнения целевого характера их обработки, определения конкретных форм предоставления согласия на обработку, закрепления права на их перенос. Для имплементации рекомендаций по развитию прозрачных конкурентных цифровых рынков необходимо внести законодательные поправки в ФЗ-152 в части уточнения обязательств оператора данных, прежде всего введения обязательства уведомления субъектов персональных данных о нарушении режима обработки персональных данных, а также в части ограничения требования о локализации персональных данных российских граждан на территории страны. На уровне рекомендательных норм Роскомнадзор может разрабатывать руководства по обработке и передаче данных, включая в них модельные оговорки по гарантиям безопасности, содействовать образованию публично-частных партнерств по обмену данными, включая создание специализированных платформ. Для повышения эффективности действующего проекта www.data.gov.ru необходимо определить виды данных, которые представляли бы практический интерес для российских компаний и могли быть доступны публично. В число таких данных могут войти сведения об уровне заболеваемости различными болезнями и результатах лечения, о циклах потребления энергии и водных ресурсов, о пассажиропотоках на маршрутах в конкретных населенных пунктах и др. Принятие таких мер, как внесение некоторых законодательных поправок и разработка рекомендаций по доступу и обороту данных из частного сектора, позволит России постепенно построить надежную конкурентную цифровую экономику, где можно имплементировать зарубежные практики и разрабатывать новые уникальные механизмы повышения доступа к данным и их передачи.

Литература

1. *Абрамова А. Г.* Современные проблемы осуществления защиты персональных данных в сети: основополагающие принципы защиты персональных данных // Регион и мир. 2020. Т. 11. № 4. С. 21–25.
2. *Бембеева Б. С.* Право на защиту персональных данных и различные категории персональных данных // Право в сфере Интернета: сборник статей / Отв. ред. М. А. Рожкова. М.: Статут, 2018. С. 48–61.

3. *Гадельшин А. А., Степанов М. М.* Cookie-файлы как объект персональных данных и способ нарушения конфиденциальности персональных данных // Вопросы российской юстиции. 2021. № 16. С. 516–531.
4. *Мамыкина Е. В.* Правовой статус субъектов, участвующих в персональных данных: субъект персональных данных; оператор персональных данных // Моя профессиональная карьера. 2020. Т. 3. № 11. С. 117–122.
5. *Петренко В. И., Суховей Д. Н.* Механизм подачи уведомления регулирующему органу и субъекту персональных данных в связи с нарушением безопасности персональных данных // Наукоемкие технологии в космических исследованиях Земли. 2012. Т. 4. № 2. С. 23–25.
6. *Braun C., Busuioc M.* Stakeholder Engagement as a Conduit for Regulatory Legitimacy? // Journal of European Public Policy. 2020. Vol. 27. No 11. P. 1599–1611.
7. *Busuioc M., Jevnaker T.* EU Agencies' Stakeholder Bodies: Vehicles of Enhanced Control, Legitimacy or Bias? // Journal of European Public Policy. 2022. Vol. 29. No 2. P. 155–175.
8. *Graef I., Prüfer J.* Governance of Data Sharing: A Law & Economics Proposal // Research Policy. 2021. Vol. 50. No 9.
9. *Hansen M.* Towards Measuring Maturity of Privacy-Enhancing Technologies // Privacy Technologies and Policy: Third Annual Privacy Forum, APF 2015 / B. Berendt, T. Engel, D. Ikonomou, D. Le Métayer, S. Schiffner (eds.). New York, NY: Springer, 2016. P. 3–20.
10. *Koops E. J.* Should ICT Regulation Be Technology-Neutral? // Starting Points for ICT Regulation / B. J. Koops, A. M. B. Lips, J. E. J. Prins, M. H. M. Schellekens (eds.). Hague: TMC Asser Press, 2006. P. 77–108.
11. *Lovelock P.* Framing Policies for the Digital Economy: Towards Policy Frameworks in the Asia-Pacific. Singapore: UNDP Global Centre for Public Excellence, 2018.
12. *Park K. B., Kang M.* South Korea—Data Protection Overview. 2021. https://www.dataguidance.com/notes/south-korea-data-protection-overview.
13. *Reinsel D., Gantz G., Rydning J.* The Digitalization of the World: From Edge to Core. 2018. https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf.
14. *Shabani M.* The Data Governance Act and the EU's Move Towards Facilitating Data Sharing // Molecular Systems Biology. 2021. Vol. 17. No 3. 2021.
15. *Shimpo F.* The Principal Japanese AI and Robot Strategy Towards Establishing Basic Principles // Research Handbook on the Law of Artificial Intelligence / W. Barfield, U. Pagallo (eds.). Cheltenham: Edward Elgar Publishing, 2018. P. 114–142.
16. *Tusikov N., Haggart B.* Implementing a National Data Strategy: The Need for Innovative Public Consultations. 2020. https://www.g20-insights.org/policy_briefs/implementing-a-national-data-strategy-the-need-for-innovative-public-consultations/.
17. *Ursic H., Nurullaev R., Cuevas M., Szulewski P.* Data Localisation Measures and Their Impacts on Data Science // Research Handbook in Data Science and Law / V. Mak, E. Tjon Tjin Tai, A. Berlee (eds.). Cheltenham: Edward Elgar Publishing, 2018. P. 322–353.
18. *Veil W.* Data Altruism: How the EU is Screwing up a Good Idea. 2022. https://algorithmwatch.org/en/eu-and-data-donations/.

References

1. Abramova A. G. Sovremennye problemy osushchestvleniya zashchity personal'nykh dannykh v seti: osnovopolagayushchie printsipy zashchity personal'nykh dannykh [Modern Problems in Personal Data Protection on the Internet: Fundamental Principles of Personal Data Protection]. *Region i mir [Region and World],* 2020, vol. 11, no. 4, pp. 21-25. (In Russ.)
2. Bembeeva B. S. Pravo na zashchitu personal'nykh dannykh i razlichnye kategorii personal'nykh dannykh [The Right to Protection of Personal Data and Different Categories of Data]. In: Rozhkova M. A. (ed.). *Pravo v sfere Interneta: sbornik statey [Law Concerning the Internet: A Collection of Essays].* Moscow, Statut, 2018, pp. 48-61. (In Russ.)

3. Gadelshin A. A., Stepanov M. M. Cookie-fayly kak ob"ekt personal'nykh dannykh i sposob narusheniya konfidentsial'nosti personal'nykh dannykh [Cookie-Files as an Object of Personal Data and a Method for Breaching Privacy]. *Voprosy rossiykoy yustitsii [Questions of Russian Justice]*, 2021, no. 16, pp. 516-531. (In Russ.)
4. Mamykina E. V. Pravovoy status sub"ektov, uchastvuyushchikh v personal'nykh dannykh: sub"ekt personal'nykh dannykh; operator personal'nykh dannykh [The Legal Status of Participants in Data Circulation: Personal Data Holder; Personal Data Operator]. *Moya professional'naya kar'era [My Professional Career]*, 2020, vol. 3, no. 11, pp. 117-122. (In Russ.)
5. Petrenko V. I., Sukhovey D. N. Mekhanizm podachi uvedomleniya reguliruyushchemu organu i sub"ektu personal'nykh dannykh v svyazi s narusheniem bezopasnosti personal'nykh dannykh [Method for Submitting Notification Concerning Violation of Personal Data Security to a Regulatory Body and to the Personal Data Subject]. *Naukoemkie tekhnologii v kosmicheskikh issledovaniyakh Zemli [Science-Driven Technologies in Space Research of the Earth]*, 2012, vol. 4, no. 2, pp. 23-25. (In Russ.)
6. Braun C., Busuioc M. Stakeholder Engagement as a Conduit for Regulatory Legitimacy? *Journal of European Public Policy,* 2020, vol. 27, no. 11, pp. 1599-1611. DOI:10.1080/13501763.2020.1817133.
7. Busuioc M., Jevnaker T. EU Agencies' Stakeholder Bodies: Vehicles of Enhanced Control, Legitimacy or Bias? *Journal of European Public Policy,* 2022, vol. 29, no. 2, pp. 155-175. DOI:10.1080/13501763.2020.1821750.
8. Graef I., Prüfer J. Governance of Data Sharing: A Law & Economics Proposal. *Research Policy,* 2021, vol. 50, no. 9. DOI:10.1016/j.respol.2021.104330.
9. Hansen M. Towards Measuring Maturity of Privacy-Enhancing Technologies. In: Berendt B., Engel T., Ikonomou D., Le Métayer D., Schiffner S. (eds.). *Privacy Technologies and Policy: Third Annual Privacy Forum, APF 2015.* New York, NY, Springer, 2016, pp. 3-20.
10. Koops E. J. Should ICT Regulation Be Technology-Neutral? In: Koops B. J., Lips A. M. B., Prins J. E. J., Schellekens M. H. M. (eds.). *Starting Points for ICT Regulation.* The Hague, TMC Asser Press, 2006, pp. 77-108.
11. Lovelock P. *Framing Policies for the Digital Economy: Towards Policy Frameworks in the Asia-Pacific.* Singapore, UNDP Global Centre for Public Excellence, 2018.
12. Park K. B., Kang M. *South Korea - Data Protection Overview.* 2021. https://www.dataguidance.com/notes/south-korea-data-protection-overview.
13. Reinsel D., Gantz G., Rydning J. *The Digitalization of the World: From Edge to Core.* 2018. https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf.
14. Shabani M. The Data Governance Act and the EU's Move Towards Facilitating Data Sharing. *Molecular Systems Biology,* 2021, vol. 17, no. 3, 2021. DOI:10.15252/msb.202110229.
15. Shimpo F. The Principal Japanese AI and Robot Strategy Towards Establishing Basic Principles. In: Barfield W., Pagallo U. (eds.). *Research Handbook on the Law of Artificial Intelligence.* Cheltenham, Edward Elgar Publishing, 2018, pp. 114-142.
16. Tusikov N., Haggart B. *Implementing a National Data Strategy: The Need for Innovative Public Consultations.* 2020. https://www.g20-insights.org/policy_briefs/implementing-a-national-data-strategy-the-need-for-innovative-public-consultations/.
17. Ursic H., Nurullaev R., Cuevas M., Szulewski P. Data Localisation Measures and Their Impacts on Data Science. In: Mak V., Tjon Tjin Tai E., Berlee A. (eds.). *Research Handbook in Data Science and Law.* Cheltenham, Edward Elgar Publishing, 2018, pp. 322-353. DOI:10.4337/9781788111300.00021.
18. Veil W. *Data Altruism: How the EU is Screwing up a Good Idea.* 2022. https://algorithmwatch.org/en/eu-and-data-donations/.