Вестник международных организаций. 2023. Т. 18. № 1. С. 7–32
Научная статья
УДК 327.7:004.6
doi:10.17323/1996-7845-2023-01-01

Возможно ли лидерство «Группы двадцати» по вопросам управления данными? Есть ли шанс на сближение подходов?[1]

М.В. Ларионова, А.В. Шелепов

Ларионова Марина Владимировна – д.полит.н., директор Центра исследований международных институтов (ЦИМИ) Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации (РАНХиГС); Россия, 119034, Москва, Пречистенская наб., д. 11; larionova-mv@ranepa.ru

Шелепов Андрей Владимирович – к.э.н., с.н.с. Центра исследований международных институтов (ЦИМИ) Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации (РАНХиГС); Россия, 119034, Москва, Пречистенская наб., д. 11; shelepovav@ranepa.ru

Аннотация

Данные – неисчерпаемый ресурс, новая форма капитала в экономике знаний. В условиях отсутствия регулирования данных глобальные технологические корпорации стремятся расширить свое влияние на всех этапах цепочек связанных с данными процессов и используют свою рыночную силу для выстраивания монополий. Данные могут быть источником не только прибыли технологических гигантов, но также и социальной ценности. Однако рыночные силы сами по себе не обеспечивают создание общественных благ на основе данных. Для этого на уровне стран требуются усилия государства, а на международном уровне – сотрудничество государств и международных организаций. Несмотря на многочисленные инициативы по созданию механизмов координации и общих подходов к регулированию данных, взаимодействие по вопросам управления данными сильно фрагментировано и находится в тупике из-за противоречий и жесткой конкуренции между ключевыми участниками. Одним из ключевых объектов разногласий является подход к регулированию трансграничного перемещения данных.

В статье рассматриваются противоречия между практиками регулирования данных ключевых игроков цифровой экономики, прежде всего США, ЕС и Китая, и подходами, продвигаемыми ими в рамках международных институтов (ВТО, «Группы двадцати», «Группы семи», ОЭСР). Особое внимание уделяется повестке «Группе двадцати» по управлению данными и Инициативе «двадцатки» по «свободному потоку данных с доверием», проблемам ее реализации и рискам стагнации сотрудничества. В заключительном разделе представлены риски и перспективы возможных сценариев дальнейшего развития сотрудничества по регулированию данных, в том числе создания «Группой двадцати» Совета по цифровой экономике и данным, реализации инициативы «Группы семи» по формированию глобального цифрового порядка, усиления сотрудничества членов «Группы семи» и углубления взаимодействия в рамках ОЭСР, реализации предложения ЮНКТАД по формированию многоуровневой распределенной полицентрической модели управления данными при центральной роли ООН. Авторами сформулировано предложение по развитию сотрудничества БРИКС, направленного на создание инклюзивного многостороннего регулирования данных.

Ключевые слова: управление данными, «Группа двадцати», локализация, свободные потоки данных

Благодарности: статья подготовлена в рамках выполнения научно-исследовательской работы государственного задания РАНХиГС.

---

[1] Статья поступила в редакцию 15.07.2022.

Для цитирования: Ларионова М.В., Шелепов А.В. Возможно ли лидерство «Группы двадцати» по вопросам управления данными? Есть ли шанс на сближение подходов? // Вестник международных организаций. 2023. Т. 18. № 1. С. 7–32 (на русском и английском языках). doi:10.17323/1996-7845-2023-01-01

Введение. Проблема регулирования данных

Данные – новая форма капитала в экономике знаний, ресурс не только для информационных, но и для всех остальных секторов современной экономики. Общепринятой стала характеристика данных как кровеносной системы экономики и торговли [OECD, 2019a], неисчерпаемого ресурса, который можно использовать неограниченное количество раз и неограниченным количеством пользователей [OECD, 2015]. Данные имеют ценность не сами по себе, она генерируется в результате их использования. Социальная и экономическая ценность данных в основном извлекается на двух этапах цепочки связанных с данными процессов: при трансформации в знание (через анализ) и при использовании знания для принятия решений. Ценность данных зависит от своевременности обработки и использования. Для конвертации данных в информацию и знания, которые затем используются в качестве продукта, нужны технологии, включая, например, программное обеспечение, искусственный интеллект. Это означает, что для эффективного использования данных по всей цепочке нужно их движение, в том числе между странами [OECD, 2020].

Исследования показывают, что повышение доступности и активизация обмена данных могут создать дополнительные экономические и социальные выгоды в объеме от 0,1 до 1,5% ВВП в случае данных государственного сектора и от 1 до 2,5% ВВП при включении в эти процессы также данных частного сектора [OECD, 2019b]. При этом остается вопрос о том, какие субъекты выигрывают в большей степени. Повышение доступности и усиление обмена могут создавать дополнительные выгоды для держателей данных (прямое воздействие), от 10 до 20 раз больше выгод для пользователей (косвенное воздействие) и от 20 до 50 раз больше – для экономики (также косвенное воздействие). Однако в некоторых случаях повышение доступности и усиление обмена могут и снижать выгоды от производства данных для держателей данных [OECD, 2020].

Для ответа на вопрос о том, кто выигрывает, необходимо иметь оценки объемов потоков данных, направления их движения (экспорта и импорта), структуры («сырые» данные – продукты данных) и стоимости, но надежной статистики по этому вопросу пока нет [UNCTAD, 2021, p. 18–21]. Прояснение вопроса о распределении выгод и рисков может помочь в оценке преимуществ различных подходов к регулированию трансграничных потоков данных. Работу по оценке потоков и их экономической стоимости еще предстоит проделать. Однако известно, что потоки «сырых» данных направлены из менее технологически развитых стран в страны, имеющие конкурентные технологические и компетентностные преимущества. Развивающиеся страны в основном являются источниками «сырых» данных, обрабатываемых и преобразуемых в продукты (информацию) в дата-центрах развитых стран, а затем платят за получаемую обратно информацию. Создается новая модель разделения труда в цепочках данных цифровой экономики, модель центра и периферии [Rikap, 2021].

Данные являются не только источником прибыли для технологических гигантов, но также могут формировать и социальную ценность (social value). Однако рыночные

силы сами по себе не обеспечивают создания общественных благ на основе данных. Для этого на уровне стран требуются усилия государства, а на международном уровне – сотрудничество государств и международных организаций. Нельзя сказать, что такое сотрудничество не осуществляется. Регулирование, направленное на защиту данных и содействие их свободному потоку, имеет долгую историю. Сложилось несколько типов инструментов такого регулирования:

– многосторонние рамочные инструменты мягкого права (Руководство по защите конфиденциальности и трансграничных потоков личных данных ОЭСР, Правила трансграничной передачи персональных данных АТЭС, Рамочное соглашение АСЕАН по защите персональных данных);

– многосторонние обязательные инструменты (Конвенция о кибербезопасности и защите личных данных Африканского союза (Конвенция Малабо), Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Конвенция 108) Совета Европы);

– торговые соглашения, содержащие положения о защите и трансграничной передаче данных, и соглашения о цифровой торговле, обязательные к исполнению для экономик-участниц;

– односторонние инструменты (регулирование в рамках национального и наднационального права, например Общий регламент по защите данных ЕС).

Несмотря на многочисленные инициативы по созданию механизмов координации, взаимодействие по вопросам управления данными сильно фрагментировано и значительно тормозится из-за противоречий и жесткой конкуренции между ключевыми участниками. Одно из ключевых разногласий связано с подходом к регулированию трансграничного перемещения данных. По уровню открытости трансграничных потоков данных национальные режимы регулирования можно разделить на три типа.

– Свободные (free-flow) (подразумевают полную свободу движения данных и последующую ответственность (ex-post accountability) в случае ненадлежащего использования данных)[2].

– Обусловленные гарантиями защитных мер (flow conditional on safeguards) (защитные меры могут включать решение об адекватности или эквивалентности условий защиты другой страны, применение стандартных контрактных обязательств или обязательных корпоративных правил. Условия трансграничной передачи данных могут включать получение согласия субъекта данных, исполнение соглашения, требующего предоставления данных, необходимость удовлетворения общественных интересов, передачу данных в рамках правового сотрудничества, необходимость защиты жизненных интересов субъекта и др.)[3].

– Ограниченные или обусловленные получением разрешений по конкретным случаям (flow conditional on ad-hoc case-by-case authorization) (такой режим относится, как правило, к персональным данным и «чувствительным» (sensitive) данным конкретных секторов или к данным, связанным с обеспечением национальной безопасности[4]) [Casalini, López González, 2019].

В условиях противоречий между ключевыми игроками, особенно США и Китаем, и отсутствия согласованного регулирования глобальные технологические корпора-

[2] Такой режим применяют, например, Гана, Филиппины и Сингапур.

[3] С разной степенью жесткости условий такой режим реализуется Аргентиной, Бразилией (законопроект), ЕС, Великобританией, Египтом, Марокко, Тунисом, ЮАР, Израилем, Японией, Таиландом.

[4] Такой режим применяют для некоторых типов данных Австралия, Новая Зеландия, Швейцария, Франция, Германия, Бельгия, Южная Корея.

ции стремятся расширить свои экосистемы данных и влияние. Цифровые платформы являются крупнейшими бенефициарами на всех этапах цепочек данных. Они заинтересованы в свободных потоках, чтобы монетизировать данные с максимальными выгодами для себя, и, соответственно, используют свою рыночную силу для выстраивания монополий и финансовые возможности для лоббирования в конгрессе США и органах ЕС, а также через экспертные центры [UNCTAD, 2021, p. 27–28]. Не стоит забывать, что цифровую торговую повестку США в основном формулировали Google, Business Software Alliance и другие технологические гиганты [Azmeh, Foster, Echavarri, 2020]. Крупнейшие компании инвестируют в искусственный интеллект, технологии 5G, а также развитие инфраструктуры, в том числе наземные сети, подводные кабели, спутниковую широкополосную связь, точки обмена интернет-трафиком (IXPs), гиперцентры данных. Инвестиции корпораций в инфраструктуру, покупки стартапов и конкурентов в развивающихся странах создают угрозы нового колониализма [Elmi, 2020].

Чтобы преодолеть серьезные экономические и социальные последствия монополии цифровых платформ, выстраивающих под себя цифровые рынки, сформировать регулирование трансграничных цифровых корпораций, включая конкурентную политику и налогообложение, необходимо инклюзивное сотрудничество с участием развивающихся стран. Однако ввиду противоречий между ключевыми участниками текущее состояние диалога по международной модели регулирования можно охарактеризовать как фактически тупиковое.

Противоречия между ключевыми игроками

Три крупнейших центра цифровой экономики – США, ЕС и Китай – реализуют три различные модели регулирования, отражающие фундаментальные различия в подходах конкурентов на глобальном цифровом рынке. Приоритетом США является свобода трансграничных потоков данных, запрет на локализацию и минимальное регулирование (дерегулирование) с использованием модели саморегулирования и наилучших практик. В концепции США данные – товар, на экспорт которых не должно налагаться ограничений. Приоритеты ЕС – защита конфиденциальности и свобода потоков данных при условии обеспечения прозрачного регулирования и адекватного уровня защиты, включая принятие и применение правил трансграничного трансфера для защиты персональных данных и конфиденциальности как фундаментального права граждан. При этом существует противоречие между обязательством по защите персональных данных в соответствии со ст. 8 Хартии ЕС о фундаментальных правах, Регламентом по защите персональных данных Европейского союза [EU, 2016] и обязательствами ЕС по либерализации торговли и обеспечению свободы потоков данных [Yakovleva, 2020]. Приоритетом Китая остается киберсуверенитет[5], безопасность данных и, соот-

[5] Суверенитет данных имеет много определений. Ключевые два касаются суверенитета государства и граждан. Так, суверенитет данных определяется как контроль государства над данными в рамках национальной юрисдикции. Может включать также контроль за данными, сгенерированными на территории юрисдикции, но хранящимися или обрабатываемыми иностранными облачными сервисами. В этом случае экстерриториальный контроль должен осуществляться на основе получения полномочий в рамках международного права или с согласия иностранного государства. Понятие суверенитета данных также используется в отношении права и возможности граждан осуществлять контроль над своими данными. См. [Hummel et al., 2021].

Цифровой суверенитет также имеет много определений, примечательно определение в применении к ЕС: «Цифровой суверенитет означает способность Европы действовать независимо в циф-

ветственно, жесткое регулирование, предполагающее требования локализации и осторожное отношение к концепции свободного потока данных[6].

Противоречия определяются национальными практиками регулирования и различиями в коммерческих интересах. Большинство американских цифровых гигантов специализируются на цифровых услугах, крупнейшие китайские – на цифровых услугах и товарах. Соответственно, США акцентируют в переговорах по электронной коммерции цифровые аспекты, а Китай традиционные аспекты регулирования торговли [Gao, 2018]. ЕС, не имеющий собственных технологических гигантов, использует регулирование по защите данных для защиты своего рынка от китайских и американских технологических компаний, то есть прибегает к своего рода «цифровому протекционизму» [Aaronson, 2019].

США [Government of the United States, 2019], ЕС [Titievskaia, 2020] и их партнеры по «Группе семи» продвигают положения о свободных потоках данных и отказе от локализации в рамках региональных и двухсторонних соглашений, а также Инициативы по электронной коммерции в ВТО. Китай участвует в переговорах, выступая против обязательств по свободным потокам данных, отказу от локализации и доступа к кодам источников, хотя последний вопрос в позиции Китая по электронной торговле не упоминается [WTO, 2019]. Индия, ЮАР и Группа африканских государств выступают против включения аспектов регулирования данных в переговоры по электронной коммерции [WTO, 2017].

Многомерная природа данных определяет необходимость их регулирования за рамками торговых переговоров и соглашений. Последствия трансграничных потоков данных выходят далеко за пределы торговых вопросов и затрагивают не только экономику и общество, но и безопасность. Кроме того, увязка условий регулирования данных с доступом к рынкам развитых стран создает дополнительные риски для развивающихся стран быть «запертыми» в рамках соглашений, последствия которых могут быть невыгодны для них в будущем и которые пока сложно оценить. Подписываясь под статьями торговых соглашений о свободных потоках данных и запрете локализации развивающиеся страны теряют возможность использовать свой ресурс – данные – для создания дополнительной стоимости.

Существует проблема учета трансграничных данных. Входящие и исходящие потоки данных отличаются от международных торговых потоков. Есть также проблема различий между потоками «сырых» данных и продуктов данных, которые могут рас-

---

ровом мире и должен пониматься в терминах механизмов защиты и инструментов наступления для продвижения цифровых инноваций». См. [Madiega, 2020].

Кибер-суверенитет (также информационный суверенитет или суверенитет данных) определяется как запрет нежелательного влияния в информационном пространстве страны и перенос управления интернетом из многостороннего форума в межгосударственный институт, такой как ООН. См. [Aaronson, 2019].

[6] Хотя Китай вместе с другими членами Всестороннего регионального экономического партнерства (ВРЭП) поставил свою подпись под положениями не требовать локализации компьютерной техники на территории страны как условия ведения коммерческой деятельности и участвует в переговорах по Совместной инициативе по электронной торговле в ВТО, китайская модель регулирования трансграничных потоков имеет весьма ограничительный характер. В настоящее время Китай завершает работу над национальной системой контроля и защиты данных, которая предполагает, что для их трансграничной передачи должны быть выполнены определенные условия, включая оценку безопасности со стороны правительственных органов, и вводится требование локализации: все операторы критической информационной инфраструктуры, понимаемой весьма широко, и установленные законом процессоры личной информации должны хранить личную информацию, собранную ими, на территории страны.

сматриваться как торговля услугами. В результате трансграничные потоки данных должны рассматриваться в рамках более широкого, интегрированного и сбалансированного формата [UNCTAD, 2021, p. 145–147]. В настоящее время мы имеем ситуацию, когда взаимодействие осуществляется в ООН, ВТО, «Группе двадцати», «Группе семи», ОЭСР, АТЭС, АСЕАН и других региональных и двухсторонних форматах. Однако перспективы конкретных сбалансированных и инклюзивных договоренностей пока не просматриваются.

Одновременно в условиях растущих геополитических противоречий и информационных войн растут недоверие и риски злоупотребления и злонамеренного использования данных. Соответственно, возрастает стремление защитить конфиденциальность усилением обусловленности трансграничного трансфера данных и/или требованием хранения и обработки в конкретных границах. Экономические и геополитические риски вынуждают многие страны[7] принимать меры по локализации данных[8]. Развивающиеся страны, не имеющие достаточных институциональных и бюрократических ресурсов для обеспечения защиты требованиями обусловленности, аналогичными европейским, рассматривают локализацию как «одно из средств обеспечения суверенитета данных (data sovereignty, digital sovereignty) в условиях, когда экстерриториальность позволяет доминирующим государствам навязывать свои законы миру, а правовые подходы развитых стран воспроизводятся до такой степени, что оказывают воздействие на суверенитет и самоопределение развивающихся стран» [Internet & Jurisdiction Policy Network, 2019]. Целью такого регулирования является сохранение контроля за данными, обеспечение кибербезопасности, национальной безопасности, киберустойчивости, защиты конфиденциальности, доступа государства к определенным категориям данных и, соответственно, создание условий для обеспечения применения национального законодательства, а также экономических конкурентных преимуществ [OECD, 2020].

США, ЕС и их партнеры по «семерке» и ОЭСР выступают против локализации. В части, касающейся безопасности, используется технологическая аргументация: локализация – только один из факторов безопасности, и безопасность и защита могут быть обеспечены за счет соответствующих технологий и программного обеспечения, например сегментирования (sharding). Новые технологии, в частности блокчейн, имеют децентрализованную природу, и, соответственно, локализация противоречит их развитию. Локализация не обеспечивает суверенитет в силу трансграничного характера природы интернета [Cory, Dascoli, 2021].

С экономической точки зрения конкурентные преимущества и экономические выгоды от локализации недостаточно обоснованы. Локализация создает риски фрагментации интернета, формируя различные требования к контролерам, вынужденным нести затраты на соблюдение негармонизированных требований [Drake, Cerf, Kleinwächter, 2016]. Стоимость локализации может быть высокой в результате затрат на создание инфраструктуры и труд, затрат на соблюдение требований регулирования и неэффективных расходов, финансовых потерь от недополученных налогов, ограничения конкуренции и стимулов для инноваций [Svantesson, 2020, p. 16]. При этом отсутствуют оценки стоимости локализации присутствия или представительства, требуе-

[7] Среди них Кения, Нигерия, Турция, Китай, Индия, Пакистан, Индонезия, Вьетнам, Россия, Саудовская Аравия, ОАЭ.

[8] Обязательные законодательные или административные «требования, прямо или косвенно стимулирующие хранение или обработку данных, исключительно или не исключительно, в определенной юрисдикции». См. [Svantesson, 2020, p. 8].

мого, например, Регламентом ЕС 2016/679, которая может быть весьма существенной и даже запретительной для предприятий из развивающихся стран [Mattoo, Meltzer, 2018].

В качестве идеологического аргумента против локализации используется вменение мотивации. Так, Федеральный закон от 21 июля 2014 г. № 242-ФЗ о хранении персональных данных вызвал глубокую озабоченность, что его реальной мотивацией является использование данных в качестве инструмента политических репрессий [Garrie, Byhovsky, 2017]. Аналогичную озабоченность вызвал Закон о кибербезопасности КНР, а именно ст. 37. При этом требования локализации Австралии, Великобритании, Германии, Дании, Бельгии, Финляндии, Швеции в отношении конкретных типов данных (паспортные данные, секторальные данные, финансовая информация) не рассматриваются как ограничения [Selby, 2017].

В рамках правовой логики доказывается, что требование локализации является отличным от требований, предписывающих обеспечение определенного уровня защиты или стандарта кибербезопасности как условие трансграничного перемещения данных. Утверждается, что хотя такие требования ограничивают хранение или обработку, они не обязательно являются правилами локализации. Условия, налагаемые на трансграничное перемещение, – не то же самое, что запрет. Если требования обусловленного экспорта данных являются настолько высокими, что, по сути, составляют абсолютное ограничение на экспорт данных, эквивалентный обязательному законодательному или административному требованию локализации, косвенно стимулируя хранение и обработку данных в рамках конкретной юрисдикции, то это требование может подпадать под определение локализации данных. Предлагается различать четыре типа требований: 1) запреты; 2) требования (защиты в третьей стране реципиенте); 3) неопределенность регулирования; 4) стимулы. Запреты предлагается однозначно рассматривать как локализацию, а требования – только в случае, если они не удовлетворяют принципу пропорциональности в соответствии с §18 Руководства ОЭСР по защите конфиденциальности и трансграничных потоков личных данных: «Любые ограничения должны быть пропорциональны рискам, учитывать чувствительность данных и контекст обработки» [OECD, 2013].

Пропорциональность предлагается оценивать с учетом законодательства ЕС, нормативной базы ВТО и различных торговых соглашений на основе критериев: 1) способности мер достигнуть поставленной цели; 2) степени ограничения по сравнению с другими возможными мерами; 3) соразмерности вмешательства, создаваемого мерой. Одновременно предлагается дополнить принцип пропорциональности оценкой обоснования страной требования локализации на основе объективного и субъективного стандартов, или prima facie теста, оценивающего заявленные цели, и субъективного теста реальных намерений. При такой оценке страна или регион с «сильными традициями защиты конфиденциальности граждан» может привести сложившуюся традицию в качестве обоснования меры, которая в противном случае могла бы трактоваться как протекционистская и не соответствующая требованию пропорциональности §18 Руководства ОЭСР по защите конфиденциальности и трансграничных потоков личных данных. Напротив, страна, имеющая историю нарушений прав человека, не сможет опровергнуть такую оценку своих мер по локализации [Svantesson, 2020].

В логике этих технологических, экономических, идеологических и правовых аргументов сформулированы рекомендации для дальнейшей работы над документами ОЭСР по защите данных и их трансграничным потокам. Очевидно, что задана тенденция существенного повышения субъективности оценки соответствия мер локализации, предпринимаемых различными странами, принципу пропорциональности. Фактически создается основа для дискриминационного оценивания действий государств,

которые рассматриваются ЕС, США и партнерами по ОЭСР как недемократические. Одновременно для ЕС и стран-партнеров обосновывается возможность применения протекционистских мер как соответствующих традициям и Хартии ЕС о фундаментальных правах.

Анализ практики взаимодействия «Группы двадцати» и ОЭСР, тенденция формирования параметров сотрудничества членов «двадцатки» по вопросам цифровой экономики на основе принципов и подходов ОЭСР, роль ОЭСР в качестве ключевого экспертного института в рабочих органах «двадцатки» [Ларионова, Шелепов, 2021] позволяют предположить, что члены «Группы семи» и ОЭСР будут стремиться продвигать свои подходы и нормы регулирования данных через «Группу двадцати», хотя тенденция к легитимации инструментов ОЭСР через «Группу двадцати» и исчерпывает себя.

Повестка «двадцатки». Инициатива по «свободному потоку данных с доверием»

Вопросы управления данными (защиты и трансграничных потоков данных) интегрированы в повестку «Группы двадцати» с 2019 г. Несмотря на значение данных для развития цифровой экономики, появившаяся в 2016 г. «новая повестка», охватывающая «политику и меры в таких областях, как инновации, новая промышленная революция, цифровая экономика» [«Группа двадцати», 2016a], вопросы данных практически не затрагивала. Коммюнике лидеров и посвященные цифровой повестке документы 2016 г., Контуры инновационного роста «Группы двадцати», План действий в области инноваций, План действий по новой индустриальной революции и Инициатива по развитию и сотрудничеству в области цифровой экономики, сотрудничество в сфере регулирования данных не упоминают, за исключением подтверждения необходимости соблюдения нормативных основ в области неприкосновенности частной жизни и защиты личных данных, а также прав интеллектуальной собственности как важного фактора укрепления доверия и развития цифровой экономики [«Группа двадцати», 2016a; 2016b].

В Гамбургском коммюнике 2017 г. «двадцатка» впервые заявила о поддержке свободного потока «информации при уважении применимых правовых рамок для неприкосновенности частной жизни, защиты данных и прав на объекты интеллектуальной собственности» [«Группа двадцати», 2017a][9]. Формулировка о необходимости свободного потока информации, идей и знаний при соблюдении соответствующих требований законодательства и защиты данных и прав интеллектуальной собственности для создания условий процветания цифровой экономики повторяется практически в неизменном виде в Декларации, согласованной по итогам саммита в Буэнос-Айресе [Group of 20, 2018b], и Декларации министров, ответственных за цифровую экономику, 2018 г. [G20, 2018a]. Но в целом Декларация министров 2018 г. сфокусирована на использовании данных как стратегического ресурса в работе государственного сектора[10] и совершенствовании измерения цифровой экономики, в том числе потоков данных[11].

[9] До этого обязательство было сформулировано в Декларации министров, ответственных за цифровую экономику. В Дорожной карте «Группы двадцати» по цифровизации министрами также было заявлено намерение сотрудничать, для того чтобы «улучшить глобальное цифровое экономическое развитие и преодолеть цифровой разрыв в сфере инфраструктуры, безопасности данных и цифровых навыков» [G20, 2017b].

[10] Приложение 1 к декларации «Принципы цифрового правительства».

[11] Приложение 3 к декларации «Измерение цифровой экономики».

В 2019 г. в рамках председательства Японии в «двадцатке» Синдзо Абэ сформулировал инициативу «свободного потока данных с доверием». По замыслу председательства, «Осакский трек» должен был запустить процесс создания международных норм для эффективного использования данных как источника экономического роста при лидирующей роли «двадцатки» [Prime Minister of Japan and His Cabinet, 2019].

Инициатива задумывалась в русле процессов, развивающихся в международных торговых соглашениях с участием Японии, включающих положения о свободных потоках данных (Всеобъемлющее и прогрессивное соглашение о Транстихоокеанском партнерстве, Соглашение о цифровой торговле Японии и США [OECD, 2020], Соглашение об экономическом партнерстве между ЕС и Японией [European Commission, 2018][12]); в «Группе семи» (в том числе обязательств по свободным потокам данных и защите данных, согласованных в рамках председательства Японии в 2016 г. в Декларации лидеров «семерки» на саммите в Исэ-Сима 2016 [G7, 2016a], заявлении лидеров «семерки» о принципах и действиях в киберсфере [G7, 2016b], Декларации министров, ответственных за ИКТ [G7, 2016c]), в ЕС как влиятельном участнике ОЭСР, «семерки» и торговом партнере Японии (Регламент защиты персональных данных [EU, 2016], Регламент по свободному потоку неперсональных данных [EU, 2018], Стратегия ЕС по данным [European Commission, 2020]), в рамках сотрудничества между ЕС и Японией (Решение ЕС об адекватности режима защиты персональных данных в Японии [EU, 2019]) и в ОЭСР (рекомендации по свободным потокам данных по итогам первой фазы проекта Going Digital “Going Digital: Shaping Policies, Improving Lives” [OECD, 2019c], исследования по регулированию трансграничных потоков данных (профинансировано правительством Японии) [OECD, 2021b]).

Однако каких-либо субстантивных решений по выработке международного режима для эффективного использования данных как источника экономического роста члены «двадцатки» не согласовали. Три документа, принятые в рамках японского председательства, фиксируют общее понимание значения трансграничных потоков данных для устойчивого развития и необходимости защиты конфиденциальности, данных и прав ИС для обеспечения свободных потоков данных. Министры, ответственные за цифровую экономику, в совместном заявлении с министрами торговли подтвердили сформулированную в 2017 г. общую позицию о необходимости уважения международных и национальных правовых рамок для обеспечения доверия и содействия свободным потокам данных и зафиксировали намерение сотрудничать с тем, чтобы способствовать интероперабельности различных правовых рамок [G20, 2019b]. С учетом решающей роли эффективного использования данных как фактора, способствующего экономическому росту, развитию и социальному благополучию, в Декларации лидеров стран «Группы двадцати» сформулировано два обязательства: содействовать международной дискуссии по вопросам мер политики в целях максимального извлечения выгод, связанных с данными, и сотрудничать в целях поощрения совместимости различных правовых рамок [«Группа двадцати», 2019a]. Оба обязательства подтверждены в Осакской декларации лидеров по вопросам цифровой экономики [«Группа двадцати»,

[12] Документ содержит положения о свободном трансфере информации или обработке информации в процессе электронной торговли и предоставлении финансовых услуг, а также праве сторон на защиту персональной информации и конфиденциальности (ч. 8). Часть по цифровой торговле (ч. 2) формулирует общие подходы сторон к необходимости принятия прозрачных и эффективных мер по защите потребителя в электронной торговле в соответствии с законодательством и регулированием сторон (ст. 8.78) и намерение сторон рассмотреть через три года после вступления соглашения в силу потребность включения положений о свободном потоке данных (ст. 8.81).

2019b]. Таким образом, в 2019 г. не удалось начать в рамках «двадцатки» процесс создания международного режима для эффективного использования данных как источника экономического роста. Не удалось также интегрировать в «двадцатку» решения и нормы, согласованные ранее в ОЭСР и «семерке», как это было, например, с Планом действий по борьбе с размыванием налогооблагаемой базы и перемещением прибыли (BEPS) в 2013 г., Принципами корпоративного управления в 2015 г. или Принципами «Группы двадцати» в области развития искусственного интеллекта (ИИ) в 2019 г. По сути, результатом инициативы стала договоренность о диалоге по использованию потенциала данных для устойчивого роста.

В условиях пандемии и необходимости мобилизации цифровых технологий для защиты населения и укрепления систем здравоохранения на экстренном саммите лидеры «двадцатки» приняли обязательство задействовать цифровые технологии для укрепления национальных, региональных и глобальных возможностей противодействия потенциальным вспышкам инфекционных заболеваний и обмениваться эпидемиологическими и клиническими данными, необходимыми для исследований и разработок средств диагностики, лечения и вакцин [«Группа двадцати», 2020b].

Соответственно, в апреле 2020 г. министры «Группы двадцати», ответственные за цифровую экономику, обозначили в качестве одного из приоритетов сотрудничества сбор, обработку и обмен надежными и точными неперсональными данными для мониторинга, понимания и предотвращения дальнейшего распространения COVID-19 и других инфекционных заболеваний, а также обеспечение сбора и обработки данных с соблюдением принципов этики, прозрачности, безопасности, интероперабельности и защиты конфиденциальности [G20, 2020b]. Прогресса в формировании общих подходов по потокам данных вновь не произошло. В июле 2020 г. министры, по сути, вернулись к формулировкам 2019 г., подтвердив значение свободных потоков данных с доверием и трансграничных потоков для экономического роста, развития и социального благополучия, а также готовность сотрудничать в целях достижения совместимости различных правовых рамок. В качестве первых шагов на этом направлении договорились об обмене опытом и лучшими практиками и выявлении общих подходов и инструментов [Ibid.].

В Эр-Риядской декларации лидеров «Группы двадцати» конкретные решения также отсутствуют. Направление дальнейших совместных действий определено в очень расплывчатом виде: «Мы признаем важность свободного перемещения данных на условиях доверия и трансграничных потоков данных. Мы выступаем за содействие формированию открытой, справедливой и недискриминационной среды, а также за защиту и расширение прав и возможностей потребителей при одновременном решении проблем, связанных с обеспечением неприкосновенности частной жизни, защиты данных, защиты прав интеллектуальной собственности и обеспечения безопасности. За счет решения этих проблем в рамках соответствующей применимой нормативно-правовой базы мы сможем и далее способствовать обеспечению свободного перемещения данных и укреплению доверия среди потребителей и бизнеса» [«Группа двадцати», 2020a].

Итальянское председательство не стало годом позитивных сдвигов в сближении позиций членов «Группы двадцати» по регулированию потоков данных. Несмотря на значительное внимание к вопросам цифровизации, расширение повестки по цифровой экономике (ЦЭ) и трансформацию целевой группы по ЦЭ в рабочую группу, по данным принято лишь два конкретных решения (из общего количества 225). Оба решения подтверждают сформулированные ранее намерения продолжить «работать над

решением проблем, связанных с обеспечением неприкосновенности частной жизни, защиты данных, безопасности и прав интеллектуальной собственности с учетом соответствующей применимой нормативно-правовой базы» (повторяется из саммита в саммит с 2017 г.) и «работать над углублением общего понимания и выявлением общих черт, взаимодополняющих элементов и совпадающих позиций в рамках анализа существующих подходов к регулированию инструментов, способствующих беспрепятственному перемещению информации на основе доверия в целях обеспечения совместимости в будущем» (согласовано в 2020 г. и фактически уже реализовано ОЭСР при финансовой поддержке правительства Японии) [«Группа двадцати», 2021].

Не способствовало повышению уровня доверия между членами «Группы двадцати» стремление председательства интегрировать в повестку дня «двадцатки» подходы ЕС и «Группы семи», например вопросы повторного использования и обмена данными и гибкого регулирования. Своего рода демонстрацией намерения членов «семерки» продвигать свои приоритеты в «двадцатке», ВТО и других институтах стало Заявление о принципах цифровой торговли, принятое фактически накануне саммита «двадцатки». В части, касающейся регулирования данных, «семерка» выступила за свободные потоки данных с доверием, против использования «требований локализации данных для протекционистских и дискриминационных целей, подрыва открытых обществ и демократических ценностей», а также «неоправданных барьеров для трансграничных потоков». «Семерка» пообещала обеспечивать защиту данных, конфиденциальности, прав интеллектуальной собственности и безопасности на основе высоких стандартов даже при трансграничном трансфере, усилить сотрудничество на основе выявления общих регуляторных подходов и работать над защитой неперсональных данных. Члены «Группы семи» также поддержали согласование общих принципов доверительного доступа правительства к данным частного сектора и соответствующую работу в ОЭСР [GOV.UK, 2021].

В общем по итогам трех лет работы над инициативой стало понятно, что легитимировать приоритеты, правила и нормы «семерки» и ОЭСР в «Группе двадцати» не получается. Не сработало и продвигаемое через экспертные центры [Heseleva et al., 2020] предложение США об использовании системы правил трансграничной конфиденциальности АТЭС как модели для глобального механизма трансфера данных, альтернативного ограничительному подходу ЕС и протекционистской модели Китая [Cory, Dascoli, 2021]. Но и каких-то новых подходов выработать не удалось.

В рамках председательства в «Группе двадцати» в 2022 г. Индонезия заявила в качестве одного из приоритетов сотрудничества ускорение цифровой трансформации экономики. Рабочая группа по цифровой экономике включила трансграничные потоки и свободные потоки данных с доверием в свой план работ наряду с вопросами связанности и постковидного восстановления, развития цифровых навыков и цифровой грамотности [G20, 2022]. Несмотря на усилия председательства по сохранению функциональности «Группы двадцати» как ключевого форума экономического сотрудничества ведущих государств с формирующимися экономиками и развитых стран и обеспечению консенсуса по фундаментальным вопросам макроэкономической политики, устойчивого роста, реформы глобальной системы здравоохранения, энергетического перехода и создания справедливой цифровой экономики, конфронтация «Группы семи» в отношении России сказалась на работе «двадцатки». Вопросы регулирования потоков данных не заняли в повестке председательства сколь-нибудь значительного места.

Заключение. Перспективы сотрудничества по регулированию потоков и защиты данных. Так возможно ли лидерство «Группы двадцати»?

Простой ответ на этот вопрос – нет. Экономическая блокада российских государственных институтов и частного бизнеса, нарушения прав собственности, конфиденциальности и злоупотребления частными данными членами «семерки» и ключевыми странами ОЭСР подорвали доверие к ценностям и институтам «демократических» государств со стороны большинства стран с формирующимися рынками. Фактически было разрушено доверие к ключевому элементу инициативы «Группы двадцати» по «свободному потоку данных с доверием».

Однако потребность в регулировании данных сохраняется, хотя бы для того, чтобы сдерживать монополии на цифровых рынках, формировать условия для развития справедливой цифровой экономики и создания общественных благ на основе данных.

«Группа двадцати» не является институтом выработки деталей регулирования. Но достижение политического консенсуса в рамках форума имеет ключевое значение для передачи «двадцаткой» мандата на разработку регулирования профильным многосторонним организациям или создания нового института и наделения его соответствующими компетенциями, как это было при создании аналогичного института, Совета финансовой стабильности, в контексте реформы глобального финансового регулирования. Рекомендации о необходимости инициативы «двадцатки» по разработке общего глобального механизма регулирования защиты и потоков данных неоднократно формулировались экспертным сообществом, включая предложения о создании Совета по управлению данными [Aaronson et al., 2021]. Действительно, координация процессов формирования механизмов коллективного регулирования цифровой экономики и данных как ее ключевого ресурса должна быть неотъемлемой составляющей повестки «Группы двадцати» как главного форума международного экономического сотрудничества, объединяющего ведущие развитые экономики и страны с формирующимися рынками. Развитие ЦЭ является обязательным условием достижения основной цели «двадцатки» по обеспечению сильного, устойчивого, сбалансированного и инклюзивного роста. Совет цифровой стабильности мог бы объединить развитые и развивающиеся страны, а также ключевые международные организации для координации процесса формирования стандартов, регулирования и политики, касающейся деятельности цифровых платформ и регулирования данных, выявления и стимулирования обмена лучшими практиками, оценки уязвимостей и формирования предложений по политике, направленной на их устранение или смягчение [Fay, Medhora, 2021].

Критика этого подхода в основном связана с тем, что как институт, созданный «двадцаткой», Совет вероятно будет «сфокусирован на “Группе двадцати”», и соответственно, не будет достаточно инклюзивен и легитимен. Кроме того, стабильность не будет одной из ключевых проблем цифровой экономики [UNCTAD, 2021, p. 185]. Хотя оба аргумента справедливы, преодоление указанных ограничений возможно за счет включения в работу института развивающихся стран и ключевых международных организаций, определения круга вопросов его мандата и компетенций и отражения сформированного мандата в названии института, например Совет по цифровой экономике и управлению данными (Digital economy and data governance board).

В условиях геополитической конфронтации шансы на формирование консенсуса в «двадцатке» ничтожны. Кроме того, риски создания специального института «двадцаткой» связаны с высокой вероятностью объединения усилий членов «семерки» для продвижения своих позиций в определении его параметров. В этом случае вполне возможно создание цифрового Бреттон-Вудского института [Medhora, Owen, 2020], который упрочит баланс сил старой системы.

Каковы же альтернативы и возможные сценарии дальнейшего развития регулирования данных? «Группа семи» будет и дальше стремиться формировать правила регулирования как для себя, так и для мира в целом. Намерение создать глобальный цифровой порядок, основанный на демократических принципах и правилах, недвусмысленно заявлено в приоритетах председательства Германии в «семерке» в 2022 г.: «Как часть нашего председательства мы хотим продвигать свободные трансграничные потоки данных с доверием, содействовать справедливой конкуренции и связанности. С нашими партнерами по “Группе семи” мы хотим работать для обеспечения отрытого, надежного и безопасного интернета, который не ограничивает, но усиливает демократические принципы и универсальные права человека. Как “Группа семи” мы хотим формировать общее понимание в отношении таких сфер, как глобальный цифровой порядок, в котором мы должны усилить международное сотрудничество с партнерами-единомышленниками. В этом контексте мы, вместе с партнерами по “семерке”, стремимся достичь более крепкого международного сотрудничества в отношении стандартов и норм, укорененных в открытом, демократическом и основанном на правилах порядке» [G7 German Presidency, 2022].

Соответственно, можно прогнозировать дальнейшее сближение и углубление сотрудничества по выработке общих подходов к регулированию потоков и защиты данных в рамках «Группы семи» и ОЭСР, с одной стороны, и стагнацию процесса в рамках «Группы двадцати» – с другой.

Процесс сближения в ОЭСР уже идет и включает: 1) собственно регулирование доступа, обработки, трансфера и защиты данных, в том числе повышение уровня доступности данных частного сектора; 2) формально технологические аспекты – технологии повышения уровня защиты, обеспечение переносимости и интероперабельности данных; 3) сближение практик администрирования, например, сотрудничество надзорных органов и сопоставимость используемого инструментария[13]; 4) формирование согласованных, основанных на общих ценностях правил и кодексов поведения как ориентиров или лучших практик использования данных [OECD, 2021a]. В инструментарий сближения, включающий исследования, обзоры, опросы, выявление лучших практик, формирование рекомендаций, интегрируются государства, не являющиеся членами ОЭСР, в том числе развивающиеся страны и члены «двадцатки». На сближение направлена и работа в рамках третьей фазы проекта Going Digital (2021–2022), включающая вопросы регулирования, доступности, обмена и контроля данных; содействия трансграничным потокам с доверием; влияния использования данных на фирмы и рынки; измерения данных и их потоков [OECD, n.d.a].

Таким образом, процесс является всеобъемлющим и затрагивает ценностно-идеологический, регуляторный, технологический и административный уровни, выходя за пределы членства ОЭСР. В условиях вероятной стагнации сотрудничества в рамках «Группы двадцати» этот управляемый, складывающийся из многих ручьев поток будет обтекать «двадцатку» и двигаться по намеченной траектории к формированию

[13] Например, сопоставимость форматов и процедур нотификации нарушений персональных данных. См. [Iwaya, Kokdsl-Oudot, Ronchi, 2021].

системы, состоящей из сопряженных сетей регулирования, задачей которой является свободное движение трансграничных потоков данных[14] как условие объективного отражения глобального распределения экономической, технологической и социальной активности, а также функционирования распределенных рынков и обществ данных [OECD, 2020].

«Семерка» уже приняла дорожную карту по сотрудничеству в отношении свободных потоков данных с доверием [G7, 2021a]. Развивается сотрудничество органов, ответственных за защиту данных [G7, 2021b]. Процесс поддерживает бизнес стран [Mastercard, 2021], в том числе технологические компании [BSA, 2022] и экспертное сообщество [Goodman, Risberg, 2021]. Сотрудничество «семерки» по цифровой экономике сильно идеологизировано и политизировано [G7 German Presidency, 2022] и, как и другие направления, активно развивается в сторону противодействия России [Jenkins, n.d.]. Однако возможные попытки «семерки» легитимировать свои подходы в «Группе двадцати» хоть и связаны с рисками, но все же оставляют окно возможностей для диалога.

ЮНКТАД предлагает поиск кооперативного решения как альтернативу конкуренции за цифровую и геоэкономическую власть, фрагментации регулирования и интернета. Новое регулирование должно учитывать все экономические и социальные измерения данных, целостным образом включать вопросы, касающиеся прав человека, национальной безопасности, торговли, конкуренции, налогообложения и управления интернетом. Соответственно, необходимо решать и вопрос о том, каким должен быть международный форум по формированию регулирования данных. Считая его возможным, поскольку, несмотря на различия в уровне приоритизации основными целями для всех стран являются экономический рост и развитие, защита данных и конфиденциальности и национальная безопасность, эксперты ЮНКТАД предлагают инициировать широкий диалог, направленный на формирование многоуровневой инклюзивной и гибкой системы управления данными. Диалог должен строиться на основе нескольких взаимосвязанных процессов:

1) выработки общего понимания основных концепций, включая таксономию данных, в том числе концепции «сырых» данных, продуктов данных, суверенитета данных;
2) определения условий доступа к данным;
3) создания системы измерения потоков данных;
4) формирования понимания данных как глобального общественного блага;
5) анализа различных формирующихся механизмов и инициатив по управлению данными;
6) определения и признания цифровых и связанных с данными прав;
7) выработки гибких, коллективно согласованных, инклюзивных стандартов, обеспечения интероперабельности и мобильности данных;
8) сотрудничества по регулированию глобальных цифровых платформ, направленного на преодоление доминирования и дисбалансов рыночной силы.

В диалоге должны участвовать профильные структуры ООН, международные и региональные организации, государства, частные структуры, бизнес, гражданское общество и экспертное сообщество, что даст возможность обеспечить многообразие, гибкость, учет различных региональных и национальных подходов. Одновременно

[14] Оно может быть ограничено только задачами обеспечения национальной безопасности и реализации законных целей государственной политики. Ограничения при этом должны быть легитимны и пропорциональны возможным рискам.

должна быть оказана помощь в создании в развивающихся странах технологического и управленческого потенциала для полноценного участия в цифровой экономике и цепочках данных на всех этапах создания стоимости. В результате на основе многостороннего диалога предполагается формирование многоуровневой распределенной полицентрической модели управления данными при центральной роли ООН или специализированного института в системе ООН.

Опыт многочисленных форумов ООН, в том числе Форума по управлению интернетом, а также диалога по реформе международной системы экономического управления и созданию Глобального экономического координационного совета (Global Economic Coordination Council) [UN, 2009] показывает, что с высокой вероятностью результатом станет появление еще одного консультативного механизма, не обладающего компетенциями для принятия решений. Очевидно, что в рамках такого механизма будут значительны риски влияния как государственных и межгосударственных институтов, так и структур управления интернетом и технологических компаний, традиционно выступающих спонсорами и активными участниками аналогичных платформ[15].

Таким образом, при обоих сценариях развития сотрудничества высоки риски альтернативного интересам и подходам России влияния в формируемых институтах. В этом контексте важным фактором может стать консолидированная позиция и сотрудничество БРИКС. Политика членов «пятерки» по управлению данными дает основание полагать, что консолидация возможна и важна для них. Одновременно, с учетом того, что миссия БРИКС – создание справедливого международного порядка, обеспечение участия и адекватного представительства развивающихся стран в системе глобального управления, содействие устойчивому развитию и инклюзивному росту, члены БРИКС должны быть заинтересованы в создании регулирования трансграничных данных и цифровых платформ, обеспечивающего сбалансированное распределение данных, преодоление угроз формирования нового колониализма и создание общественных благ на основе данных.

Однако пока в институциональной повестке «пятерки» вопросы регулирования данных не занимали значительного места. Это может быть связано с понимаем БРИКС необходимости выстраивать регулирование цифровых рынков в более широком формате с партнерами по «двадцатке». Но в условиях конфронтации, кризиса доверия, стремления «семерки» формировать глобальный цифровой порядок по своим правилам, вероятности стагнации сотрудничества в «двадцатке» совершенно необходимо активизировать взаимодействие в БРИКС, затем продвигая общие позиции в «Группе двадцати».

Основа жизнеспособного и инклюзивного многостороннего регулирования – договоренность по сближению регулирования данных при сохранении суверенитета стран над управлением данными. Консенсус по защите данных в таком случае касается в первую очередь не регуляторной практики, а уровня защиты, не навязывает и не ограничивает режим защиты требованиями обусловленности или локализации, а определяет принципы сотрудничества и взаимодействия уполномоченных органов стран-участниц. Ведь, как известно, режим обусловленности потоков данных может быть эквивалентен требованиям локализации хранения (и обработки данных)[16], а требование локализации хранения не обязательно означает полное ограничение потоков данных [Casalini, López González, 2019]. Более того, локализация не обязательно под-

[15] Правительства «семерки» и ЕК, Корпорация по присвоению доменных имен (ICANN), Общество Интернета, Microsoft, Google, Amazon и др. См., например, IGF [n.d.], [OECD, n.d.b].

[16] См., например, оценку в отношении Регламента ЕС в [Cory, Dascoli, 2021].

разумевает привязку к юрисдикции хранения и обработки данных, но может предполагать локализацию контролера и процессора [de la Chapelle, Porciuncula, 2021, p. 18]. Различия между национальными стандартами регулирования неизбежны, они есть и у стран БРИКС, но можно договориться о принципах. При этом страны назначения данных могут обязаться обеспечивать защиту данных граждан страны-источника в обмен на обязательство последней не ограничивать потоки данных. Первым шагом может быть определение условий защиты страной-источником данных, вторым – признание соответствия уровня защиты в случае, если есть уверенность в ее обеспечении, даже если регуляторные практики при этом различаются [Mattoo, Meltzer, 2018].

Для начала можно было бы инициировать в БРИКС анализ сопоставимости регулирования данных стран-членов, обмен опытом и выявление наилучших практик. Выполнение такой работы в 2022–2023 гг. позволило бы выйти на формирование принципов регулирования потоков и защиты данных БРИКС в 2024–2025 гг. В дальнейшем принципы могли бы стать основой для добровольного механизма регулирования потоков и защиты данных, открытого для присоединения других стран, в том числе партнеров по региональным интеграционным объединениям членов «пятерки».

Общие подходы и апробированные механизмы могли бы стать фундаментом для формирования согласованных позиций и реализации лидерского потенциала «пятерки» и дать новый импульс перспективам сотрудничества по регулированию потоков и защиты данных в «Группе двадцати».

Список источников

Aaronson S.A. (2019) What Are We Talking About When We Talk About Digital Protectionism? // World Trade Review. Vol. 18. Issue 4. P. 541–577. Режим доступа: https://doi.org/10.1017/S1474745618000198.

Aaronson S.A., Kimura F., Lee-Makiyama H., Stephenson S.M. (2021) Actions to Make “Data Free Flow With Trust” Operational in Practice. G20 Insights Policy Brief, 30 September. Режим доступа: https://www.g20-insights.org/policy_briefs/actions-to-make-data-free-flow-with-trust-operational-in-practice/ (дата обращения: 25.07.2022).

Azmeh S., Foster C., Echavarri J. (2020) The International Trade Regime and the Quest for Free Digital Trade // International Studies Review. Vol. 22. Issue 3. P. 671–92. Режим доступа: https://doi.org/10.1093/isr/viz033.

BSA (2022) Virtual Event: G7 Multi-Stakeholder Conference on Data Governance and Flows. 6 April. Режим доступа: https://www.bsa.org/news-events/events/virtual-event-g7-multi-stakeholder-conference-on-data-governance-and-flows (дата обращения: 23.01.2023).

Casalini F., López González J. (2019) Trade and Cross-Border Data Flows. OECD Trade Policy Papers No. 220, Organisation for Economic Co-operation and Development. Режим доступа: http://dx.doi.org/10.1787/b2023a47-en.

Cory N., Dascoli L. (2021) How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them. Information Technology & Innovation Foundation (ITIF), 19 July. Режим доступа: https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/ (дата обращения: 25.07.2022).

de la Chapelle B., Porciuncula L. (2021) We Need to Talk About Data: Framing the Debate Around Free Flow of Data and Data Sovereignty. Internet and Jurisdiction Policy Network. Режим доступа: https://www.internetjurisdiction.net/uploads/pdfs/We-Need-to-Talk-About-Data-Framing-the-Debate-Around-the-Free-Flow-of-Data-and-Data-Sovereignty-Report-2021.pdf (дата обращения: 25.07.2022).

Drake W., Cerf V., Kleinwächter W. (2016) Internet Fragmentation: An Overview. Future of the Internet Initiative White Paper, World Economic Forum. Режим доступа: http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf (дата обращения: 25.07.2022).

Elmi N. (2020) Is Big Tech Setting Africa Back? Foreign Policy, 11 November. Режим доступа: https://foreignpolicy.com/2020/11/11/is-big-tech-setting-africa-back/ (дата обращения: 25.07.2022).

European Commission (EC) (2018) Proposal for a Council Decision on the Conclusion of the Economic Partnership Agreement Between the European Union and Japan. COM(2018) 192 final. Brussels, 18 April. Режим доступа: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018PC0192#document2 (дата обращения: 25.07.2022).

European Commission (EC) (2020) Communication From the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A European Strategy for Data. COM(2020) 66 final. Brussels, 19 February. Режим доступа: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066 (дата обращения: 25.07.2022).

European Union (EU) (2016) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons With Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (Text With EEA relevance). Режим доступа: https://eur-lex.europa.eu/eli/reg/2016/679/2016-05-04 (дата обращения: 25.07.2022).

European Union (EU) (2018) Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a Framework for the Free Flow of Non-Personal Data in the European Union (Text With EEA Relevance) // Official Journal of the European Union, L 303/59. Режим доступа: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1807 (дата обращения: 25.07.2022).

European Union (EU) (2019) Commission Implementing Decision (EU) 2019/419 of 23 January 2019 Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the Adequate Protection of Personal Data by Japan Under the Act on the Protection of Personal Information (Text With EEA Relevance) // Official Journal of the European Union, L 76/1. Режим доступа: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019D0419 (дата обращения: 25.07.2022).

Fay R., Medhora R. (2021) A Global Governance Framework for Digital Technologies. T20 Policy Brief. Режим доступа: https://www.t20italy.org/wp-content/uploads/2021/09/TF4-PB5-Fay-1.pdf (дата обращения: 25.07.2022).

Gao H. (2018) Digital or Trade? The Contrasting Approaches of China and US to Digital Trade // Journal of International Economic Law. Vol. 21. Issue 2. P. 297–321. Режим доступа: https://doi.org/10.1093/jiel/jgy015.

Garrie D., Byhovsky I. (2017) Privacy and Data Protection in Russia // Journal of Law & Cyber Warfare. Vol. 5. Issue 2. P. 235–253. Режим доступа: https://www.jlcw.org/wp-content/uploads/2017/07/JLCW_5_2_Final.pdf (дата обращения: 25.07.2022).

Goodman M.P., Risberg P. (2021) Advancing Data Governance in the G7. Center for Strategic & International Studies (CSIS), 2 February. Режим доступа: https://www.csis.org/analysis/advancing-data-governance-g7 (дата обращения: 25.07.2022).

GOV.UK (2021) G7 Trade Ministers' Digital Trade Principles. News Story, 22 October. Режим доступа: https://www.gov.uk/government/news/g7-trade-ministers-digital-trade-principles (дата обращения: 25.07.2022).

Government of the United States (2019) Joint Statement on Electronic Commerce. Communication From the United States. Режим доступа: https://docs.wto.org/dol2fe/Pages/FE_Search/DDFDocuments/252610/q/INF/ECOM/5.pdf (дата обращения: 25.07.2022).

Group of 20 (G20) (2016a) Коммюнике лидеров «Группы двадцати» по итогам саммита в Ханчжоу (КНР). Режим доступа: http://kremlin.ru/supplement/5108 (дата обращения: 25.07.2022).

Group of 20 (G20) (2016b) Инициатива «Группы двадцати» по развитию и сотрудничеству в области цифровой экономики. Режим доступа: http://kremlin.ru/supplement/5111 (дата обращения: 25.07.2022) (in Russian).

Group of 20 (G20) (2017a) Коммюнике лидеров «Группы двадцати» по итогам саммита в Гамбурге (Германия). Режим доступа: http://static.kremlin.ru/media/events/files/ru/Gn9x4LcdfsmHANRguAmG-8ghIYMwzLrxX.doc (дата обращения: 25.07.2022).

Group of 20 (G20) (2017b) Digital Economy Ministerial Declaration: Shaping Digitalisation for an Interconnected World. Düsseldorf, 7 April. Режим доступа: http://www.g20.utoronto.ca/2017/170407-digitalization.html (дата обращения: 25.07.2022).

Group of 20 (G20) (2018a) Digital Economy Ministerial Declaration. Salta, 24 August. Режим доступа: http://www.g20.utoronto.ca/2018/2018-08-24-digital.html (дата обращения: 25.07.2022).

Group of 20 (G20) (2018b) Декларация лидеров «Группы двадцати». Режим доступа: http://kremlin.ru/supplement/5373 (дата обращения: 25.07.2022).

Group of 20 (G20) (2019a) Осакская декларация лидеров стран «Группы двадцати». Режим доступа: http://kremlin.ru/supplement/5425 (дата обращения: 25.07.2022).

Group of 20 (G20) (2019b) Ministerial Statement on Trade and Digital Economy. Tsukaba City, 8–9 June. Режим доступа: https://www.ranepa.ru/images/News_ciir/Project/Ministerial_Statement_on_Trade_and_Digital_Economy.pdf (дата обращения: 25.07.2022).

Group of 20 (G20) (2019c) Осакская декларация по вопросам цифровой экономики. Режим доступа: http://kremlin.ru/supplement/5427 (дата обращения: 25.07.2022).

Group of 20 (G20) (2020a) Digital Economy Ministerial Declaration. Virtual Meeting, July 22. Режим доступа: http://www.g20.utoronto.ca/2020/2020-g20-digital-0722.html (дата обращения: 25.07.2022).

Group of 20 (G20) (2020b) Extraordinary G20 Digital Economy Ministerial Meeting: COVID-19 Response Statement. Virtual Meeting, 30 April. Режим доступа: http://www.g20.utoronto.ca/2020/2020-g20-digital-0430.html (дата обращения: 25.07.2022).

Group of 20 (G20) (2020c) Экстренный саммит лидеров «Группы двадцати». Заявление по новой коронавирусной инфекции COVID 19. Режим доступа: http://kremlin.ru/supplement/5485 (дата обращения: 25.07.2022).

Group of 20 (G20) (2020d) Декларация Эр-Риядского саммита лидеров «Группы двадцати» (21–22 ноября 2020 г.). Режим доступа: http://kremlin.ru/supplement/5585 (дата обращения: 25.07.2022).

Group of 20 (G20) (2021) Римская декларация лидеров «Группы двадцати». Режим доступа: http://www.kremlin.ru/supplement/5729 (дата обращения: 25.07.2022).

Group of 20 (G20) (2022) MCI Consolidates Digital Issues in Indonesia's G20 Presidency through DEWG to Achieve Stronger Recovery. URL: https://g20.org/mci-consolidates-digital-issues-in-indonesias-g20-presidency-through-dewg-to-achieve-stronger-recovery-2/ (дата обращения: 25.07.2022).

Group of 7 (G7) (2016a) Leaders' Declaration. Ise-Shima, 27 May. Режим доступа: http://www.g7.utoronto.ca/summit/2016shima/ise-shima-declaration-en.html#cyber (дата обращения: 25.07.2022).

Group of 7 (G7) (2016b) G7 Principles and Actions on Cyber. Ise-Shima, 27 May. Режим доступа: http://www.g7.utoronto.ca/summit/2016shima/cyber.html (дата обращения: 25.07.2022).

Group of 7 (G7) (2016c) Joint Declaration by G7 ICT Ministers (Action Plan on Implementing the Charter). Takamatsu, 30 April. Режим доступа: http://www.g7.utoronto.ca/ict/2016-ict-declaration.html (дата обращения: 25.07.2022).

Group of 7 (G7) (2021a) Ministerial Declaration. G7 Digital and Technology Ministers' Meeting, 28 April. Режим доступа: https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/presentation/pdf/G7_Digital_and_Technology_Ministerial_Declaration.pdf (дата обращения: 25.07.2022).

Group of 7 (G7) (2021b) Communiqué: "Data Free Flow With Trust." Roundtable of G7 Data Protection and Privacy Authorities, 7–8 September. Режим доступа: https://www.priv.gc.ca/en/opc-news/speeches/2021/communiqué-g7_210907/ (дата обращения: 25.07.2022).

Group of 7 (G7) German Presidency (2022) Policy Priorities for Germany's G7 Presidency in 2022. Режим доступа: http://www.g7.utoronto.ca/summit/2022elmau/2022-01-21-g7-programm-en-data.pdf (дата обращения: 25.07.2022).

Heseleva K., Ramos V.J., Ichilevici de Oliveira A. (2020) Towards a Multilateral Consensus on Data Governance. G20 Insights Policy Brief, 29 May. Режим доступа: https://www.g20-insights.org/policy_briefs/towards-a-multilateral-consensus-on-data-governance/ (дата обращения: 25.07.2022).

Hummel P., Braun M., Tretter M., Dabrock P. (2021) Data Sovereignty: A Review // Big Data & Society. Vol. 8. Issue 1. Режим доступа: http://dx.doi.org/10.1177/2053951720982012.

Internet & Jurisdiction Policy Network (2019) 2019 Internet & Jurisdiction Global Status Report. Режим доступа: https://connect.internetjurisdiction.net/zs/4uhWUc (дата обращения: 23.01.2023).

Internet Governance Forum (IGF) (n.d.) Donors to the IGF Trust Fund. Режим доступа: https://www.intgovforum.org/en/about#donors-to-the-igf-trust-fund (дата обращения: 23.01.2023).

Iwaya S., Koksal-Oudot E., Ronchi E. (2021) Promoting Comparability in Personal Data Breach Notification Reporting. OECD Digital Economy Papers No. 322, Organisation for Economic Co-operation and Development. Режим доступа: https://doi.org/10.1787/88f79eb0-en.

Jenkins F. (n.d.) G7 Help Ukraine in Cyberspace. The Munich Eye. Режим доступа: https://themunicheye.com/g7-help-ukraine-in-cyberspace-4805 (дата обращения: 25.07.2022).

Larionova M.V., Shelepov A.V. (2021) Emerging Mechanisms for Regulating the Digital Economy: Risks and Opportunities for the Multilateral System of Global Governance // International Organisations Research Journal. Vol. 16. No. 1. P. 29–63. Режим доступа: https://doi.org/10.17323/1996-7845-2021-01-02 (in Russian and English).

Madiega T. (2020) Digital Sovereignty for Europe. EPRS Ideas Paper PE 651.992, European Parliamentary Research Service. Режим доступа: https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf (дата обращения: 25.07.2022).

Mastercard (2021) Setting Principles for the Digital Economy: Establishing a G7 Data and Technology Forum. 22 March. Режим доступа: https://www.mastercard.com/news/insights/2021/setting-principles-for-the-digital-economy-establishing-a-g7-data-and-technology-forum/ (дата обращения: 25.07.2022).

Mattoo A., Meltzer J.P. (2018) International Data Flows and Privacy: The Conflict and Its Resolution. Policy Research Working Paper No. 8431, World Bank Group. Режим доступа: http://hdl.handle.net/10986/29837 (дата обращения: 25.07.2022).

Medhora R.P., Owen T. (2020) A Post-COVID-19 Digital Bretton Woods. Centre for International Governance Innovation, 19 April. Режим доступа: https://www.cigionline.org/articles/post-covid-19-digital-bretton-woods/ (дата обращения: 25.07.2022).

Organisation for Economic Co-operation and Development (OECD) (2013) Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. OECD/LEGAL/0188. Режим доступа: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188 (дата обращения: 25.07.2022).

Organisation for Economic Co-operation and Development (OECD) (2015) Data-Driven Innovation: Big Data for Growth and Well-Being. Режим доступа: http://dx.doi.org/10.1787/9789264229358-en.

Organisation for Economic Co-operation and Development (OECD) (2019a) Data in the Digital Age. OECD Going Digital Policy Note. Режим доступа: https://www.oecd.org/digital/ieconomy/data-in-the-digital-age.pdf (дата обращения: 25.07.2022).

Organisation for Economic Co-operation and Development (OECD) (2019b) Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use Across Societies. Режим доступа: https://doi.org/10.1787/276aaca8-en.

Organisation for Economic Co-operation and Development (OECD) (2019c) Going Digital: Shaping Policies, Improving Lives. Режим доступа: https://www.oecd.org/digital/going-digital-shaping-policies-improving-lives-9789264312012-en.htm (дата обращения: 25.07.2022).

Organisation for Economic Co-operation and Development (OECD) (2020) Mapping Approaches to Data and Data Flows: Report for the G20 Digital Economy Task Force, Saudi Arabia. Режим доступа: https://www.oecd.org/trade/documents/mapping-approaches-to-data-and-data-flows.pdf (дата обращения: 25.07.2022).

Organisation for Economic Co-operation and Development (OECD) (2021a) Good Practice Principles for Data Ethics in the Public Sector. Режим доступа: https://www.oecd.org/gov/digital-government/good-practice-principles-for-data-ethics-in-the-public-sector.pdf (дата обращения: 25.07.2022).

Organisation for Economic Co-operation and Development (OECD) (2021b) Mapping Commonalities in Regulatory Approaches to Cross-Border Data Transfers. TAD/TC/WP(2020)15/FINAL, 23 April. Режим доступа: https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=TAD/TC/WP(2020)15/FINAL&docLanguage=En (дата обращения: 25.07.2022).

Organisation for Economic Co-operation and Development (OECD) (n.d.a) Going Digital Project. Режим доступа: https://www.oecd.org/digital/going-digital-project/ (дата обращения: 23.01.2023).

Organisation for Economic Co-operation and Development (OECD) (n.d.b) Internet Policy and Governance. Режим доступа: https://www.oecd.org/sti/broadband/internet-policy-and-governance.htm (дата обращения: 23.01.2023).

Prime Minister of Japan and His Cabinet (2019) Toward a New Era of "Hope-Driven Economy:" The Prime Minister's Keynote Speech at the World Economic Forum Annual Meeting. 23 January. Режим доступа: https://japan.kantei.go.jp/98_abe/statement/201901/_00003.html (дата обращения: 23.01.2023).

Rikap C. (2021) Intellectual Monopoly Capitalism and Its Effects on Development: Intellectual Monopoly Capitalism Uncovered. Developing Economics, 7 April. Режим доступа: https://developingeconomics.org/2021/04/07/intellectual-monopoly-capitalism-and-its-effects-on-development/ (дата обращения: 25.07.2022).

Selby J. (2017) Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both? // International Journal of Law and Information Technology. Vol. 25. Issue 3. P. 213–232. Режим доступа: https://doi.org/10.1093/ijlit/eax010.

Svantesson D. (2020) Data Localisation Trends and Challenges: Considerations for the Review of the Privacy Guidelines. OECD Digital Economy Papers No. 301, Organisation for Economic Co-operation and Development. Режим доступа: http://dx.doi.org/10.1787/7fbaed62-en.

Titievskaia J. (2020) WTO E-Commerce Negotiations. EPRS PE 659.263, European Parliamentary Research Service. Режим доступа: https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/659263/EPRS_ATA(2020)659263_EN.pdf (дата обращения: 25.07.2022).

United Nations (UN) (2009) Report of the Commission of Experts of the President of the United Nations General Assembly on Reforms of the International Monetary and Financial System. Режим доступа: https://www.un.org/en/ga/econcrisissummit/docs/FinalReport_CoE.pdf (дата обращения: 25.07.2022).

United Nations Conference on Trade and Development (UNCTAD) (2021) Digital Economy Report 2021. Cross-Border Data Flows and Development: For Whom the Data Flow. Режим доступа: https://unctad.org/system/files/official-document/der2021_en.pdf (дата обращения: 25.07.2022).

World Trade Organization (WTO) (2017) The Work Programme on Electronic Commerce: Statement by the African Group. WT/MIN(17)/21, 6 December. Режим доступа: https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/MIN17/21.pdf&Open=True (дата обращения: 25.07.2022).

World Trade Organization (WTO) (2019) Joint Statement on Electronic Commerce: Communication From China. INF/ECOM/19, 23 April. Режим доступа: https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/INF/ECOM/19.pdf&Open=True (дата обращения: 25.07.2022).

Yakovleva S. (2020) Personal Data Transfers in International Trade and EU Law: A Tale of Two "Necessities" // The Journal of World Investment & Trade. Vol. 21. No. 6. P. 881–919. Режим доступа: https://doi.org/10.1163/22119000-12340189.

International Organisations Research Journal, 2023, vol. 18, no 1, pp. 7–32
Original Article
doi:10.17323/1996-7845-2023-01-01

Opportunities and Constraints for G20 Leadership in Data Governance: Is There a Chance for Convergence in Approaches?[1]

M. Larionova, A. Shelepov

Marina Larionova – PhD, Head, Centre for International Institutions Research (CIIR), Russian Presidential Academy of National Economy and Public Administration (RANEPA); 11 Prechistenskaya naberezhnaya, Moscow, 119034, Russia; larionova-mv@ranepa.ru

Andrey Shelepov – Candidate of Economic Sciences, Senior Researcher, Centre for International Institutions Research (CIIR), Russian Presidential Academy of National Economy and Public Administration; 11 Prechistenskaya naberezhnaya, 119034, Moscow, Russia; shelepov-av@ranepa.ru

Abstract

Data is an infinite resource, a new form of capital in the knowledge economy. In absence of data regulation, global technological corporations seek to expand their influence at each link in data chains and use their market power to build monopolies. Data can generate not only profits for tech giants but also social value; however, market forces by themselves will not create data-based public goods. For this, government actions are needed at the county level, and interstate and multilateral institutional cooperation is required at the international level. To date, despite numerous initiatives to establish coordination mechanisms and data regulation, cooperation on data governance is highly fragmented and gridlocked due to contradictions and tough competition between players. One of the key disagreements is related to the regulation of cross-border data flows.

The article explores contradictions between the regulatory practices of the central actors in the digital economy, the U.S., the European Union (EU) and China in the first place, and the approaches they promote in international institutions such as the World Trade Organization (WTO), the Group of G20 (G20), the Group of 7 (G7), and the Organisation for Economic Co-operation and Development (OECD). In particular, the authors look at the G20's agenda on data governance and the initiative on free data flow with trust and consider its challenges and the risks of cooperation stagnation. The conclusion presents possible scenarios for future cooperation on data governance, their risks and perspectives, including the establishment of the Digital Economy and Data Governance Board by the G20, the G7's initiative on shaping global digital order, deepening of cooperation on data governance within the G7 and the OECD, and the United Nations Conference on Trade and Development (UNCTAD) proposal on building a multilevel, distributed polycentric data-governance model with the UN playing a central role. The authors conclude with a proposal on cooperation within BRICS (Brazil, Russia, India, China and South Africa) aimed at shaping inclusive multilateral data governance.

Keywords: Data governance, G20, localization, free data flows

Acknowledgments: the article was written on the basis of the RANEPA state assignment research programme.

For citation: Larionova M., Shelepov A. (2023) Opportunities and Constraints for G20 Leadership in Data Governance: Is There a Chance for Convergence in Approaches? *International Organisations Research Journal*, vol. 18, no 1, pp. 7–32 (in English). doi:10.17323/1996-7845-2023-01-01

References

Aaronson S.A. (2019) What Are We Talking About When We Talk About Digital Protectionism? *World Trade Review*, vol. 18, issue 4, pp. 541–77. Available at: https://doi.org/10.1017/S1474745618000198.

Aaronson S.A., Kimura F., Lee-Makiyama H., Stephenson S.M. (2021) Actions to Make "Data Free Flow With Trust" Operational in Practice. G20 Insights Policy Brief, 30 September. Available at: https://www.g20-

[1] This article was submitted 15.07.2022.

insights.org/policy_briefs/actions-to-make-data-free-flow-with-trust-operational-in-practice/ (accessed 25 July 2022).

Azmeh S., Foster C., Echavarri J. (2020) The International Trade Regime and the Quest for Free Digital Trade. *International Studies Review*, vol. 22, issue 3, pp. 671–92. Available at: https://doi.org/10.1093/isr/viz033.

BSA (2022) Virtual Event: G7 Multi-Stakeholder Conference on Data Governance and Flows, 6 April. Available at: https://www.bsa.org/news-events/events/virtual-event-g7-multi-stakeholder-conference-on-data-governance-and-flows (accessed 30 January 2023).

Casalini F., López González J. (2019) Trade and Cross-Border Data Flows. OECD Trade Policy Papers No 220, Organisation for Economic Co-operation and Development. Available at: http://dx.doi.org/10.1787/b2023a47-en.

Cory N., Dascoli L. (2021) How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them. Information Technology & Innovation Foundation (ITIF), 19 July. Available at: https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/ (accessed 25 July 2022).

de la Chapelle B., Porciuncula L. (2021) We Need to Talk About Data: Framing the Debate Around Free Flow of Data and Data Sovereignty. Internet and Jurisdiction Policy Network. Available at: https://www.internetjurisdiction.net/uploads/pdfs/We-Need-to-Talk-About-Data-Framing-the-Debate-Around-the-Free-Flow-of-Data-and-Data-Sovereignty-Report-2021.pdf (accessed 25 July 2022).

Drake W., Cerf V., Kleinwächter W. (2016) Internet Fragmentation: An Overview. Future of the Internet Initiative White Paper, World Economic Forum. Available at: http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf (accessed 25 July 2022).

Elmi N. (2020) Is Big Tech Setting Africa Back? Foreign Policy, 11 November. Available at: https://foreignpolicy.com/2020/11/11/is-big-tech-setting-africa-back/ (accessed 25 July 2022).

European Commission (EC) (2018) Proposal for a Council Decision on the Conclusion of the Economic Partnership Agreement Between the European Union and Japan. COM(2018) 192 final. Brussels, 18 April. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018PC0192#document2 (accessed 25 July 2022).

European Commission (EC) (2020) Communication From the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A European Strategy for Data. COM(2020) 66 final. Brussels, 19 February. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066 (accessed 25 July 2022).

European Union (EU) (2016) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons With Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (Text With EEA relevance). Available at: https://eur-lex.europa.eu/eli/reg/2016/679/2016-05-04 (accessed 25 July 2022).

European Union (EU) (2018) Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a Framework for the Free Flow of Non-Personal Data in the European Union (Text With EEA Relevance). *Official Journal of the European Union*, L 303/59. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1807 (accessed 25 July 2022).

European Union (EU) (2019) Commission Implementing Decision (EU) 2019/419 of 23 January 2019 Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the Adequate Protection of Personal Data by Japan Under the Act on the Protection of Personal Information (Text With EEA Relevance). *Official Journal of the European Union*, L 76/1. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019D0419 (accessed 25 July 2022).

Fay R., Medhora R. (2021) A Global Governance Framework for Digital Technologies. T20 Policy Brief. Available at: https://www.t20italy.org/wp-content/uploads/2021/09/TF4-PB5-Fay-1.pdf (accessed 25 July 2022).

Gao H. (2018) Digital or Trade? The Contrasting Approaches of China and US to Digital Trade. *Journal of International Economic Law*, vol. 21, issue 2, pp. 297–321. Available at: https://doi.org/10.1093/jiel/jgy015.

Garrie D., Byhovsky I. (2017) Privacy and Data Protection in Russia. *Journal of Law & Cyber Warfare*, vol. 5, issue 2, pp. 235–53. Available at: https://www.jlcw.org/wp-content/uploads/2017/07/JLCW_5_2_Final.pdf (accessed 25 July 2022).

Goodman M.P., Risberg P. (2021) Advancing Data Governance in the G7. Center for Strategic & International Studies (CSIS), 2 February. Available at: https://www.csis.org/analysis/advancing-data-governance-g7 (accessed 25 July 2022).

GOV.UK (2021) G7 Trade Ministers' Digital Trade Principles. News Story, 22 October. Available at: https://www.gov.uk/government/news/g7-trade-ministers-digital-trade-principles (accessed 25 July 2022).

Government of the United States (2019) Joint Statement on Electronic Commerce. Communication From the United States. Available at: https://docs.wto.org/dol2fe/Pages/FE_Search/DDFDocuments/252610/q/INF/ECOM/5.pdf (accessed 25 July 2022).

Group of 20 (G20 (2016a) Kommyunike liderov "Gruppy dvadcati" po itogam sammita v Hanchzhou (KNR) [Communiqué of the Leaders of the G20 Following the Summit in Hangzhou (PRC)]. Available at: http://kremlin.ru/supplement/5108 (accessed 25 July 2022) (in Russian).

Group of 20 (G20) (2016b) Iniciativa "Gruppy dvadcati" po razvitiyu i sotrudnichestvu v oblasti cifrovoj ekonomiki [G20 Digital Economy Development and Cooperation Initiative]. Available at: http://kremlin.ru/supplement/5111 (accessed 25 July 2022) (in Russian).

Group of 20 (G20) (2017a) Kommyunike liderov "Gruppy dvadcati" po itogam sammita v Gamburge (Germaniya) [Communiqué of the G20 Leaders Following the Summit in Hamburg (Germany)]. Available at: http://static.kremlin.ru/media/events/files/ru/Gn9x4LcdfsmHANRguAmG8ghIYMwzLrxX.doc (accessed 25 July 2022).

Group of 20 (G20) (2017b) Digital Economy Ministerial Declaration: Shaping Digitalisation for an Interconnected World. Düsseldorf, 7 April. Available at: http://www.g20.utoronto.ca/2017/170407-digitalization.html (accessed 25 July 2022).

Group of 20 (G20) (2018a) Digital Economy Ministerial Declaration. Salta, 24 August. Available at: http://www.g20.utoronto.ca/2018/2018-08-24-digital.html (accessed 25 July 2022).

Group of 20 (G20) (2018b) Deklaraciya liderov "Gruppy dvadcati" [G20 Leaders' Declaration]. Available at: http://kremlin.ru/supplement/5373 (accessed 25 July 2022) (in Russian).

Group of 20 (G20) (2019a) Osakskaya deklaraciya liderov stran "Gruppy dvadcati" [G20 Leaders' Osaka Declaration]. Available at: http://kremlin.ru/supplement/5425 (accessed 25 July 2022) (in Russian).

Group of 20 (G20) (2019b) Ministerial Statement on Trade and Digital Economy. Tsukaba City, 8–9 June. Available at: https://www.ranepa.ru/images/News_ciir/Project/Ministerial_Statement_on_Trade_and_Digital_Economy.pdf (accessed 25 July 2022).

Group of 20 (G20) (2019c) Osakskaya deklaraciya po voprosam cifrovoj ekonomiki [Osaka declaration on digital economy]. Available at: http://kremlin.ru/supplement/5427 (accessed 25 July 2022) (in Russian).

Group of 20 (G20) (2020a) Digital Economy Ministerial Declaration. Virtual Meeting, July 22. Available at: http://www.g20.utoronto.ca/2020/2020-g20-digital-0722.html (accessed 25 July 2022).

Group of 20 (G20) (2020b) Extraordinary G20 Digital Economy Ministerial Meeting: COVID-19 Response Statement. Virtual Meeting, 30 April. Available at: http://www.g20.utoronto.ca/2020/2020-g20-digital-0430.html (accessed 25 July 2022).

Group of 20 (G20) (2020c) Ekstrennyj sammit liderov "Gruppy dvadcati". Zayavlenie po novoj koronavirusnoj infekcii COVID 19 [Extraordinary G20 Leaders' Summit. Statement on COVID-19]. Available at: http://kremlin.ru/supplement/5485 (accessed 25 July 2022) (in Russian).

Group of 20 (G20) (2020d) Deklaraciya Er-Riyadskogo sammita liderov "Gruppy dvadcati" (21–22 noyabrya 2020 goda) [G20 Riyadh Summit G20 Leaders' Declaration (November 21–22, 2020)]. Available at: http://kremlin.ru/supplement/5585 (accessed 25 July 2022) (in Russian).

Group of 20 (G20) (2021) Rimskaya deklaraciya liderov "Gruppy dvadcati" [G20 Rome Leaders' Declaration]. Available at: http://www.kremlin.ru/supplement/5729 (accessed 25 July 2022) (in Russian).

Group of 20 (G20) (2022) MCI Consolidates Digital Issues in Indonesia's G20 Presidency through DEWG to Achieve Stronger Recovery. URL: https://g20.org/mci-consolidates-digital-issues-in-indonesias-g20-presidency-through-dewg-to-achieve-stronger-recovery-2/ (accessed 25 July 2022)/

Group of 7 (G7) (2016a) Leaders' Declaration. Ise-Shima, 27 May. Available at: http://www.g7.utoronto.ca/summit/2016shima/ise-shima-declaration-en.html#cyber (accessed 25 July 2022).

Group of 7 (G7) (2016b) G7 Principles and Actions on Cyber. Ise-Shima, 27 May. Available at: http://www.g7.utoronto.ca/summit/2016shima/cyber.html (accessed 25 July 2022).

Group of 7 (G7) (2016c) Joint Declaration by G7 ICT Ministers (Action Plan on Implementing the Charter). Takamatsu, 30 April. Available at: http://www.g7.utoronto.ca/ict/2016-ict-declaration.html (accessed 25 July 2022).

Group of 7 (G7) (2021a) Ministerial Declaration. G7 Digital and Technology Ministers' Meeting, 28 April. Available at: https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/presentation/pdf/G7_Digital_and_Technology_Ministerial_Declaration.pdf (accessed 25 July 2022).

Group of 7 (G7) (2021b) Communiqué: "Data Free Flow With Trust." Roundtable of G7 Data Protection and Privacy Authorities, 7–8 September. Available at: https://www.priv.gc.ca/en/opc-news/speeches/2021/communiqué-g7_210907/ (accessed 25 July 2022).

Group of 7 (G7) German Presidency (2022) Policy Priorities for Germany's G7 Presidency in 2022. Available at: http://www.g7.utoronto.ca/summit/2022elmau/2022-01-21-g7-programm-en-data.pdf (accessed 25 July 2022).

Heseleva K., Ramos V.J., Ichilevici de Oliveira A. (2020) Towards a Multilateral Consensus on Data Governance. G20 Insights Policy Brief, 29 May. Available at: https://www.g20-insights.org/policy_briefs/towards-a-multilateral-consensus-on-data-governance/ (accessed 25 July 2022).

Hummel P., Braun M., Tretter M., Dabrock P. (2021) Data Sovereignty: A Review. *Big Data & Society*, vol. 8, issue 1. Available at: http://dx.doi.org/10.1177/2053951720982012.

Internet & Jurisdiction Policy Network (2019) 2019 Internet & Jurisdiction Global Status Report. Available at: https://connect.internetjurisdiction.net/zs/4uhWUc (accessed 30 January 2023).

Internet Governance Forum (IGF) (n.d.) Donors to the IGF Trust Fund. Available at: https://www.intgovforum.org/en/about#donors-to-the-igf-trust-fund (accessed 30 January 2023).

Iwaya S., Koksal-Oudot E., Ronchi E. (2021) Promoting Comparability in Personal Data Breach Notification Reporting. OECD Digital Economy Papers No 322, Organisation for Economic Co-operation and Development. Available at: https://doi.org/10.1787/88f79eb0-en.

Jenkins F. (n.d.) G7 Help Ukraine in Cyberspace. The Munich Eye. Available at: https://themunicheye.com/g7-help-ukraine-in-cyberspace-4805 (accessed 25 July 2022).

Larionova M.V., Shelepov A.V. (2021) Emerging Mechanisms for Regulating the Digital Economy: Risks and Opportunities for the Multilateral System of Global Governance. *International Organisations Research Journal*, vol. 16, no 1, pp. 29–63. Available at: https://doi.org/10.17323/1996-7845-2021-01-02 (in Russian and English).

Madiega T. (2020) Digital Sovereignty for Europe. EPRS Ideas Paper PE 651.992, European Parliamentary Research Service. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf (accessed 25 July 2022).

Mastercard (2021) Setting Principles for the Digital Economy: Establishing a G7 Data and Technology Forum. 22 March. Available at: https://www.mastercard.com/news/insights/2021/setting-principles-for-the-digital-economy-establishing-a-g7-data-and-technology-forum/ (accessed 25 July 2022).

Mattoo A., Meltzer J.P. (2018) International Data Flows and Privacy: The Conflict and Its Resolution. Policy Research Working Paper No 8431, World Bank Group. Available at: http://hdl.handle.net/10986/29837 (accessed 25 July 2022).

Medhora R.P., Owen T. (2020) A Post-COVID-19 Digital Bretton Woods. Centre for International Governance Innovation, 19 April. Available at: https://www.cigionline.org/articles/post-covid-19-digital-bretton-woods/ (accessed 25 July 2022).

Organisation for Economic Co-operation and Development (OECD) (2013) Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. OECD/LEGAL/0188. Available at: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188 (accessed 25 July 2022).

Organisation for Economic Co-operation and Development (OECD) (2015) Data-Driven Innovation: Big Data for Growth and Well-Being. Available at: http://dx.doi.org/10.1787/9789264229358-en.

Organisation for Economic Co-operation and Development (OECD) (2019a) Data in the Digital Age. OECD Going Digital Policy Note. Available at: https://www.oecd.org/digital/ieconomy/data-in-the-digital-age.pdf (accessed 25 July 2022).

Organisation for Economic Co-operation and Development (OECD) (2019b) Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use Across Societies. Available at: https://doi.org/10.1787/276aaca8-en.

Organisation for Economic Co-operation and Development (OECD) (2019c) Going Digital: Shaping Policies, Improving Lives. Available at: https://www.oecd.org/digital/going-digital-shaping-policies-improving-lives-9789264312012-en.htm (accessed 25 July 2022).

Organisation for Economic Co-operation and Development (OECD) (2020) Mapping Approaches to Data and Data Flows: Report for the G20 Digital Economy Task Force, Saudi Arabia. Available at: https://www.oecd.org/trade/documents/mapping-approaches-to-data-and-data-flows.pdf (accessed 25 July 2022).

Organisation for Economic Co-operation and Development (OECD) (2021a) Good Practice Principles for Data Ethics in the Public Sector. Available at: https://www.oecd.org/gov/digital-government/good-practice-principles-for-data-ethics-in-the-public-sector.pdf (accessed 25 July 2022).

Organisation for Economic Co-operation and Development (OECD) (2021b) Mapping Commonalities in Regulatory Approaches to Cross-Border Data Transfers. TAD/TC/WP(2020)15/FINAL, 23 April. Available at: https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=TAD/TC/WP(2020)15/FINAL&docLanguage=En (accessed 25 July 2022).

Organisation for Economic Co-operation and Development (OECD) (n.d.a) Going Digital Project. Available at: https://www.oecd.org/digital/going-digital-project/ (accessed 30 January 2023).

Organisation for Economic Co-operation and Development (OECD) (n.d.b) Internet Policy and Governance. Available at: https://www.oecd.org/sti/broadband/internet-policy-and-governance.htm (accessed 30 January 2023).

Prime Minister of Japan and His Cabinet (2019) Toward a New Era of "Hope-Driven Economy": The Prime Minister's Keynote Speech at the World Economic Forum Annual Meeting. 23 January. Available at: https://japan.kantei.go.jp/98_abe/statement/201901/_00003.html (accessed 30 January 2023).

Rikap C. (2021) Intellectual Monopoly Capitalism and Its Effects on Development: Intellectual Monopoly Capitalism Uncovered. *Developing Economics*, 7 April. Available at: https://developingeconomics.org/2021/04/07/intellectual-monopoly-capitalism-and-its-effects-on-development/ (accessed 25 July 2022).

Selby J. (2017) Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both? *International Journal of Law and Information Technology*, vol. 25, issue 3, pp. 213–32. Available at: https://doi.org/10.1093/ijlit/eax010.

Svantesson D. (2020) Data Localisation Trends and Challenges: Considerations for the Review of the Privacy Guidelines. OECD Digital Economy Papers No 301, Organisation for Economic Co-operation and Development. Available at: http://dx.doi.org/10.1787/7fbaed62-en.

Titievskaia J. (2020) WTO E-Commerce Negotiations. EPRS PE 659.263, European Parliamentary Research Service. Available at: https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/659263/EPRS_ATA(2020)659263_EN.pdf (accessed 25 July 2022).

United Nations (UN) (2009) Report of the Commission of Experts of the President of the United Nations General Assembly on Reforms of the International Monetary and Financial System. Available at: https://www.un.org/en/ga/econcrisissummit/docs/FinalReport_CoE.pdf (accessed 25 July 2022).

United Nations Conference on Trade and Development (UNCTAD) (2021) Digital Economy Report 2021. Cross-Border Data Flows and Development: For Whom the Data Flow. Available at: https://unctad.org/system/files/official-document/der2021_en.pdf (accessed 25 July 2022).

World Trade Organization (WTO) (2017) The Work Programme on Electronic Commerce: Statement by the African Group. WT/MIN(17)/21, 6 December. Available at: https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/MIN17/21.pdf&Open=True (accessed 25 July 2022).

World Trade Organization (WTO) (2019) Joint Statement on Electronic Commerce: Communication From China. INF/ECOM/19, 23 April. Available at: https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/INF/ECOM/19.pdf&Open=True (accessed 25 July 2022).

Yakovleva S. (2020) Personal Data Transfers in International Trade and EU Law: A Tale of Two "Necessities". *The Journal of World Investment & Trade*, vol. 21, no 6, pp. 881–919. Available at: https://doi.org/10.1163/22119000-12340189.