

Я.Н. ШЕВЧЕНКО*

**ЦИФРОВОЙ СУВЕРЕНИТЕТ ЕВРОПЫ
В КОНТЕКСТЕ ПОЛИТИКИ
ГЛОБАЛЬНОГО УПРАВЛЕНИЯ ДАННЫМИ**

Аннотация. Исследовательская цель настоящей статьи заключается в определении места объединенной Европы в международном информационно-коммуникационном пространстве. Акцент делается на необходимости обеспечения цифрового суверенитета Европейского союза (ЕС) в контексте политики глобального управления данными, что предполагает создание самобытного европейского информационно-телекоммуникационного пространства, независимого от любого внешнего влияния. Таким образом, цифровой суверенитет для Европы является гарантией обеспечения ее стратегической автономии в условиях растущего влияния США и Китая как ключевых акторов мировой политической системы в цифровую эпоху.

Опираясь на принципы регионального подхода и мультипарадигмальный метод И.Н. Барыгина, автор экстраполирует отдельные положения теории гегемонистской стабильности (в интерпретации Р. Гилпина) на современное технологическое соперничество государств на международной арене. Такой подход позволяет выявить два взаимосвязанных комплекса факторов, объективно препятствующих успешной реализации общеевропейской «Стратегии в области данных». Во-первых, это продолжающаяся зависимость ЕС от иностранных технологий и услуг, а во-вторых, недостаточная инвестиционная привлекательность Евросоюза (по сравнению с Китаем и США), необходимая для всесторонней поддержки европейской промышленной политики (в том числе и в сфере цифровых технологий). Кроме того в статье показано, что для эффективного управления в цифровом секторе необходимо использовать модель многостороннего участия (без отказа от роли государства в регулировании рынка). Государство в цифро-

* **Шевченко Ян Николаевич**, аспирант кафедры мировой политики, Санкт-Петербургский государственный университет (Санкт-Петербург, Россия), e-mail: ian.chevtchenko@gmail.com

вую эпоху должно оставаться органичной частью цифровой экосистемы, чтобы защищать интересы своих граждан.

Ключевые слова: цифровой суверенитет; Евросоюз; кибербезопасность; глобальное управление; персональные данные; цифровая геополитика.

Для цитирования: Шевченко Я.Н. Цифровой суверенитет Европы в контексте политики глобального управления данными // Политическая наука. – 2021. – № 3. – С. 251–270. – DOI: <http://www.doi.org/10.31249/poln/2021.03.11>

Введение

В последние несколько месяцев вопрос о европейском цифровом суверенитете¹ является одной из наиболее обсуждаемых тем в рамках геополитической повестки Европейской комиссии, объявленной ее председателем Урсолой фон дер Ляйен [Polito, 2021, p. 2].

Не в последнюю очередь широкий интерес к этой дискуссии спровоцирован отдельными последствиями пандемии COVID-19, которая среди прочего наглядно продемонстрировала, насколько сильно современные компании зависят от подходов к управлению данными, стабильности информационных сетей и, в более широком плане, от появления новых моделей и практик функционирования общественно-политической сферы в технологически развитых государствах, т.е. всего того, что сегодня в совокупности принято обозначать термином «цифровизация» [Билотта, 2020, с. 30–31; Darnis, 2021 b]. Такая трактовка, разумеется, лишь дополняет, а не отменяет более техницистскую интерпретацию феномена цифровизации, в рамках которой последняя подразумевает прежде всего процессы инкорпорации в различные сферы общественной жизнедеятельности специализированных платформ, ресурсов, технологий, решений и практик, позволяющих заменить в конечном итоге традиционные аналоговые коммуникации цифровыми [Во-

¹ Термин «цифровой суверенитет» (*souveraineté numérique*) впервые был предложен авторитетным французским исследователем цифровых технологий Пьером Белланже в качестве замены морально устаревшего, по его мнению, терминологического комплекса «технологический суверенитет», введенного в академический оборот еще в начале 80-х годов прошлого века [Шестопал, Мамычев, 2020, с. 399–400] или даже в 1967 г., когда Научный совет Канады представил стратегию «технологического суверенитета», определив его как инструмент «развития и контроля над технологиями и как средство поддержания национального суверенитета» [Кутюр, Тоупин, 2020, с. 54].

лоденков, 2020, с. 8]. В этой связи нам представляется сложным игнорировать тот факт, что глобальный коронакризис значительно укрепил убежденность большинства европейцев в необходимости как можно скорее достичь стратегической автономии в области разработки собственных цифровых решений [Билотта, 2020]¹. Тем более, что такая установка в полной мере соответствует основополагающим принципам и ценностям ЕС, а также его растущей заинтересованности в инвестициях в цифровую экономику и нормативно-правовой регламентации данной сферы [Autolitano, 2020; Picchiarelli, 2020; Darnis, 2021 b; Martino, 2021].

Тем не менее, несмотря на очевидную значимость проблемы обретения цифрового суверенитета для объединенной Европы, в Брюсселе, по всей видимости, пока не удалось выработать сколь-нибудь универсального подхода к пониманию того, на какие конкретно политико-дипломатические компромиссы в краткосрочной и долгосрочной перспективе готов будет пойти Евросоюз ради достижения этой цели.

К определению цифрового суверенитета

Не лишено проблематичности и само определение цифрового суверенитета [Гаврилов, 2020; Кутюр, Тоупин, 2020; Шестопал, Мамычев, 2020; Autolitano, Pawlowska, 2021, р. 3–5]. Будучи одним из основополагающих принципов, закрепленных в Уставе Организации Объединенных Наций, классический государственный суверенитет тесно связан с другими принципами международного права, такими как: принцип невмешательства в дела, входящие во внутреннюю компетенцию других государств, и принцип разрешения международных споров мирными средствами. В целом концепция цифрового суверенитета, понимаемая на сегодняшний день как право конкретного государства самостоятельно определять ключевые направления, приоритеты и цели своей политики в циф-

¹ Об этой тенденции свидетельствуют также результаты исследований итальянского Института международных отношений (*Istituto Affari Internazionali, IAI*), которые проводились в 2019–2021 гг. в рамках проекта «Геополитика цифрового пространства» (*La geopolitica del digitale*) под руководством доцента Университета Лазурного берега (*Université Côte d'Azur*) Жана-Пьера Дарни [Darnis, 2021 a; Polito, 2021; Autolitano, Pawlowska, 2021; Ghiretti, 2021].

ровой сфере, а также его способность распоряжаться соответствующей инфраструктурой и ресурсами, обеспечивать информационную безопасность и т.п. [Бухарин, 2016, с. 77], к сожалению, до сих пор не получила широкой поддержки мирового сообщества.

Первая проблема, связанная с этим рабочим определением, носит формальный характер и касается вопросов применения международного права к цифровой сфере. В настоящее время активное обсуждение данной проблематики ведется в двух параллельных группах в Организации Объединенных Наций – *UN Group of Governmental Experts* и *UN Open Ended Working Group*, в рамках, в которых заинтересованные государства пытаются разработать систему принципов и норм, которые могли бы эффективно регулировать их поведение в киберпространстве. Среди наиболее дискуссионных тем следует упомянуть определение кибератаки и условия, при которых такая атака может быть квалифицирована как применение силы, и, следовательно, в каких случаях в ответ на кибератаку государство может воспользоваться своим правом на самооборону. Однако все это отчасти нивелируется проблемой относительного бездействия членов международного сообщества в деле продвижения общей повестки дня. В последние годы дебаты по вопросу об управлении Интернетом, как представляется, оказались в тупике из-за банальной неспособности государств договориться об общих целях и задать более или менее единый вектор международного сотрудничества в цифровой сфере [Darnis, 2021 a; Martino, 2021].

Таким образом, утверждение цифрового суверенитета ЕС происходит в условиях постоянно меняющейся парадигмы международной среды, единственная константа которой, собственно, и заключается в ее неопределенности. Очевидно, что такая ситуация может иметь серьезные последствия для Брюсселя, поскольку и само стремление европейцев к цифровому суверенитету, и его достижение могут быть совершенно по-разному восприняты партнерами ЕС в различных регионах мира. В частности, в случае с Китаем его интерпретация концепта «цифровой суверенитет» в значительной степени обусловлена самим суверенным субъектом, т.е. цифровой суверенитет Китая (как суверенитет-для-себя) и цифровой суверенитет условной Европы (как пример суверенитета-для-других) теоретически вполне могут трактоваться Пекином в противоположном ключе. Тем не менее, общая тенденция такова, что китайским приоритетом в области цифровой безопасности и

управления интернетом традиционно принято считать стремление официального Пекина балканизировать киберпространство с тем, чтобы каждое государство могло наиболее эффективно контролировать информационный контент и всю цифровую инфраструктуру на своей территории [Todaro, 2020]. Не случайно в качестве хрестоматийного примера такой политики и в западных, и в российских исследованиях неизменно приводят именно китайскую систему фильтрации контента, известную под названием «Золотой щит», или «Великий китайский файрвол» (*The Great Firewall of China*) [см., например: Polito, 2021, p. 3; Барышников, Туленков, 2012, с. 126].

Препятствия на пути обретения Европой цифрового суверенитета

Отдельный интерес для исследователей цифрового суверенитета в европейском контексте, безусловно, представляют те препятствия, которые стоят на пути европейского проекта по созданию на территории ЕС «самобытного информационно-телекоммуникационного пространства, которое отличалось бы независимостью от любого внешнего влияния» [Панцеров, 2019, с. 12]. В этой связи мы, вслед за исследователями Каролиной Полито и Жаном-Пьером Дарни из Института международных отношений (Рим, Италия), считаем целесообразным выделить два комплекса факторов, препятствующих на сегодняшний день успешной реализации европейского цифрового суверенитета [Darnis, 2021 b; Polito, 2021, p. 3–5], как то: зависимость европейцев от иностранных цифровых технологий и услуг, а также относительно низкий уровень европейских инвестиций в цифровую сферу (по сравнению с другими технологически развитыми государствами [подробнее см.: Autolitano, Pawlowska, 2021]).

Зависимость от иностранных цифровых технологий и услуг. В условиях отсутствия у ЕС сколько-нибудь полноценной стратегической автономии в глобальных цепочках добавленной стоимости (ГЦДС) весьма показателен пример технологии 5 G, ГЦДС которой характеризуется, в первую очередь, двумя параметрами. Это, с одной стороны, сильная взаимозависимость и глобальное производство, в значительной степени ориентированное на различные географические регионы мира, – с другой. Здесь (в рамках ГЦДС 5 G)

европейские компании, бесспорно, занимают лидирующие позиции (особенно если говорить об оптической литографии, или фотолитографии как о наиболее универсальной технологии, используемой в производстве полупроводниковых интегральных микросхем) [Polito, 2021, p. 4]. Однако растущая обеспокоенность представителей европейского экспертно-аналитического сообщества связана с тем, что на данном рынке все чаще доминируют иностранные компании, под контролем которых в перспективе могут оказаться и довольно крупные сегменты этой цепочки.

В частности, Европейский парламент выразил озабоченность по поводу роли китайских технологических компаний, таких как *Huawei* и *ZTE*, на европейском рынке *5 G* и, в более общем плане, относительно растущей зависимости Европы от отдельных поставщиков оборудования и комплектующих из КНР и других стран. Очевидно, что эти опасения европейских парламентариев связаны не только с соображениями кибербезопасности, но и с имеющимися вопросами в отношении поставок основных комплектующих, необходимых для эффективного развертывания сетей *5 G* в периоды сильной напряженности и растущей международной конкуренции. Более того, эти опасения, разумеется, не ограничиваются одним только рынком *5 G*, и они, будучи экстраполированы на более высокий уровень, адресуют нас к проблеме общей зависимости Европы от импорта важнейших видов сырья, о чем говорится в том числе и в новой промышленной стратегии ЕС¹. Так, если основными комплектующими, которые необходимы для производства практически всех инновационных цифровых технологий, являются жесткие диски, полупроводники и аккумуляторы, то поставки указанных комплектующих в Европу осуществляются преимущественно китайскими компаниями².

Другим примером информационно-технологической зависимости ЕС от иностранных партнеров является использование облачных технологий. Государства – члены Евросоюза практически лишены возможности контролировать данные, передача которых

¹ Una nuova strategia industriale per l'Europa (COM/2020/102) // Commissione europea. – 2020. – March 10. – Mode of access: <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52020DC0102> (accessed: 27.04.2021).

² Theodosopoulos V. Looking beyond 5G: Why Europe Is Far from Naïve when It Comes to Issues of Strategic Dependence // EUROPP blog. – 2020. – July 20. – Mode of access: <https://wp.me/p2MmSR-cPI> (accessed: 27.04.2021).

происходит при помощи облачных сервисов, поскольку они, как правило, оказываются под юрисдикцией США, что неизбежно подвергает граждан и резидентов ЕС, частные предприятия и даже европейские органы государственной власти угрозе конфликта юрисдикций, который может потенциально возникнуть в этой связи¹.

Дефицит инвестиций как стратегическая угроза цифровому суверенитету ЕС. Рассмотренные выше проблемы напрямую связаны со вторым крупным комплексом препятствий на пути реализации европейского суверенитета в цифровой сфере. Речь идет об относительно слабой привлекательности европейских компаний (по сравнению с компаниями КНР и США) для зарубежных инвесторов и вытекающей отсюда их сравнительно невысокой конкурентоспособности на глобальном рынке цифровых технологий. Так, по мнению европейского политолога Андреаса Актудианакиса, возможности ЕС конкурировать на мировом рынке облачных хранилищ данных в значительной степени ограничены. Лидерами на этом рынке сегодня являются *Amazon* (45%), *Microsoft* (17,9%), *Alibaba* (9,1%), *Google* (5,3%) и *Tencent* (2,8%). Согласно экспертным оценкам, 92% данных, полученных на Западе, в настоящее время хранятся в США, в то время как лишь 4% этих данных размещены на серверах, расположенных в Европе².

Что же касается рынка *5 G*, успешному внедрению этой технологии в Европе препятствуют задержки с переходом от инфраструктуры *4 G* к *5 G*, которые в конечном итоге значительно усугубляют технологическое отставание Европы, не позволяя ей в полной мере завершить переход хотя бы к технологии *4 G*. Кроме того, аукционы по распределению частотных диапазонов *5 G* были особенно дорогими в Европе, что также не могло не повлиять на снижение доходности инвестиций; в то время как сложные процедуры распределения этих диапазонов на фоне слабой координации процесса принятия решений в ЕС еще больше подорвали планы частных инвесторов.

¹ Aktoudianakis A. Fostering Europe's Strategic Autonomy. Digital Sovereignty for Growth, Rules and Cooperation // EPC Analyses. – 2020. – December. – Mode of access: <https://www.epc.eu/en/Publications/~3a8090> (accessed: 27.04.2021).

² Ibid.

Наконец, еще одним объяснением относительного дефицита европейских инвестиций в цифровую сферу является область искусственного интеллекта. Здесь Европа следует за Китаем и США с точки зрения венчурного капитала (рисковый капитал, инвестируемый третьими сторонами для финансирования начала деятельности в отраслях с высоким потенциалом развития). Искусственный интеллект для Европы можно считать основой ее экономического развития и краеугольным камнем инноваций всего европейского континента [Picchiarelli, 2020; Ghiretti, 2021], тогда как в более общем плане данная область может вызывать практический интерес в том числе и в контексте разработки и внедрения аппаратных и программных технологий¹.

Европейская стратегия и проект *GAIA-X*

Европейская комиссия осуществляет долгосрочную стратегию по решению этих проблем и реализует ряд инициатив в рамках «Европейской стратегии в области данных»². Главная цель этой стратегии заключается в том, чтобы гарантировать свободную передачу данных через государства-члены ЕС, обеспечивая при этом полное соблюдение всех европейских стандартов и правил, касающихся, в частности, конфиденциальности и защиты данных, а также правил относительно доступа к этим данным и их использования. Непосредственно в тексте стратегии говорится, что ЕС стремится:

- установить четкие и справедливые правила доступа к данным и их повторного использования;
- инвестировать в инструменты и инфраструктуру для хранения и обработки данных, объединив усилия в развитии облачных технологий Европы;
- поддержать создание ряда единых европейских пространств данных в стратегических областях;

¹ Castro D., McLaughlin M. Who Is Winning the AI Race: China, the EU, or the United States? – 2021 Update // Center for Data Innovation. – 2021. – January. – Mode of access: <https://datainnovation.org/?p=14466> (accessed: 27.04.2021.)

² Una strategia europea per i dati (COM/2020/66) // Commissione europea. – 2020. – February 19. – Mode of access: <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52020DC0066> (accessed: 27.04.2021).

▪ предоставить пользователям права, инструменты и компетенции для осуществления полного контроля над их персональными данными.

Что касается планов Еврокомиссии по наращиванию потенциала в сфере облачных технологий, в этой связи нельзя не упомянуть амбициозную европейскую инициативу *GALIA-X*. Последняя является некоммерческой организацией, созданной 22 членами, среди которых не только поставщики облачных услуг, но и рядовые пользователи, а также представители академического сообщества. Более 160 партнеров по всему миру, включая американские и китайские компании, вносят свой вклад в проект *GALIA-X*, хотя и предполагается, что каждая участвующая в нем компания должна базироваться в ЕС. Цель *GALIA-X* заключается в создании универсальных «информационных пространств», предназначенных для пользователей, которые хотят обмениваться своими бизнес-данными [Autolitano, Pawlowska, 2021, p. 12–18]. Вполне очевидно, что такие информационные пространства должны обеспечивать: а) общую онтологию обмена данными, предусматривающую единые механизмы, при помощи которых пользователь мог бы идентифицировать, использовать или запрашивать необходимые ему данные; а также б) оперативную совместимость между различными поставщиками облачных услуг. Так, например, *Philips* планирует создать специализированное информационное пространство в сфере здравоохранения, к участию в котором смогут подключиться отдельные больницы, частные компании и другие пользователи, заинтересованные в данной сфере. В таком случае любой пользователь получает возможность обращаться к этим данным, не переключаясь между различными поставщиками облачных услуг, что в конечном итоге и является основной целью проекта *GALIA-X* – обеспечить максимально возможную совместимость и расширить существующие на сегодняшний день возможности переноса данных между различными облачными сервисами¹.

¹ Microsoft. Decoding Europe's Data Sovereignty (video). – 2020. – December 10. – Mode of access: <https://www.politico.eu/event/decoding-europes-data-sovereignty> (accessed: 27.04.2021).

Отсутствие системы глобального управления данными

Едва ли имеет смысл рассматривать Европейскую стратегию в области данных в отрыве от международного контекста. Но здесь мы наталкиваемся на любопытный парадокс: ключевой проблемой глобального управления данными на сегодняшний день является его отсутствие как таковое. Для того чтобы быть эффективной, глобальная экономика данных требует взаимного доверия между различными участниками международного общения, а его в современных условиях, как представляется, явно не хватает. В 2019 г. Япония, будучи председателем *G20*, призвала участников клуба к созданию набора международных правил, которые способствовали бы свободному перемещению данных поверх государственных границ. Эта концепция, известная как «свободный поток данных на основе взаимного доверия», была впервые упомянута тогдашним премьер-министром Японии Синдзо Абэ в его речи на ежегодном совещании Всемирного экономического форума в Давосе (Швейцария) в январе 2019 г. *«Мне бы хотелось, чтобы осацкая Группа двадцати надолго запомнилась как саммит, который дал старт глобальному управлению данными»*, – сказал он в своем выступлении¹. Однако японское предложение о «свободном потоке данных на основе взаимного доверия» не сумело пройти испытание суровой практикой международной жизни, в которой это взаимное доверие серьезно подорвано.

К примеру, государства – члены ЕС преисполнены скепсиса, когда речь заходит о гарантиях конфиденциальности и кибербезопасности, введенных другими странами. В этом отношении имеет место существенное различие между философскими подходами к политике управления данными, которых придерживаются США и страны континентальной Европы. Не совпадают, соответственно, и правовые системы ЕС и США в области управления персональными данными, так как основаны они на двух радикально отличающихся друг от друга концепциях права на неприкосновенность частной жизни. Так, после принятия Общего регламента защиты

¹ Abe S. *Toward a New Era of “Hope-Driven Economy”*: the Prime Minister’s Keynote Speech at the World Economic Forum Annual Meeting. – 2019. – January 23. – Mode of access: http://japan.kantei.go.jp/98_abe/statement/201901/_00003.html (accessed: 27.04.2021).

персональных данных (*General Data Protection Regulation, GDPR*) ЕС создал централизованную систему защиты персональных данных своих граждан, тогда как правовая система США исходит из необходимости регулировать обработку данных в конкретных отраслях экономики (например, в сфере здравоохранения). Иными словами, в США неприкосновенность частной жизни охраняется только в контексте коммерческой практики, когда субъект данных, претендующий на какие-либо гарантии со стороны государства, рассматривается скорее как потребитель, а не гражданин. Этот подход находит свое отражение и в том, что в качестве основного органа по защите частной жизни в США выступает Федеральная торговая комиссия – независимое агентство американского правительства, призванное защищать права потребителей. В Европе же принцип неприкосновенности частной жизни был изначально сформулирован в рамках Европейской конвенции о защите прав человека и основных свобод 1950 г. и впоследствии подтвержден в Хартии ЕС об основных правах от 7 декабря 2000 г.

Эти различия нередко приводят к серьезным противоречиям между традиционными режимами управления данными на противоположных берегах Атлантики и порождают немало вопросов относительно возможных путей и способов сопряжения правовых систем ЕС и США. Показательным в этом смысле можно считать решение Европейского суда в отношении трансатлантического соглашения *Privacy Shield*, которое признало данный механизм неэффективным и недостаточным для гарантирования права граждан ЕС на защиту их персональных данных¹. Помимо рядовых граждан и резидентов Евросоюза это решение неминуемо затронет по меньшей мере 5 300 европейских компаний, которые в течение последних лет использовали *Privacy Shield* в качестве управленческого инструмента для обмена данными с американскими партнерами. Более того, Европейский суд не просто аннулировал соглашение *Privacy Shield*, но и сформулировал так называемые «стандартные договорные условия», представляющие собой набор положений, устанавливающих договорные обязательства для экспортеров и

¹ Sentenza nella causa C-311/18: Data Protection Commissioner v. Facebook Ireland Ltd e Maximillian Schrems // Corte di Giustizia dell'Unione europea. – 2020. – July 16. – Mode of access: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&doclang=IT> (accessed: 27.04.2021).

импортеров данных, которые многие европейские компании приняли для облегчения передачи необходимых данных своим иностранным партнерам. После вынесения решения суда стороны должны будут следить за соответствием используемых ими систем передачи данных новым европейским стандартам. Такое положение вещей представляется крайне обременительным, прежде всего для экспортеров данных, которым предстоит взвалить на себя задачу по исправлению «недостатков» правовой системы США с тем, чтобы последующий трансатлантический обмен данными в полной мере соответствовал требованиям «стандартных договорных условий» ЕС. В этом смысле решение Европейского суда имеет почти идеологическое значение, предполагая, что право на защиту данных нуждается в объективной защите, которая не заканчивается на этапе переговоров между заинтересованными сторонами. Последствия этого решения для частного сектора определенно будут иметь большое значение, поскольку они не только заставят компании, в том числе и европейские, инвестировать огромные ресурсы в изучение правовой системы США, но и могут стать ощутимым препятствием на пути поощрения конкурентоспособности европейских многонациональных компаний, действующих на обоих рынках.

В то же время еще одним аспектом, существенно ограничивающим международный обмен данными в глобальном и региональном масштабе, безусловно, является общемировая тенденция к локализации данных. Такая локализация может напрямую предписываться законом или являться следствием ограничительных мер политического характера, которые в конечном итоге либо значительно осложняют процесс передачи данных, либо и вовсе делают его невозможным. Подобного рода политика, как правило, требует от компаний хранить резервную копию данных на местном уровне, обрабатывать данные также на местном уровне и заручаться согласием со стороны отдельных лиц или правительства, когда необходимо эти данные куда-либо передать. В настоящее время в ЕС не существует специальных нормативно-правовых актов в отношении политики локализации данных, если, конечно, не рассматривать аннулирование вышеупомянутого трансатлантического соглашения *Privacy Shield* как меру по имплицитной инкорпорации в европейскую правовую систему соответствующего требования об обязательной локализации данных. Тем не менее, в целом ряде госу-

дарств, включая Россию, Объединенные Арабские Эмираты, Вьетнам, Саудовскую Аравию и Индию, законы о локализации данных уже действуют [Polito, 2021, p. 8]. Здесь же, например, уместно будет вспомнить, как Резервный банк Индии в апреле 2018 года попросил иностранные платежные компании хранить все данные, касающиеся сделок с участием индийских граждан, исключительно на серверах, размещенных на индийской территории [Polito, 2019, p. 118].

Все эти аспекты в совокупности заставляют усомниться в перспективах практической применимости концепции глобального управления данными на современном этапе, что демонстрирует если не принципиальную ошибочность данной теоретической концепции, то, во всяком случае, ее излишне предварительный характер в условиях, когда взаимная напряженность и недоверие, как представляется, превалируют над возможностями международного сотрудничества.

Неизбежность использования модели многостороннего участия

Отсутствие внятной системы глобального управления данными среди прочего может быть следствием того положения, в котором пребывает современная мировая политическая система в целом. Согласно теории системных изменений, с геополитической точки зрения исторический момент, в котором мы живем, можно определить как момент гегемонистского перехода. Последовательные апологеты гегемонистских теорий общественно-политического развития (Р. Гилпин [Gilpin, 1987], А. Органски [Organski, 1968], Ч. Киндлбергер [Kindleberger, 1973], С. Краснер [Krasner, 1976], Т. Маккьюэн [McKeown, 1983], А. Стейн [Stein, 1984] и Э. Мэнсфилд [Mansfield, 1992]), как правило, в своих трудах называют технологическое лидерство и бесперебойный доступ к экономическим ресурсам в числе ведущих факторов, способных обеспечить появление на международной арене очередной гегемонистской державы¹. Со временем некогда пере-

¹ См., например, классическую работу «Война и изменение в мировой политике» (1981) Роберта Гилпина, чья интерпретация теории гегемонистской стабильности (гегемонизма) приобрела наибольшую популярность в рамках неореа-

довые технологии распространяются среди других участников международной системы и перестают быть конкурентным преимуществом гегемона, в результате чего влияние последнего постепенно утрачивается. Представим себе классическую международную систему, состоящую из n государств, в которой государство i (не гегемонистский элемент системы n) примет решение не проводить ревизионистскую политику до тех пор, пока выгоды, гарантированные поддержанием статус-кво, не превысят соответствующие издержки. Однако когда государство i начнет считать, что издержки от поддержания статус-кво ощутимо превышают конкретные выгоды от сложившегося международного положения, оно попытается изменить ситуацию либо: а) путем территориальной экспансии, либо б) посредством увеличения экономического роста и интенсификации военно-технического развития (или же используя оба сценария одновременно). В свете такого рода теоретических predispositions торговую войну между Соединенными Штатами и Китаем можно рассматривать как проявление попытки гегемонистской державы (США) сдержать рост Китая или, по крайней мере, ограничить его геополитическое и геостратегическое влияние. Учитывая размеры рынков США и Китая, оба государства в совокупности образуют на сегодняшний день своего рода цифровую дуополию, которая периодически сотрясается санкционными или торгово-экономическими войнами¹, по инициативе то одной, то другой стороны. Так, например, недавнее противостояние между двумя экономическими гигантами заключалась во введении администрацией Трампа 25-процентной пошлины на китайский импорт (включая и товары, связанные с искусственным интеллектом) общей стоимостью в 34 миллиарда долларов, на что Китай отреагировал симметричными мерами, введя 25-процентные пошлины на 540 американских товаров [Бирон, 2019; Mialhe, 2018, p. 105–117].

Казалось бы, описанная выше модель не только отлично иллюстрирует современное международное положение с точки зре-

лизма [Gilpin, 1981]. Кроме того, тема гегемонии развивается на иной идейной основе в парадигме глобализма [Chase-Dunn, Rubinson, 1977; Chase-Dunn, 1989; Boswell, 1995].

¹Подробнее о категориально-теоретическом размежевании торговых и санкционных войн можно почитать, например, в работах И.Н. Тимофеева [Тимофеев, 2018, с. 33–36] или Д.В. Мухамадеева и Я.Н. Шевченко [Мухамадеев, Шевченко, 2020].

ния теории системных изменений, но и довольно точно отображает актуальные реалии международно-политической жизни в том виде, в каком ее привыкли обсуждать зачастую далекие от теоретической схоластики политики-практики и разного рода политические обозреватели. Тем не менее необходимо отметить, что данная модель совершенно не учитывает роли частного сектора и, в более широком плане, влияния различных заинтересованных сторон в определении глобального геополитического баланса, в том числе и в цифровой сфере. Такие американские и китайские компании, как *Google*, *Apple*, *Facebook*, *Amazon* и *Microsoft*, а также *Baidu*, *Huawei*, *Alibaba*, *Tencent* и *Xiaomi*, соответственно, будучи не только лидерами в области высоких технологий, но и конечными обладателями контроля над накопленными данными, все чаще поддаются искушению использовать свое экономическое и информационно-технологическое могущество в политических целях (например, для усиления своих переговорных позиций на международной арене). С другой стороны, в новых условиях изменившейся парадигмы международной среды, в эпоху дисплейной коммуникации [Костомаров, 2010] и тотальной цифровизации даже рядовые пользователи ИКТ и цифровых услуг приобретают более важное стратегическое значение. Без их доверия к новым цифровым разработкам и внедряемым информационным системам развитие современной цифровой экосистемы невозможно, как невозможно без учета многостороннего участия и определение геополитического баланса будущего.

В этом контексте частный сектор и пользователи во всем мире, в отличие от суверенных государств или их региональных блоков, имеют в основном более схожие интересы. Именно по этой причине модель управления, которая в последние годы предлагается в качестве наиболее оптимальной для цифрового сектора, есть, по сути, модель инклюзивная. Она направлена прежде всего на то, чтобы дать право голоса максимальному числу заинтересованных субъектов, что, безусловно, является сильной стороной данной модели (хотя и она не лишена отдельных недостатков и требует известной корректировки). В этой связи государствам придется прислушиваться к потребностям и нуждам не только традиционных, но и широкого круга негосударственных акторов, с тем чтобы на новом витке международно-политического развития пожинать плоды взаимовыгодного сотрудничества, а не возвращаться к рас-

ширенной версии сценария «война всех против всех» с поправкой на цифровые реалии. Однако не менее важно, как нам представляется, чтобы расширение круга субъектов глобальной и региональной международной политики в цифровую эпоху не приводило к тому, чтобы интересы суверенных государств оказались подчинены потребностям частного сектора.

Заключение

В статье были подвергнуты теоретическому анализу проблемы, ставшие предельно актуальными в условиях новой цифровой реальности. Последняя включает в себя расширенный инструментарий коммуникаций (в том числе и дисплейной [Костомаров, 2010]), ресурсы и технологии *Big Data*, искусственный интеллект и нейросетевые алгоритмы работы с цифровыми данными, технологии наблюдения и распознавания визуальных образов, а также модели профилирования граждан на основе их персональных цифровых следов [Володенков, 2020, с. 7]. Иными словами, современная цифровая среда существования людей не столько противопоставляется традиционной «офлайновой» среде, сколько имплементируется в нее, вызывая к жизни все новые синергетические эффекты и порождая новые риски.

▪ В этом контексте попытки Европы утвердить свой суверенитет в цифровой сфере сталкиваются с очевидными проблемами, такими как зависимость ЕС от иностранных технологий и услуг, а также известный дефицит инвестиций, которые прежде направлялись на поддержку европейской промышленной политики.

▪ Евросоюз пытается преодолеть эти проблемы с помощью амбициозной стратегии, эффективность которой, однако, может быть оценена только в перспективе нескольких лет. Данная стратегия в значительной степени зависит от международного контекста, в котором, хотя и проявляется интерес к проблемам цифровой экономики, отсутствует система глобального управления данными.

▪ Международная система в посткоронавирусную эпоху характеризуется глубокой напряженностью между основными субъектами международного общения, каждый из которых стремится реализовать свою собственную автономию, в том числе и в цифровой сфере. Во многом эта напряженность вызвана глубокой и

структурной перестройкой геополитического равновесия на глобальном и региональном уровне, что отражается также и в растущей конкуренции между США и Китаем.

▪ Представляется, что для эффективного управления в цифровом секторе необходимо использовать подход, предусматривающий вовлечение максимально широкого круга участников, заинтересованных в определении общих правил обеспечения «свободного потока данных на основе взаимного доверия» во всемирном масштабе, что, однако, не должно приводить к отказу от роли государства в регулировании рынка. Государство в цифровую эпоху должно быть органичной частью цифровой экосистемы, и даже фундаментальной ее частью, потому что только государство может в конечном итоге защитить интересы своих граждан.

Ya.N. Shevchenko*

Digital sovereignty for Europe in the context of global data governance

Abstract. The European Union (EU) has been advocating a strategy to assert its digital sovereignty for a relatively long period of time. This attempt, however, runs up against a range of obvious problems and obstacles, such as a united Europe's dependence on foreign technologies and services and the inadequacy of investments made to support its industrial policy (in particular in the digital sphere). The EU is trying to overcome these problems with an ambitious strategy, the "European strategy for data", which will enable the Union to navigate in an international context characterized by a substantial lack of a global data governance system, but the efficiency and effectiveness of the strategy can only be assessed in a few years' time. According to the author of this paper's point of view, to achieve its policy objectives, the EU must pay attention to safeguarding the competitiveness of its companies, pursuing policies that, in defending the right to privacy and security of European users, are clear and harmonized. At the same time, the EU must implement policies that are able to redistribute the wealth produced in the digital field, countering the current dangerous concentrations of wealth and power in the hands of a few oligopolistic companies.

Keywords: digital sovereignty; European Union; cybersecurity; global governance; personal data; digital geopolitics.

For citation: Shevchenko Ya.N. Digital sovereignty for Europe in the context of global data governance. *Political science (RU)*. 2021, N 3, P. 251–270. DOI: <http://www.doi.org/10.31249/poln/2021.03.11>

* **Shevchenko Yan**, Saint Petersburg State University (St. Petersburg, Russia), e-mail: ian.chevtchenko@gmail.com

References

- Autolitano S. A Europe fit for the digital age: the quest for cybersecurity unpacked. *IAI Papers*. 2020, N 20|07, P. 1–5.
- Autolitano S., Pawlowska A. Europe's quest for digital sovereignty: GAIA-X as a case study. *IAI Papers*. 2021, N 21|14, P. 1–22.
- Baryshnikov D.N., Tulenkov A.Yu. “Digital diplomacy” and the state sovereignty at the age of globalization. *Vestnik of Saint Petersburg University. Series 6. Philosophy. Culturology. Political science. Law. International relations*. 2012, N 4, P. 121–128. (In Russ.)
- Bilotta N. Beyond the digital tax: the challenges of the EU’s scramble for technological sovereignty. *International organisations research journal*. 2020, Vol. 15, N 4, P. 30–47. DOI: <http://doi.org/10.17323/1996-7845-2020-04-02> (In Russ.)
- Biron Yu.S. US-China trade war: the fight for influence in Sub-Saharan Africa. *Theories and problems of political studies*. 2019, Vol. 8, N 2 A, P. 141–150. (In Russ.)
- Boswell T. Hegemony and bifurcation points in world history. *Journal of world-systems research*. 1995, Vol. 1, N 1, P. 178–209. DOI: <https://doi.org/10.5195/jwsr.1995.49>
- Bukharin V.V. The Russian’s digital sovereignty as a technical basis of information security. *MGIMO review of international relations*. 2016, N 6 (51), P. 76–91. (In Russ.)
- Chase-Dunn C. *Global formation: structures of the world economy*. Cambridge : Basil Blackwell, 1989, 419 p.
- Chase-Dunn C., Rubinson R. Toward a structural perspective on the world-system. *Politics & society*. 1977, Vol. 7, N 4, P. 453–476. DOI: <https://doi.org/10.1177/003232927700700403>
- Couture S., Toupin S. What does the notion of “sovereignty” mean when referring to the digital? *International organisations research journal*. 2020, Vol. 15, N 4, P. 48–69. DOI: <https://doi.org/10.17323/1996-7845-2020-04-03> (In Russ.)
- Darnis J.-P. Le relazioni transatlantiche al tempo del digitale: la questione del trasferimento di dati. *IAI Papers*. 2021 a, N 21|02, P. 1–11.
- Darnis J.-P. L’Union européenne entre autonomie stratégique et souveraineté technologique: impasses et opportunités. *FRS Recherches & Documents*. 2021 b, N 8, 17 p. (In French.)
- Gavrilov E.O. Digital sovereignty in the context of globalization: philosophical and legal aspects. *Bulletin of Kemerovo State University. Series: humanities and social sciences*. 2020, Vol. 4, N 2 (14), P. 146–152. DOI: <https://doi.org/10.21603/2542-1840-2020-4-2-146-152> (In Russ.)
- Ghiretti F. Technological Competition: Can the EU Compete with China? *IAI Papers*. 2021, N 21|15, P. 1–17.
- Gilpin R. *The political economy of international relations*. Princeton : Princeton university press, 1987, 472 p.
- Gilpin R. *War and change in world politics*. New York, Cambridge : Cambridge university press, 1981, 272 p.
- Kindleberger C.P. *The world in Depression, 1929–1939*. Berkeley : University of California press, 1973, 344 p.

- Kostomarov V.G. Display text as a form of network communication. *Russian language journal*. 2010, Vol. 60, P. 139–145. (In Russ.)
- Krasner S. State power and the structure of international trade. *World politics*. 1976, Vol. 28, N 3, P. 317–343. DOI: <https://doi.org/10.2307/2009974>
- Mansfield E.D. The Concentration of capabilities and international trade. *International organization*. 1992, Vol. 46, N 3, P. 731–764. DOI: <https://doi.org/10.1017/s0020818300027880>
- Martino L. Le iniziative diplomatiche per il cyberspazio: punti di forza e di debolezza. *IAI Papers*. 2021, N 21|13, P. 1–18. (In Italian.)
- McKeown T.J. Hegemonic stability theory and 19 th century tariff levels in Europe. *International organization*. 1983, Vol. 37, P. 73–91. DOI: <https://doi.org/10.1017/s0020818300004203>
- Miaillhe N. Géopolitique de l'Intelligence artificielle: le retour des empires? *Politique étrangère*. 2018, N 3, P. 105–117. DOI: <https://doi.org/10.3917/pe.183.0105> (In French.)
- Mukhamadeev D.V., Shevchenko Ya.N. Trade, economic and sanctions wars: an attempt to theoretically differentiate the ideas in the context of the international relations science. *World politics*. 2020, N 1, P. 12–22. DOI: <https://doi.org/10.25136/2409-8671.2020.1.29072> (In Russ.)
- Organski A.F.K. *World politics*. New York : Knopf, 1968, 509 p.
- Pantserev K. States of Sub-Saharan Africa at the digital age: to the problem of the ensuring of the information sovereignty. *Asia and Africa today*. 2019, N 10, P. 10–16. DOI: <https://doi.org/10.31857/s032150750006520-4> (In Russ.)
- Picchiarelli A. Per un'intelligenza artificiale a misura d'uomo: una possibile regolamentazione valoriale? *IAI Papers*. 2020, N 20|47, P. 1–14. (In Italian.)
- Polito C. Il future dell'Internet governance e le crescenti spinte verso una sovranità cibernetica. In: Darnis J.-P., Polito C. (eds). *La geopolitica del digitale*. Rome, Nuova Cultura, 2019, P. 105–121. (In Italian.)
- Polito C. La governance globale dei dati e la sovranità digitale europea // *IAI Papers*. 2021, N 21|11, P. 1–12. (In Italian.)
- Shestopal S.S., Mamychev A. Yu. Sovereignty in the global digital space: current trends. *Baltic humanitarian journal*. 2020, Vol. 9, N 1 (30), P. 398–403. DOI: <https://doi.org/10.26140/bgz3-2020-0901-0098> (In Russ.)
- Stein A.A. The hegemon's dilemma: Great Britain, the United States, and the international economic order. *International organization*. 1984, Vol. 38, P. 355–386. DOI: <https://doi.org/10.1017/s0020818300026758>
- Timofeev I.N. Economic sanctions as a concept of power politics. *MGIMO review of international relations*. 2018, N 2 (59), P. 26–42. DOI: <https://doi.org/10.24833/2071-8160-2018-2-59-26-42> (In Russ.)
- Todaro D. Tecnologia e azione pubblica in Cina: il codice sanitario individuale e le principali tendenze delle politiche digitali cinesi contemporanee. *IAI Papers*. 2020, N 20|46, P. 1–16. (In Italian.)
- Volodenkov S.V. The contemporary political processes transformation in the context of society digitalization: key scenarios. *Outlines of global transformations: politics, economics, law*. 2020, Vol. 13, N 2, P. 6–24. DOI: <https://doi.org/10.23932/2542-0240-2020-13-2-1> (In Russ.)

Литература на русском языке

- Барышников Д.Н., Туленков А.Ю.* «Цифровая дипломатия» и государственный суверенитет в эпоху глобализации // Вестник Санкт-Петербургского университета. Серия 6: Философия. Культурология. Политология. Право. Международные отношения. – 2012. – № 4. – С. 121–128.
- Билотта Н.* Что стоит за цифровым налогом: вызовы борьбы Европейского союза за технологический суверенитет // Вестник международных организаций: образование, наука, новая экономика. – 2020. – Т. 15, № 4. – С. 30–47. – DOI: <https://doi.org/10.17323/1996-7845-2020-04-02>
- Бирон Ю.С.* Торговая война США и Китая: борьба за влияние в Африке южнее Сахары // Теории и проблемы политических исследований. – 2019. – Т. 8, № 2 А. – С. 141–150.
- Бухарин В.В.* Компоненты цифрового суверенитета Российской Федерации как техническая основа информационной безопасности // Вестник МГИМО-Университета. – 2016. – № 6 (51). – С. 76–91.
- Володенков С.В.* Трансформация современных политических процессов в условиях цифровизации общества: ключевые сценарии // Контуры глобальных трансформаций: политика, экономика, право. – 2020. – Т. 13, № 2. – С. 6–24. – DOI: <https://doi.org/10.23932/2542-0240-2020-13-2-1>
- Гаврилов Е.О.* Цифровой суверенитет в условиях глобализации: философский и правовой аспекты // Вестник Кемеровского государственного университета. Серия Гуманитарные и общественные науки. – 2020. – Т. 4, № 2 (14). – С. 146–152. – DOI: <https://doi.org/10.21603/2542-1840-2020-4-2-146-152>
- Костомаров В.Г.* Дисплейный текст как форма сетевого общения // Russian Language Journal. – 2010. – Vol. 60. – P. 139–145.
- Кутюр С., Тоулин С.* Что означает понятие «суверенитет» в цифровом мире? // Вестник международных организаций: образование, наука, новая экономика. – 2020. – Т. 15, № 4. – С. 48–69. – DOI: <https://doi.org/10.17323/1996-7845-2020-04-03>
- Мухаммадеев Д.В., Шевченко Я.Н.* Войны торгово-экономические и санкционные: попытка теоретического размежевания в свете науки о международных отношениях // Мировая политика. – 2020. – № 1. – С. 12–22. – DOI: <https://doi.org/10.25136/2409-8671.2020.1.29072>
- Панцеров К.А.* Страны Африки южнее Сахары в цифровую эпоху: к вопросу обеспечения информационного суверенитета // Азия и Африка сегодня. – 2019. – № 10. – С. 10–16. – DOI: <https://doi.org/10.31857/s032150750006520-4>
- Тимофеев И.Н.* Экономические санкции как политическое понятие // Вестник МГИМО-Университета. – 2018. – № 2 (59). – С. 26–42. – DOI: <https://doi.org/10.24833/2071-8160-2018-2-59-26-42>
- Шестопал С.С., Мамычев А.Ю.* Суверенитет в глобальном цифровом измерении: современные тренды // Балтийский гуманитарный журнал. – 2020. – Т. 9, № 1(30). – С. 398–403. – DOI: <https://doi.org/10.26140/bgз3-2020-0901-0098>