

ОРИГИНАЛЬНАЯ СТАТЬЯ

DOI: 10.26794/2226-7867-2021-11-6-67-72
УДК 321.01(045)

Регулирование IT-сферы как политико-теоретическая и практическая проблема*

С.П. Митрахович

Финансовый университет, Москва, Россия
<https://orcid.org/0000-0003-2252-6006>

АННОТАЦИЯ

В статье рассматривается вопрос развития теоретических и практических представлений о значимости политического регулирования IT-сферы, а также государственного контроля над определенными компаниями, относящимися к информационной отрасли. И западный, и китайский опыт в вопросах регулирования IT-сферы парадоксальным образом оказываются сходны в попытках ограничить число игроков, занимающихся большими данными, организациями работы ключевых цифровых платформ и т.п. В России глобальный масштаб проблемы IT-олигархии, которую практически невозможно регулировать на уровне отдельно взятого национального государства, усиливается еще и традиционным подходом властей и оппозиции (включая интеллектуальную фронду различных идеологических оттенков) к оправданию своих действий и позиций ссылками на зарубежный опыт, что побуждает к его изучению.

Ключевые слова: IT; большие данные; олигархия; регулирование

Для цитирования: Митрахович С.П. Регулирование IT-сферы как политико-теоретическая и практическая проблема. *Гуманитарные науки. Вестник Финансового университета*. 2021;11(6):67-72. DOI: 10.26794/2226-7867-2021-11-6-67-72

ORIGINAL PAPER

Regulation of the IT Sphere as a Politico-Theoretical and Practical Problem**

S.P. Mitrakhovich

Financial University, Moscow, Russia
<https://orcid.org/0000-0003-2252-6006>

ABSTRACT

The article discusses the development of theoretical and practical ideas about the significance of political regulation of the IT sphere, state control over certain campaigns related to the information industry. Both Western and Chinese experience in regulating the IT sphere is paradoxically similar in attempts to limit the number of players involved in big data, organizations of key digital platforms and the like. In Russia, the global scale of the problem of IT oligarchy also makes it necessary to study it. It is conditioned by almost impossible regulation at the level of a single national state alone. Besides, it is strengthened by the traditional approach of both the authorities and the opposition (including the intellectual front of various ideological connotations) to justify their actions and positions by referring to foreign experience.

Keywords: IT; big data; oligarchy; regulation

For citation: Mitrakhovich S.P. Regulation of the IT sphere as a politico-theoretical and practical problem. *Gumanitarnye Nauki. Vestnik Finansovogo Universiteta = Humanities and Social Sciences. Bulletin of the Financial University*. 2021;11(6):67-72. (In Russ.). DOI: 10.26794/2226-7867-2021-11-6-67-72

* Статья подготовлена по результатам исследований, выполненных за счет бюджетных средств по государственному заданию Финансовому университету.

** The article was prepared based on the results of studies carried out at the expense of budgetary funds on the state task of the Financial University.

Экономические процессы в сфере управления и организации хозяйственной деятельности развиваются в прямой взаимосвязи с процессами политическими, в фокусе которых (как принято считать в академической науке как минимум со времен известного теоретика Роберта Даля) [1] находится принятие стратегических решений, касающихся значительной части общества. Политика как сфера борьбы за принятие стратегических решений важна именно потому, что относительно экономической деятельности или ее отдельных сегментов могут сосуществовать очень различные точки зрения на происходящие и ожидаемые события. В каждой из хозяйственных сфер существуют разные взгляды на оптимальные стратегии развития, что обусловлено собственным видением образа будущего и различием в ценностных установках (субъективных оценках того, как именно — в лучшую или худшую сторону — будет изменена жизнь людей в рамках той или иной формы хозяйственного развития).

Элиминировать политическую составляющую в хозяйственном развитии можно разве что в условном трансгуманистическом будущем в сценарии исчезновения ценностных споров и конфликтов внутри человечества. Некоторые теоретики трансгуманизма предрекают наступление «морфологической свободы», когда индивид получает свободу не только поступать так, как хочется, но и быть абсолютно всем, кем хочется (с соответствующим снижением роли общественных ограничений и зависимости от общественных процессов). До этого же момента любая выработка стратегии для той ли иной отрасли (будь то нефтегаз, девелопмент или ИТ) будет нуждаться в политических (стратегических и ценностных) решениях. Пока же на горизонте не просматривается ситуация, при которой сугубо отраслевые эксперты могли бы решить вопросы вроде того, можно ли застраивать те или иные участки земли (ведь это влияет на общество в целом), разрабатывать месторождения в Арктике или легализовывать систему очень плотного контроля государства с помощью современных цифровых методов за любыми аспектами жизни граждан, включая личную жизнь.

Ответы на эти вопросы требуют именно политического решения, а если человек, являющийся отраслевым специалистом (строитель, нефтяник, компьютерный инженер и т.д.), займет государственную должность (президент, министр, депутат

и пр.), он станет политиком и будет продуцировать политические решения. При этом, несмотря на резко возросшую за период глобализации роль негосударственных акторов в принятии политически значимых решений даже на планетарном уровне (или во влиянии на принятие этих решений), все равно основное «регулирующее слово» остается за государствами.

Ключевой чертой олигархии в ее академическом понимании (в признанной традиции Ч.Р. Миллса, У. Домхоффа и др.) принято считать совмещение контроля над экономическими и политическими значимыми активами и позициями. Олигархические группы образуются при возможности установления прочных связей между владельцами и управленцами крупного бизнеса, с одной стороны, и политиками — с другой. Олигархия может пониматься и как очень тонкая социальная прослойка, как сообщество немногочисленных индивидов со своими клиентами и зависимыми группами интересов, формирующее специфические правила игры, минимизирующие конкуренцию.

На Западе формально ключевые ИТ-компании являются частными, их деятельность противопоставляется, например, технологическим компаниям из России и Китая, подконтрольным местным правительствам прямо, как «Ростех», или косвенно, как Huawei. Но эффект монополизации действительно сходен — хотя компании предоставляют свои коммерческие услуги, но их значимость столь велика, а количество альтернативных поставщиков столь мало (либо вообще отсутствует), что государство (в том числе на Западе) считает возможным даже официальным образом вмешиваться в дела бизнеса.

Поскольку соперничество между олигархическими кланами (включая государственную олигархию, когда влияние создается по восходящей линии не от денег к власти, а от власти к деньгам, что характерно для КНР, Турции, РФ) тоже существует, то эффект полной монополии не достигается — вместо нее вполне ожидаемо появляются олигополии. Последние используют свой потенциал для максимизации выгоды через практику, метко названную американским социологом Шошаной Зубофф «surveillance capitalism» (в русском академическом переводе — «капитализм слежки», «шпионский капитализм», «надзорный капитализм» и т.д.). Через сбор больших данных о пользователях (от которого фактически невозможно уклониться) компании в сфере Big Data оказываются способны эксплуатировать, причем до недавнего времени

практически бесконтрольно, огромный объем не просто личных данных, а данных о реальном поведении людей во всех аспектах жизни. В терминологии McKinsey Big Data — это набор данных, чей размер превышает возможности использования программных инструментов традиционных баз данных для их сбора, хранения, управления и анализа. По сути, в таком подходе расширенное понятие «большие данные» означает и собственно данные, и технологии по их анализу, и правила регулирования этих технологий. Предупредить чрезмерное коммерческое использование собранных больших данных часто призваны специальные ограничительные режимы, вводимые государствами или группами государств, как в случае с европейским General Data Protection Regulation (GDPR или EU-GDPR, «Общий регламент защиты персональных данных» [2].

Цифровые технологии и технологии цифровой коммуникации оказались «зажаты» между глобализацией и национализмом в современном мире. Более того, еще с «нулевых» годов развилась дискуссия о возможном обращении глобализации вспять и возрождении национальных государств как ключевых игроков и на мировой арене, и в сфере регулирования национальных экономик национальными же правительствами. Подъем стран Юго-Восточной Азии в конце XX и начале XXI в. практически стал подъемом именно национальных, во многом даже националистических государств, хотя и умудрявшихся получать выгоды от либерализованных глобализацией потоков капиталов, людей и технологий. В социально-психологическом смысле торговля и взаимные инвестиции парадоксальным образом сочетались с ростом националистических настроений. Националистические настроения в странах Юго-Восточной Азии даже сравнивают с ситуацией в Европе перед Первой мировой войной. По мере роста скептических настроений в отношении глобализации на Западе (Brexit, голосования за Д. Трампа, за евроскептиков и пр.) политический и экономический национализм в некоторых регионах мира, в том числе в Азии, только укрепился.

Среди всех ресурсов большие данные и прочие аспекты цифровизации экономики больше других оказались «зажаты» между глобализацией и возрождающимся национализмом. Компьютерная техника и способы ее применения в хозяйственной деятельности и в социальной жизни являются западными изобретениями (причем в основном

именно англосаксонской части западного мира). Использование западных цифровых изобретений, технологий и конечных цифровых продуктов, с одной стороны, поспособствовало экономическому росту незападных стран, с другой стороны, сделало эти страны очень зависимыми от Запада в области контроля над модернизацией, развитием и перестройкой ключевых цифровых платформ.

Ярким примером зависимости незападных стран от Запада в IT-сфере может служить медийное давление и санкции. Западные (особенно, опять же, англосаксонские) газеты, журналы, телеканалы и интернет-издания, работающие в том числе на глобальную аудиторию, получают преференции за счет дублирования и продвижения своих изданий в социальных сетях, контролируемых все теми же ключевыми западными IT-компаниями вроде Facebook, Twitter, Google (Youtube) и пр. Возникает эффект синергии, который очень сложно преодолеть конкурентам: мейнстримные медиа (MSM) поддерживаются мейнстримными же социальными сетями, в то время как альтернативные медиа, например китайские или российские, «заглушаются», частота их представления аудитории в выборке поисковых систем снижается. О «теневом заглушении» (shadow silencing, shadow ban) активно говорили скептики в отношении западных цифровых платформ, испытывая его на себе.

Так, о подобной намеренной практике в отношении своих личных аккаунтов и медиа-структур, где они работали, заявляли известные российские журналисты Маргарита Симоньян (RT) и Владимир Соловьев (ВГТРК). В конце марта 2021 г. YouTube заблокировал канал RT Arabic под предлогом жалобы на нарушение авторских прав. При этом нет сомнений, что подобные или сходные предлоги легко могут быть использованы и далее. Серьезных механизмов давления на западные цифровые площадки, даже не имеющие зачастую офисов в той же России, просто нет (кроме разве что полной блокировки, которая является «палкой о двух концах»).

Не существует и арбитража в спорах страны и западных социальных сетей, способных исполнять любые предлоги в любых интерпретациях для сдерживания политически нежелательного контента без прямых последствий для себя. Так, в мае 2020 г. алгоритмы Facebook реализовывали цензуру постов, содержащих репродукцию исторической картины водружения Знамени Победы над Рейхстагом. Ссылки на технические ошибки, допущенные сетью, выглядели крайне натянуты-

ми с учетом политического контекста момента: на Западе распространено крайне критическое отношение к российской практике использования памяти о победе в Великой Отечественной войне как механизма легитимации существующего политического режима и сталинского СССР.

Поэтому поверить в «случайную ошибку» Facebook именно в столь важный с идеологической точки зрения для РФ день очень сложно. По мнению некоторых специалистов по цифровым социальным сетям, история с «заглушением» Знамени Победы стала важным мотивом в попытках российских властей заставить западные платформы активнее сотрудничать с ними или готовиться к блокировке. Существует также информация о намеренной ставке Facebook на приоритетное принятие на работу по модерированию русскоязычного сегмента сети выходцев с Украины, что приводит и к конфликтам с российским идеологическим мейнстримом, и к частой блокировке украинских медийных фигур, оппозиционных «Майдану».

Не только перманентный сбор и анализ больших данных (необходимый для выстраивания работы алгоритмов большой социальной сети уровня Facebook, Twitter или Youtube), но и анализ отклонений от декларируемых честных правил игры ложится на плечи ограниченного числа все тех же западных игроков. Так, расследования относительно российских хакеров, якобы приведших к власти Д. Трампа в 2016 г., велись западными компаниями, не желавшими проводить альтернативную экспертизу. Было объявлено, что в 2016 г. группировка связываемых с российскими властями хакеров Cozy Bear совместно с другой группировкой, Fancy Bear, обошла цифровую защиту Национального комитета Демократической партии, похитив ее данные. В 2019 г. те же хакеры якобы взломали серверы посольства одного из членов Евросоюза в США. Данные анализа этого события представляла IT-компания ESET, занимающаяся в том числе антивирусами. При этом экспертиза с другой стороны (условно, Kaspersky) не была востребована. В 2019 г. в США запретили софт Kaspersky Lab.

При этом часть злоупотреблений сбором и использованием больших массивов персональных данных, изначально приписываемых тем же российским хакерам, в итоге вынужденно признавалась проблемой западных цифровых площадок. Речь идет о громком скандале с IT-компанией Cambridge Analytica, которая воспользовалась не-

доработками в системе безопасности Facebook и смогла получить личные данные около 50 млн пользователей без их согласия [3]. Агрегированный Cambridge Analytica массив данных дал возможность компании создавать для каждого пользователя (и одновременно избирателя) его уникальный портрет и с учетом индивидуальных особенностей этого портрета предлагать конкретному избирателю сверхтаргетированную рекламу. Например, если человек — сторонник «прогрессивистских» взглядов, именно ему будет показана реклама с высказываниями представителей левого крыла Демократической партии с фокусом внимания на повестке продвижения интересов меньшинств и т.д. Действия политических рекламщиков оценили как заказанное республиканцами манипулирование мнением граждан с помощью политической рекламы. Хотя на деле, если это манипулирование и происходило, то на фоне еще более очевидного искажения правил конкуренции за счет практики игры почти всех мейнстримных западных медиа «в одни ворота» — против Д. Трампа и в пользу Демократической партии.

Укрепление китайского суверенитета в сфере цифровых платформ оказалось возможным в силу масштаба экономики, населения и технологических возможностей Китая. При этом в рамках условной новой холодной войны (конфронтации США и Китая) часть китайского опыта по блокировке западных сервисов (Facebook, Twitter, Youtube) с их заменой на китайские аналоги (свои социальные сети, платежные системы вроде Baidu, WeChat и пр.) вызывает интерес в России.

Пекин уже неоднократно показывал, что готов при необходимости идти на эскалацию конфликта. Например, после отзыва британским медиа-регулятором Ofcom лицензии на вещание в Соединенном королевстве у китайского государственного телеканала China Global Television Network's (CGTN) Китай оперативно запретил вещание в КНР британского канала BBC World News. Фрагментация интернета и экономический национализм с частичным разворотом глобализации вспять в информационно-коммуникативном и цифровом аспекте явно будет набирать ход.

Актуальные тренды эволюции глобальной политики предполагают, что практика взаимных запретов цифровых и коммуникационно-цифровых сервисов, цифровых технологических платформ и IT-решений продолжится. Китайские магазины приложений для мобильной электроники и электронные маркетплейсы (магазины Huawei, Xiaomi,

Vivo, Tencent, Alibaba, JD.com и др.) одновременно заблокировали и удалили все упоминания знаменитого шведского магазина одежды H&M. Xiaomi и Huawei также удалили приложения Nike и Adidas, — это была месть за попытки данных брендов в угоду политической повестке западных правительств осуждать Китай за якобы нарушения прав человека в Сяньцзян-уйгурском автономном районе КНР и отказ покупать хлопковое сырье из этого региона. С точки зрения же глобальной перспективы китайские блокировки западных ресурсов уже чередуются с аналогичными блокировками Запада, а также санкциями вроде лишения Huawei доступа к сервисам Google для операционной системы Android. Huawei из-за американских санкций был еще и лишен возможности заказывать выпуск процессоров у тайваньской компании TSMC, находящейся под давлением властей США и использующей американские технологии при изготовлении своей продукции.

Не отдавая Западу контроль над коммуникациями и персональными данными своего огромного населения, китайское правительство решает не только задачу внешнеполитического характера, но и собственно реализует выбранную схему развития политического режима и общества в целом. Китайское видение гражданского общества похоже на специфическую интерпретацию западной L-парадигмы (когда гражданское общество не противопоставляется власти, поскольку предполагается, что граждане не будут и не хотят осуществлять никакие инициативы вне государства — и тем более против государственной власти). Китайский опыт контроля переписки, финансовых транзакций и физического перемещения людей, вероятно, является самым продвинутым в мире. На базе этого контроля реализуется знаменитый проект социального рейтинга граждан КНР и государственно-общественные инициативы, которые на Западе считают имитацией гражданского общества. Для режимов, считающихся недемократическими (для той же КНР), цифровые технологии, по сути, стали еще и способом соответствующей «вертикальной» организации социума.

В западном восприятии китайский (а заодно российский, турецкий и т.п.) опыт является образцом «цифрового авторитаризма», причем, опасного, склонного к экспансии. Например, по оценкам исследователей из Финского института международных отношений, Китай и Россия не только продвигаются по пути цифрового авторитаризма, но и сотрудничают друг с другом в этом

вопросе [4] — указывается на вероятную перспективу дальнейшей фрагментации международного цифрового сообщества, правда, упускается из виду факт влияния на эту фрагментацию предшествовавшей и отчасти продолжающейся западной цифровой экспансии. Экспансия же приводит к тому, что первичным мотиватором для действий политического режима хоть в РФ, хоть в КНР в отношении IT-бизнеса все же является очевидная «реактивная защитная реакция», направленная на самосохранение и недопущение инспирированного извне свержения власти. Таким образом, ограничительные меры в отношении медиапространства в интернете в последние годы оказались довольно масштабными [5, 6].

Россия на фоне экспансии всего лишь нескольких мощных игроков тоже идет по пути концентрации IT-бизнеса, причем в окологосударственных структурах [7]. Отдельное место занимают цифровые платформы для избирательных процессов [8]. Экспансия «Ростеха» и «Сбера», особенно учитывая попытки последнего получить контроль над «Яндексом», являются тому доказательством. Во многих аспектах российский кейс будет (ре)комбинацией западного и китайского опыта.

Практика последних лет показывает, что перед государством возникает триединая задача: необходимо сохранить автономию от внешнего влияния через соответствующую систему ограничений для нерезидентов, развить собственные альтернативные платформы и найти баланс между рыночной автономией этих платформ и государственным регулированием (а также оказанием госуслуг через эти же платформы). Границы между рыночной составляющей бизнеса в сфере Big Data и непосредственным вмешательством в эти рыночные процессы государства обещают быть весьма условными и подвижными, тем более что западный политический мейнстрим вроде Демпартии США намерен еще сильнее влиять на цифровые платформы, подавая другим пример. Не исключено, что в России окончательно сформируется феномен условной «государственной IT-олигархии» и корпоративистской модели развития на новом уровне, при которой бизнес-успех возможен только при его интеграции с государственными задачами и программами развития. Возможности же саморегулирования отрасли будут ограничены, поскольку в российских условиях в данном сценарии все равно создаются риски все того же укрепления IT-олигархии, но при первенстве зарубежных компаний, особенно американских.

СПИСОК ИСТОЧНИКОВ/ REFERENCES

1. Dahl R. A. Decision-Making in a Democracy: The Supreme Court as a National Policy-Maker. *Journal of Public Law*. 1957;(6):279–295.
2. Соколова М. Первые успехи нового европейского общего регламента по защите персональных данных. *Современная Европа*. 2020;(2):56–66.
Sokolova M. The first successes of the new European general regulation on the protection of personal data. *Sovremennaya Yevropa = Modern Europe*. 2020;(2):56–66. (In Russ.).
3. Мухаметов Д. Р. Технологии big data в политических процессах: возможности и риски. *Гуманитарные науки. Вестник Финансового университета*. 2019;9(5):143–149. DOI: 10.26794/2226–7867–2019–9–6–143–149
Mukhametov D. R. Big data technologies in political processes: opportunities and risks. *Gumanitarnyye nauki. Vestnik Finansovogo universiteta = Humanities and Social Sciences. Bulletin of the Financial University*. 2019;9(5):143–149. (In Russ.). DOI: 10.26794/2226–7867–2019–9–6–143–149.
4. Sinkkonen E., Lassila J. Digital authoritarianism in China and Russia: Common goals and diverging standpoints in the era of great-power rivalry. URL: <https://www.fiaa.fi/en/publication/digital-authoritarianism-in-china-and-russia>.
5. Каминская Т. Л. Ответственность за медиаконтент и проблема цензурирования коммуникационного пространства России. *Гуманитарные науки. Вестник Финансового университета*. 2021;11(2):96–101. URL: <https://doi.org/10.26794/2226–7867–2021–11–2–96–101>.
Kaminskaya T. L. Responsibility for media content and the problem of censoring the communication space in Russia. *Gumanitarnyye nauki. Vestnik Finansovogo universiteta = Humanities and Social Sciences. Bulletin of the Financial University*. 2021;11(2):96–101. URL: <https://doi.org/10.26794/2226–7867–2021–11–2–96–101>. (In Russ.).
6. Shcherbovich A. A. Comparative analysis of the legislation in sphere of Internet governance in Central and Eastern Europe. *Pravo*. 2019;(327):325–338. URL: <https://doi.org/10.19195/0524–4544.327.21>.
7. Ефферен Я. Ю., Россотто К. М., Хохолов Ю. Е. Цифровые платформы в России: конкуренция между национальными и зарубежными многосторонними платформами стимулирует экономический рост и инновации. *Информационное общество*. 2020;(1–2):16–34.
Eferen Ya. Yu., Rossotto K. M., Khokholov Yu. E. Digital platforms in Russia: competition between national and foreign multilateral platforms stimulates economic growth and innovation. *Informatsionnoye obshchestvo = Information society*. 2020;(1–2):16–34. (In Russ.).
8. Ерохина О. В. Электронное голосование в России: технологический и политический аспекты. *Гуманитарные науки. Вестник Финансового университета*. 2021;11(3):55–61. URL: <https://doi.org/10.26794/2226–7867–2021–11–3–55–61>
Erokhina O. V. Electronic voting in Russia: technological and political aspects. *Gumanitarnyye nauki. Vestnik Finansovogo universiteta = Humanities and Social Sciences. Bulletin of the Financial University*. 2021;11(3):55–61. URL: <https://doi.org/10.26794/2226–7867–2021–11–3–55–61>. (In Russ.).

ИНФОРМАЦИЯ ОБ АВТОРЕ

Станислав Павлович Митрахович — старший преподаватель, старший научный сотрудник Департамента политологии и массовых коммуникаций, Финансовый университет, Москва, Россия
smitrahovich@fa.ru

ABOUT THE AUTHOR

Stanislav P. Mitrahovich — Senior Lecturer and Senior Researcher, Department of Political Sciences and Mass Communications, Financial University, Moscow, Russia
smitrahovich@fa.ru

Статья поступила 21.09.2021; принята к публикации 20.10.2021.

Автор прочитал и одобрил окончательный вариант рукописи.

The article was received on 21.09.2021; accepted for publication on 20.10.2021.

The author read and approved the final version of the manuscript.