Цифровой паноптикум. Как автократии используют технологическую инфраструктуру?[1]

Томин Л. В.[1], ***, Балаян А. А.**[2]

[1] Санкт-Петербургский государственный университет, Санкт-Петербург; Российская Федерация; e-mail: * leopolit@yandex.ru

[2] Национальный исследовательский университет «Высшая школа экономики», Санкт-Петербург, Российская Федерация

РЕФЕРАТ

Целью данной статьи является рассмотрение причин и последствий формирования в недемократических государствах цифровой инфраструктуры контроля и подавления общества. В качестве методов исследования были использованы сравнительное case-study в интерпретации А. Лейпхарта и кросс-темпоральное сравнение как анализ динамических изменений в конкретные промежутки времени. Нужно отметить, что сравнение здесь выступает и как особый взгляд на политический феномен (в данном случае использование цифровых технологий в автократиях). Рассмотрены теоретические основы появления современных автократий и причины увеличения государственного внимания к технологиям. На конкретных примерах рассматриваются использование цифровых технологий для контроля над обществом и укрепления политического режима автократий. Раскрываются как политические, так и социально-экономические аспекты функционирования современных авторитарных систем на примере КНР и Филиппин. В завершение текста рассматривается вероятность распространения подобных практик на Российскую Федерацию. На основании теоретического и практического анализа авторы приходят к следующим выводам: автократии используют цифровую технологическую инфраструктуру для формирования системы контроля над гражданами; технологическим лидером в формировании подобных систем контроля является Китайская Народная Республика, которая экспортирует другим автократиям элементы технологической инфраструктуры через связанные с государством корпорации; в Российской Федерации после целого ряда законодательных изменений в информационной сфере при поддержке КНР формируются элементы контроля над интернетом и подчиненной государству системы сбора больших данных.

Ключевые слова: автократия, цифровизация, интернет, права человека, система социального кредита

Digital Panopticon. How Do Autocracies Use Technological Infrastructure?

Leonid V. Tomin [a], ***, Aleksandr A. Balayan**[b]

[a] St. Petersburg State University, Saint Petersburg, Russian Federation; * leopolit@yandex.ru

[b] Higher School of Economics University, Saint Petersburg, Russian Federation

ABSTRACT

The purpose of this article is to examine the causes and consequences of the formation in a non-democratic state of the digital infrastructure of control and suppression of society. As a research method, a comparative case study was used in the interpretation of A. Lijphart and a cross-temporal comparison, as an analysis of dynamic changes in specific periods of time. It should be noted that the comparison here also serves as a special view at the political phenomenon (in this case, the use of digital technology in autocracies). The theoretical foundations of the emergence of modern autocracies and the reasons for increasing government attention to technology are considered. Specific examples consider the use of digital technologies to control society and strengthen the political regime of autocracies. Both political and socio-economic aspects of the functioning of modern authoritarian systems are revealed on the example of the China and the Philippines. At the end of the text is considered the probability of the spread of such practices in modern Russian Federation. Based on a theoretical and practical analysis, the authors come to the following conclusions: autocracies use digital technological infrastructure to form a system of control over citizens; the technological leader in the formation of such control systems is China, which exports elements of the technological infrastructure to other autocracies through state-owned corporations; In the Russian Federation, after a number of legislative changes in the information sphere, with the support of the China, elements of control over the internet and a system of big data collection subordinate to the state are being formed.

Keywords: autocracy, digitalization, Internet, human rights, social credit system

[1] Работа выполнена при поддержке гранта РНФ «Политическая онтология цифровизации: исследование институциональных оснований цифровых форматов государственной управляемости» № 19-18-00210.

Введение

Авторитарные страны трансформируются вместе с технологическим многообразием современного мира. Постепенно технологии начинают играть важную роль для общества и входить в противоречие с самими основами недемократических режимов. Одна из наиболее распространенных сегодня типов автократий — электоральный авторитаризм определяется как режим, не являющийся демократией, но не использующий репрессивные практики регулярно, поскольку: «Организуя периодически выборы, подобные режимы пытаются получить хотя бы подобие демократической легитимности, надеясь удовлетворить как внешних, так и внутренних акторов» [14, p. 39]. Соответственно, власть в современной автократии рано или поздно сталкивается с необходимостью влиять на цифровые сферы жизни общества, чтобы сохранить контроль над системой.

Б. Геддес отмечает, что важнейшей проблемой формирующихся автократий режимов выступает тот факт, что правящие элиты, принимающие политические решения, обладают слишком большим контролем над государственными ресурсами и СМИ, что приводит к формированию неравных условий для конкурентной борьбы за власть [9, p. 115]. Однако исследователь придавала низкое значение роли цифровых площадок в начале 2000-х, что вполне объяснимо. Между тем Г. Шэпрон видит множество рисков во внедрении новых технологий в существующую систему государственного управления. Ключевой проблемой здесь является нежелание представителей государства создавать более прозрачную и подотчетную структуру с эффективной системой управления. Таким образом, остановить рост и развитие новых технологий уже невозможно, поэтому власти, так или иначе, придется считаться с инновациями [7, p. 403].

После событий «арабской весны» 2011–2012 гг. многие недемократические режимы осознали довольно известную фразу эксперта в компьютерной индустрии Эстер Дайсон: «Великое достоинство интернета заключается в том, что он размывает власть. Он высасывает власть» [3, p. 70]. Эту фразу вполне можно экстраполировать на инновации в целом, поскольку именно они меняют общество, а следовательно, угрожают авторитарной власти. Соответственно, для власти становится жизненно необходимым поставить эти изменения под контроль.

Особенностью закрытых политических систем является и то, что инновации перестали быть только инструментом удержания власти. М. Броуэр отмечает, что автократии извлекают излишки из общества тремя разными путями: монополизацией рынка, оплатой труда людей ниже рыночной и посредством инноваций [6]. Можно констатировать, что такие режимы используют новые технологии для более эффективного управления, но эффективность эта понимается как формирование инструментов контроля, функционирующих в интересах государства.

Однако это не значит, что государство должно демократизироваться именно посредством технологических инноваций. Напротив, государство может консолидировать подобные изменения для реализации своих специфических задач, таких как точечные репрессии или подавление свобод. Здесь важно отметить, что устранение посредника с помощью цифровизации — это иллюзия, ведь посредниками вместо реальных людей и организаций становятся цифровые агенты. Многие авторы отмечают, что цифровые технологии изменяют посредников в различных сферах жизни, но не избавляют от них [1]. Таким образом, цифровой агент в виде интернет-портала становится новым посредником, который располагает большей информацией о каждом своем пользователе, чем посредники, существующие в реальном мире. Ситуация характерна и для значительного количества социальных сетей, новых медиа и прочих аналогичных площадок.

Поэтому вполне очевидно, что интернет не избавил общество от посредников, он, напротив, дал возможности для эволюции этого института, что делает интернет-агентов мощным инструментом манипуляции и анализа общества. Интернет-агентов в контексте государственного управления можно разделить на два типа: агрегаторы информации; кураторы контента. Агрегаторы информации — это сайты, которые собирают персональную информацию и составляют полный профиль человека по его действиям. К таким компаниям-посредникам можно причислить любой сайт с большим трафиком, ведь информация о посетителях может быть монетизирована. Роль этих интернет-агентов заключается в том, чтобы собрать и обработать информацию о человеке, вычленить из нее какие-то выводы для последующей передачи или продажи. Кураторы контента — это люди и программы, редактирующие выбор и содержание потребляемого нами контента. С их помощью власть может смещать фокус внимания общества с важных политических проблем на незначительные локальные политические победы. В автократиях же власть сама становится посредником в цифровой сфере, что приводит к тотализации контроля над обществом.

Автократии цифрового контроля

Интересную для анализа модель цифровизации в условиях недемократического политического режима демонстрирует Китай. Если говорить о новых технологиях, то можно отметить, что в Китае проводится строгий отбор специфических инноваций, которые имеют потенциал быть внедренными в государственные структуры. Сильное авторитарное правительство обладает всеми инструментами, чтобы лишить интернет главной возможности — быстро мобилизовать массы. Важнейшим из этих инструментов является «Золотой щит» — «Великий китайский файрвол» (The Great Firewall of China). Интернет — это не абстрактная сеть, она обладает конкретным физическим обличием, находящимся во власти государства или подчиненных власти ведомств. Пример радикальных действий китайского правительства имел место в 2009 г.: «Китайские власти, обеспокоившись… растущим недовольством населения Синьцзян-Уйгурского автономного округа, попросту отключили все интернет-коммуникации в этом регионе на десять месяцев. В менее угрожающей ситуации хватило бы и нескольких недель» [2, с. 37]. Имея полный доступ к интернет-каналам, китайское правительство полностью контролирует данную сферу. А учитывая то, что значительная доля китайского населения активно использует интернет [11], для правительства он становится ключевым инструментом социально-политического контроля.

Интересной представляется программа внедрения модели «умных городов», которая реализуется в КНР государством в сотрудничестве с крупнейшими IT-компаниями (Alibaba, Tencent). Власти планируют, что данная программа охватит около 500 городов, среди них почти все провинциальные центры и города уровня автономных префектур. Из уже реализованных примеров — Ханчжоу, город в котором находится штаб-квартира Alibaba, где уже существует система искусственного интеллекта, управляющая светофорами, отслеживающая аварии и пробки на дорогах. Магазины и общественный транспорт оснащаются терминалами мобильного платежного сервиса Alipay, которые также начали внедрение системы оплаты товаров и услуг по системе распознавания лиц.

«Умные города» в КНР являются частью созданной по инициативе государства системы социального кредита — индикатора, основанного на обработке больших данных, который учитывает поведение человека в различных сферах (оплата налогов, счетов ЖКХ и штрафов; погашение кредитов; характер покупок; активность в интернете и социальных сетях). Социальный кредит — совместный проект государства и частных компаний, прежде всего Alibaba. Он разработан по модели рейтинговой системы Alibaba — Sesame Credit, анализирующей потребительское поведение клиентов, а затем начисляющей им специальные баллы, дающие право на льготные условия по кредитам, онлайн-покупкам, аренде автомобилей и номеров в гостиницах [5, p. 12–17]. Для частных компаний это эффективный маркетинговый инструмент, для государства — элемент новой модели управления.

Власти КНР интегрируют в систему социального кредита огромную сеть государственных и частных камер наблюдения (примерно 176 млн единиц), оснащенных функцией распознавания лиц, объединенную и управляемую в том числе инфраструктурой и алгоритмами «умных городов». До недавнего времени система тестировалась в отдельных городах и награждала обладателей хорошего рейтинга льготами, аналогичными существующим в Sesame Credit. С середины 2018 г. к обладателям низкого рейтинга стали применяться санкции: отказ в приеме на работу в системе государственной службы и отдельные должности в частном секторе, внесение в черный список с запретом покупки авиабилетов, бронирования гостиниц, обучения детей в частных школах. Механизм начисления личного рейтинга не раскрывается, но, учитывая, что он формируется и на основе мониторинга социальных сетей, складывается система, когда на рейтинг гражданина влияют его друзья в социальных сетях и их поведение [Там же, p. 32–55].

В КНР, где неолиберальная экономика сочетается с политическим режимом технократической автократии, процесс цифровизации и проекты «умных городов» формируют новую модель управления, своеобразную авторитарную версию теории подталкивания (nudge theory) [3]. В ее рамках производится тип субъективности, частично интернализирующий функции политического и социального контроля, которые раньше осуществлял аппарат государства. Эта авторитарная версия теории подталкивания, учитывая вовлеченность китайских частных компаний, в работу системы социального кредита действует не только как машина политического контроля, но и как маркетинговая.

Несмотря на конфликты с властями и нарушения прав человека, иностранные IT-компании хотят работать на китайском рынке. Возникает вопрос: можно ли рассчитывать на существующие

механизмы контроля за их поведением, для того чтобы предотвратить или приостановить сомнительные бизнес-практики, затрагивающие вопросы свободы и прав человека? В 2011 г. Совет ООН по правам человека единогласно одобрил документ «Руководящие принципы предпринимательской деятельности в аспекте прав человека» (The Guiding Principles on Business and Human Rights), призывающий бизнес-структуры, особенно транснациональные корпорации, ставить права и свободы граждан выше потенциальной прибыли [10]. Помимо этого, большое распространение получила практика отчетов о корпоративной социальной ответственности, которые, по идее, должны были стать механизмом корпоративного саморегулирования и сделать деятельность ТНК более прозрачной. Насколько такие документы и механизмы саморегулирования работают на практике? Рассмотрим несколько примеров, связанных с крупнейшими IT-компаниями.

Первый пример связан с ведением бизнеса IT-компаниями в недемократических странах, где существует политическая цензура. Для того чтобы продолжать работать на рынке КНР, Google в 2006 г. согласилась цензурировать результаты поиска китайских пользователей. В 2010 г. после хакерской атаки, организованной, по мнению специалистов компании, властями страны, когда, помимо прочего, были взломаны аккаунты правозащитников на сервисе Gmail, руководство Google заявило об отказе от практики цензурирования в китайской версии своего поисковика. Власти КНР расценили это как нарушение закона и приняли решение о блокировке почти всех сервисов компании. Тем более что тогда уже шла реализация проекта «Золотой щит», более известного как «Великий китайский файрвол», системы фильтрации интернета, способной блокировать доступ к официально запрещенным иностранным сайтам и цензурировать интернет-поиск по ключевым словам. Возможности данной системы были продемонстрированы в период после волнений в Синьцзян-Уйгурском автономном районе, когда власти одновременно заблокировали доступ к Youtube, Facebook и Twitter.

С тех пор Google формально декларировал неприятие практик цензурирования, но с 2015 г. руководство компании приняло неофициальное решение о необходимости вернуться на китайский рынок. После этого специалисты Google в закрытом режиме ведут разработку специального приложения для операционных систем Android and iOS — Dragonfly. Данное приложение разрабатывается в соответствии с правилами цензуры, существующими в КНР, оно позволяет властям отслеживать поисковые запросы пользователей и блокировать страницы с запрещенным политическим контентом, например, по темам «права человека» или «студенческие протесты» [7]. Сведения о разработке приложения Dragonfly стали известны общественности после того, как часть сотрудников компании, обеспокоенная информацией о негласном изменении позиции руководства по вопросу отношения к интернет-цензуре в КНР, провела собственное расследование и передала собранные данные в СМИ. Разразился скандал, группа сотрудников в знак протеста уволилась из компании, более шестидесяти правозащитных организаций обратилась к Google с требованием о прекращении разработки приложения [Там же]. Несмотря на все это, руководство компании продолжает публично отрицать работу над Dragonfly.

Второй пример — сотрудничество IT-компании с режимом, известным массовым нарушением прав человека. В 2012 г. IBM заключила контракт с городскими властями филиппинского города Давао на создание Интеллектуального операционного центра (Intelligent Operations Center). В то время мэром Давао был нынешний президент Филиппин Родриго Дутерте, которого международные и местные правозащитные организации обвиняли в массовых нарушениях прав человека. Согласно их отчетам, Р. Дутерте на посту мэра, а затем главы государства в рамках т. н. «войны с наркоторговлей» использовал нелегальные вооруженные отряды («эскадроны смерти») для внесудебных расправ над подозреваемыми. В ходе данных незаконных операций были убиты и пропали без вести оппозиционные депутаты и активисты, журналисты, католические священники и рядовые граждане [15]. За последние три года в стране несколько раз вводилось военное положение, и в результате т. н. «войны с наркоторговлей» погибло, по разным оценкам, от 5 до 27 тыс. чел. Официальные власти и полиция Филиппин не противодействовали этим преступлениям, более того, в ряде случаев они сами в них участвовали [13].

Невзирая на данные факты, IBM сотрудничала с властями в создании Интеллектуального операционного центра, основная цель которого — интеграция и управление для нужд полиции системы камер наблюдения, оборудованных технологией распознавания лиц. Учитывая вовлеченность полиции в нарушения прав человека, правозащитники и политические активисты опасаются, что данные, собранные и обработанные центром, могут передаваться «эскадронам смерти» для внесудебных расправ с подозреваемыми в преступлениях и убийств противников режима. IBM в своих официальных заявлениях, посвященных теме соблюдения прав человека, прямо ссылается на

упоминаемые выше разработанные ООН «Руководящие принципы предпринимательской деятельности в аспекте прав человека» [12]. Практика показывает, что в реальности отдает приоритет не правам человека, а своим бизнес-интересам. С точки зрения оценки эффективности механизмов саморегулирования важен тот факт, что ни в одном отчете о корпоративной социальной ответственности IBM факт сотрудничества с властями Давао не упоминается [Там же].

Власти Филиппин планируют в ближайшие несколько лет начать реализацию программы «Безопасные Филиппины», которая заключается в расширении до национального уровня практик, внедренных в Давао. Обеспечивать технологиями и координировать реализацию будет китайская компания Huawei. Сама программа «Безопасные Филиппины» будет частично копировать опыт системы социального кредита, аккумулируя данные из разных источников в единую базу [Там же]. Оппозиционные политики и журналисты опасаются, что новые технологические инструменты превратят страну в цифровую диктатуру.

В Российской Федерации после ряда событий властями также создаются элементы инфраструктуры для контроля интернета со стороны государства: запуск единой биометрической системы (ЕБС) для банков; сбор персональной информации граждан; введение единых карт для жителей крупных городов; приход на российский рынок китайской платежной системы Alipay. В начале 2019 г. стало известно об участии китайской компании Huawei в технологическом обеспечении «пакета Яровой — Озерова», и, скорее всего, этим дело не ограничится, Huawei могут подключить и к созданию аппаратной базы для реализации закона о «суверенном интернете». Все это говорит о возможной подготовке к созданию технологической инфраструктуры для отечественного аналога системы социального кредита, существующей в КНР. Она, скорее всего, не станет копией китайской системы и будет носить более децентрализованный характер.

Литература

1. *Ву Т.* Главный рубильник. Расцвет и гибель информационных империй от радио до интернета. Litres, 2017.
2. *Морозов Е.* Интернет как иллюзия. Обратная сторона сети. М. : АСТ: CORPUS. 2014.
3. *Паризер Э.* За стеной фильтров. Что интернет скрывает от вас. М. : Альпина Бизнес Букс. 2012.
4. *Талер Р., Санстейн К.* Nudge. Архитектура выбора. М. : Манн, Иванов и Фербер. 2018.
5. *Botsman R.* Who Can You Trust?: How Technology Brought Us Together and Why It Could Drive Us Apart. PublicAffairs. 2018.
6. *Brouwer M.* Governance and Innovation: a Historical View. Routledge, 2015.
7. *Chapron G.* The Environment Needs Cryptogovernance // Nature News. 2017. Т. 545. №. 7655. P. 403–405.
8. *Gallagher R.* Google Employees Uncover Ongoing Work on Censored China Search [Электронный ресурс] / The Intercept [сайт]. URL: https://theintercept.com/2019/03/04/google-ongoing-project-dragonfly/ (дата обращения: 09.04.2019).
9. *Geddes B.* What do We Know About Democratization After Twenty Years? // Annual Review of Political Science. Vol. 2. P. 115–44.
10. Guiding Principles on Business and Human Rights [Электронный ресурс] / The Office of the United Nations High Commissioner for Human Rights [сайт]. URL: https://www.ohchr.org/DOcuments/Publications/GuidingPrinciplesBusinessHR_EN.pdf (дата обращения: 22.03.2019).
11. Internet World Stats [Электронный ресурс]. Статистика о пользователях сети Интернет во всем мире. URL: https://www.internetworldstats.com/stats.htm (дата обращения: 10.05.2019).
12. *Joseph G.* Inside the Video Surveillance Program IBM Built for Philippine Strongman Rodrigo Duterte [Электронный ресурс] / The intercept [сайт]. URL: https://theintercept.com/2019/03/20/rodrigo-duterte-ibm-surveillance/ (дата обращения: 22.03.2019).
13. Philippines: Political and Human Rights Activists Killed with Impunity [Электронный ресурс] / Amnesty International [сайт]. URL: https://www.amnesty.org.au/philippines-political-human-rights-activists-killed-impunity/ (дата обращения: 26.03.2019).
14. *Schedler A.* The Menu of Manipulation // Journal of Democracy. 2002. Vol. 13. № 2. P. 36–50.
15. You Can Die Any Time. Death Squad Killings in Mindanao [Электронный ресурс] / Humans Right Watch [сайт]. URL: https://www.hrw.org/sites/default/files/reports/philippines0409webwcover_0.pdf (дата обращения: 26.03.2019).

Об авторах:

Томин Леонид Владимирович, доцент кафедры политического управления Санкт-Петербургского государственного университета (Санкт-Петербург, Российская Федерация), кандидат политических наук; leopolit@yandex.ru

Балаян Александр Александрович, доцент департамента прикладной политологии национального исследовательского университета «Высшая школа экономики» (Санкт-Петербург, Российская Федерация), кандидат политических наук; alexandr1138@mail.ru

About the authors:

Leonid V. Tomin, Associate Professor at the Department of Political Governance of St. Petersburg State University (Saint Petersburg, Russian Federation), PhD in Political Sciences; leopolit@yandex.ru

Aleksandr A. Balayan, Associate Professor at the Department of Political Science of Higher School of Economics University (Saint Petersburg, Russian Federation), PhD in Political Sciences; alexandr1138@mail.ru