ВОЛКОВ С. Ю., КОНДРАТЬЕВ А. С.

ФОРМИРОВАНИЕ ЦИФРОВОЙ ДИКТАТУРЫ КАК АКТУАЛЬНАЯ ОБЩЕСТВЕННО-ПОЛИТИЧЕСКАЯ ПРОБЛЕМА

Аннотация. В статье проведен анализ использования в различных странах информационных технологий, которые в недалекой перспективе способны привести к формированию так называемой «цифровой диктатуры», т.е. системы тотального контроля властей за гражданами. Проблема значительно актуализировалась в результате введения чрезвычайных мер по борьбе с пандемией COVID-19. С точки зрения общественно-политической практики, это содержит в себе угрозы потенциального фрагментирования существующих социальных институтов и деформации идентичности отдельных людей.

Ключевые слова: цифровая диктатура, информационные технологии, COVID-19.

VOLKOV S. YU., KONDRATIEV A. S.

FORMATION OF DIGITAL DICTATORSHIP AS A CURRENT SOCIO-POLITICAL PROBLEM

Abstract. The article analyzes the use of information technologies in various countries, which in the near future can lead to the formation of the so-called "digital dictatorship", i.e. systems of total control of the authorities over citizens. The problem has become significantly more urgent because of the introduction of emergency measures to combat the COVID-19 pandemic. From the point of view of socio-political practice, this contains the threat of potential fragmentation of existing social institutions and deformation of the identity of individuals.

Keywords: digital dictatorship, information technology, COVID-19.

Сложившуюся в мире в 2020-2022 гг. ситуацию часто описывают выражением «идеальный шторм», имея в виду сочетание множества негативных для всего человечества факторов. Глубокий экономический кризис, усугубляемый пандемией коронавируса, происходит на фоне глобальной политической нестабильности и многочисленных вооруженных конфликтов. Согласно известному принципу, «отчаянные времена требуют отчаянных мер», однако нужно учитывать, что жесткие решения, которые принимаются в настоящее время правительствами различных стран и наднациональными организациями с целью скорейшего преодоления текущих проблем, будут определять облик цивилизации не только на ближайшие годы, но и в долгосрочной перспективе. Несмотря на очевидную необходимость экстренных действий, следует уделять внимание и их неизбежным тревожным последствиям. Существует реальная опасность закрепления временных ограничительных мер в повседневной общественной и политической практике на постоянной основе.

Непроверенные и рискованные средства зачастую используются сейчас без особых раздумий, потому что бездействие в таких ситуациях намного хуже. Одной из ключевых потенциально опасных технологий являются системы цифрового контроля, которые получают все большее распространение во всем мире. Это сопровождается созданием огромных баз персональных данных граждан, а также методов распознавания лиц и других сопутствующих инноваций. Огромный объем информации о частной жизни людей ежедневно поступает в сетевые хранилища. Совокупность перечисленных факторов позволяет констатировать очевидную тенденцию к формированию полноценной «цифровой диктатуры».

Понятия «цифровое государство» и «цифровая демократия» не являются новыми в научном пространстве. Исследование этого феномена началось еще в конце 1990-х гг. с момента возникновения цифровой экономики. Долгое время их изучали нераздельно. Одними из первых, кто дал определение понятию «digital democracy», были Кеннет Л. Хакер и Ян ван Дейк, которые использовали этот термин для описания динамических отношений между государством и технологиями. Цифровая демократия включает «набор попыток практиковать демократию без ограничений во времени, пространстве и других физических условий, используя вместо этого информационно-коммуникационные технологи или компьютерную опосредованность в качестве дополнения, а не замены традиционных «аналоговых» политических практик» [12].

К преимуществам использования подобных инструментов в политическом процессе относят снижение затрат на управление, предоставление информации о гражданской активности и качестве политики. Эффективность использования ресурсов – наиболее распространенное обоснование перехода к цифровым технологиям в регулировании общественных отношений, это позволяет государству своевременно и без больших затрат донести информацию до максимального числа людей [11, с. 361]. Долгое время к феномену «цифрового государства» относились на Западе преимущественно положительно: там подобные системы активно применялись в США, Германии, Великобритании и Франции. Однако все изменилось, когда лидером стал Китай, который начал еще более масштабно использовать практики цифровизации. Его система контроля сетевого пространства «Золотой щит» работает уже почти 20 лет. В КНР запрещено посещать зарубежные сайты, а специальный отдел «Интернет-полиции» контролирует запросы граждан в сети: каждый запрос пользователя проверяется и в случае обнаружения неблагонадежной информации Интернет-соединение сбрасывается. Списки запрещенных ресурсов постоянно пополняется.

После запуска «Золотого Щита» и системы социального кредита в научном сообществе встала необходимость внедрения нового термина, который учитывал бы опыт Китая. В зарубежной литературе стали использовать, в основном, нейтральное «digital government».

В отечественном же научном пространстве стали разграничивать понятия «цифровая диктатура» и «цифровая демократия» как принципиально разные объекты исследования [1].

Существуют различные практики «цифровой диктатуры», но каждая из них неизменно включает в себя следующие компоненты:

- система цифрового контроля;
- единый реестр персональных данных;
- единое сетевое пространство;
- система социального рейтинга/кредита.

Система цифрового контроля включает в себя государственную информационную систему для сбора, обработки и хранения видеозаписей с камер, систему непрерывного видеонаблюдения за перемещениями, электронный анализ и контроль действий и поведения граждан. Также в рамках «цифровой диктатуры» необходим единый реестр персональных данных граждан, чтобы систематизировать основную информацию о каждом из них.

Следующим компонентом «цифровой диктатуры» является единое сетевое пространство, которое подразумевает систему фильтрации контента в соответствующем сегменте Интернета, а также включает в себя такие подсистемы, как управление безопасностью, информирование о правонарушениях, контроль выхода и ввода, информационная система мониторинга, управление трафиком. Она создается с целью ограничения иностранных сайтов, фильтрации веб-страниц по «ключевым словам», а также создания любому заблокированному ресурсу соответствующего аналога, который сделан с учетом местного потребительского менталитета.

Последним, но при этом немаловажным компонентом является система социального кредита (также встречаются названия «система социального рейтинга», «система социального доверия») – система оценки отдельных граждан и/или организаций по различным параметрам, значения которых получаются с помощью инструментов массового наблюдения и использующих технологию анализа больших данных [5].

Самым ярким на сегодняшний день примером формирования элементов «цифровой диктатуры» является Китай, где система социального кредита разрабатывается уже давно. В 2007 году были размещены «Некоторые замечания канцелярии Госсовета КНР о создании системы социального кредита», в соответствие с которой уже в 2010 году начался первый эксперимент с внедрением данной технологии в провинции Сычуань, уезд Суйнин. Суть его состояла в том, что первоначально каждый гражданин получал 1000 условных кредитных баллов, и за каждое социально положительное или отрицательное действие рейтинг соответственно увеличивался или убавлялся. «Баллы могли вычитаться за нарушение конкретных правовых, административных или моральных норм. Например, наказание за

вождение в нетрезвом виде оценивалось в 50 баллов, рождение второго ребенка – в 35 баллов, а невозврат кредитов – от 30 до 50 баллов. Потерянные очки могли быть восстановлены в течение 2-5 лет, в зависимости от вида проступка и серьезности нарушения. В итоге на основе полученных баллов граждане классифицировались по категориям от A до D» [7, с. 89]. Лицам, имеющим рейтинг D («тотальный аутсайдер»), стали отказывать в работе и социальных услугах. Примерные граждане с рейтингом A получили приоритет при трудоустройстве или при получении кредитов. Суйнин был лишь испытательной площадкой, и вслед за ним появилось более 40 городов (а к 2020 году в Китае действовали уже 352 «умных города» [3]), разрабатывающих собственные локальные системы социального кредита.

Пандемия коронавируса значительно ускорила внедрение подобного рода технологий по всему миру. В попытках справиться со стремительным распространением вируса по меньшей мере 24 страны [15] установили цифровое наблюдение за своими гражданами. Данные технологии включают в себя специализированное приложения COVID-19, данные о местоположении и электронные метки. Например, Центр по контролю и профилактике заболеваний в США отслеживает информацию о путешествиях отдельных лиц, используя данные авиапассажиров [14]. В Гонконге власти требуют ношения браслета и использования приложения для всех вновь прибывающих из-за границы. Технология GPS используется для отслеживания местоположения людей в Южной Корее, чтобы предотвратить нарушения карантина, посылая предупреждения пользователю и властям, если человек покидает назначенные места [13]. В Сингапуре люди должны были сообщать о своем местонахождении с фотографическими доказательствами. Таиланд использует приложение и SIM-карты для всех прибывших из-за границы, чтобы обеспечить соблюдение их карантина. Индия планирует производить браслеты для определения местоположения и контроля температуры граждан. В Европейском союзе одно из первых приложений для контроля над гражданами, обязанными соблюдать карантин, появилось в Польше.

Российская Федерация в этом вопросе не отстает от глобальных трендов. Еще в 2014 году стали обсуждаться меры по отключению Рунета от внешнего мира ради национальной безопасности [9]. Это дало толчок для разработки различных законов по охране персональных данных граждан. В ноябре 2019 года появился закон о «суверенном Интернете». С этого момента у всех операторов связи должны стоять устройства с функциями «противодействия внешним угрозам» и блокировки запрещенного контента из реестра Роскомнадзора, также был создан Центр мониторинга и управления сетями связи. Главные нововведения согласно данному закону: во-первых, Роскомнадзор реализует «централизованное управление» Рунетом, во-вторых, Роскомнадзор полномочен ограничивать доступ к запрещенным в России сайтам, в-третьих, создается национальная

система доменных имен и, в-четвертых, операторы связи должны заносить в регистр и применять исключительно эти точки обмена.

Другим законом, обращенным к операторам связи и Интернет-провайдерам, стал закон (или пакет) Яровой, состоящий из двух законов, которые были приняты в июле 2016 года. Они, в частности, обязуют операторов связи хранить звонки и сообщения абонентов за период, определяемый Правительством Российской Федерации (но не больше, чем за 6 месяцев), а информацию о фактах приема, передачи, доставки и обработки сообщений и звонков – 3 года [8]. Затем был подписан закон о создании единого федерального информационного регистра сведений о населении [2]. Идентификаторы: документ, удостоверяющий личность, регистрационный учет, воинский учет – всего более 25 параметров о каждом гражданине. Доступ к информационному регистру имеют органы государственной власти, органы местного самоуправления, внебюджетные фонды, многофункциональные центры, избирательные комиссии, нотариусы, физическое лицо, его законный представитель.

Таким образом, в Российской Федерации уже появился «суверенный Интернет» и единый регистр персональных данных, на базе которых можно создать систему социального рейтинга. Для борьбы с пандемией повсеместно в регионах были запущены приложения для граждан, которые должны соблюдать самоизоляцию. Были созданы платформы для выдачи цифровых пропусков для контроля режима самоизоляции. В Москве это приложение «Социальный мониторинг», в Республике Татарстан была введена система SMS-пропусков. Жителям Нижнего Новгорода необходимо было подтверждать выход на улицу через сервис «Карта жителя Нижегородской области» [10]. Эти сервисы имеют мобильные приложения, которые, при их установке, получают доступ к фото- и видеосъемке, к точному местоположению, к разрешению на совершение звонков, к данным о статусе телефона, к просмотру, изменению или удалению данных на накопителе, к запуску активных сервисов, к запуску приложения при включении смартфона, неограниченный доступ к сети и к получению данных, обеспечивают просмотр сетевых подключений и многое другое [4].

Безусловно, электронные системы государственного контроля за населением позволяют добиться высоких результатов при решении самых разнообразных общественно важных задач: от борьбы с распространением эпидемий и оперативного оповещения населения в чрезвычайных ситуациях до выявления разыскиваемых преступников, предотвращения террористических угроз, поиска пропавших или заблудившихся людей и т.п. Однако возможное дальнейшее продвижение по пути КНР влечет за собой также и специфичные проблемы.

Во-первых, это проблема надежного хранения и использование персональных данных граждан. Уже сейчас остро стоит этот вопрос с системой «Безопасный город» в Москве. Дело в том, что все записи с обычных камер, а также с камер, оборудованных системой

распознавания лиц, интегрированной с базами МВД, отправляются на хранение в «Единый центр обработки и хранения данных». Вход осуществляется по логину и паролю, никаких других способов защиты от взлома у этой системы нет. На форумах и чатах уже продают доступ к любой городской камере, архивы и прямые эфиры, также можно найти предложения о покупке неограниченного доступа к камерам [6].

Во-вторых, обостряется вопрос о роли и месте человека в новом цифровом мире. Представители классического гуманизма ставили человека в центр мира, считали жизнь человека наивысшей ценностью. Для них было характерно внимание к проблемам личностного развития и становления человека, к его взаимоотношениям в общественно-политической среде. В современном мире человек все чаще становится лишь единицей информации для государства и коммерческих компаний, он перестает быть уникальной, индивидуальной личностью и превращается в безликий пункт из реестра данных. Появление «цифровой диктатуры» также влияет и на социальные отношения, на отношения в семьях, а также на саму личность человека. Такие феномены как, например, система социального рейтинга заставляют людей соперничать друг с другом в погоне за наивысшей оценкой и последующими привилегиями. Доносы здесь хороший способ поднять свой рейтинг и понизить рейтинг «соперника».

Пандемия COVID-19 привела к чрезвычайному расширению полномочий властей по контролю за гражданами. Возможно, методы цифрового мониторинга в дальнейшем, после их анализа, будут признаны эффективными в борьбе с вирусом, но останутся ли они в повседневной общественно-политической практике – вопрос открытый.

СПИСОК ЛИТЕРАТУРЫ

1. Ведута Е. Н., Потеряйко А. Ю. Цифровая диктатура или цифровая демократия? // Актуальные вопросы экономики, управления и права: Сборник научных трудов (ежегодник). – 2020. – № 4. – С. 4–34.

2. Громова А., Калюков Е. Путин подписал закон о создании единого регистра сведений о населении // РБК [Электронный ресурс]. – Режим доступа: https://www.rbc.ru/rbcfreenews/5ede351c9a794710ce94854d (дата обращения 08.04.2022).

3. Данилин П. Н., Хилько И. Ю. История развития и перспективы внедрения системы социального кредита (рейтинга) в Китайской народной республике и Российской Федерации // Евразийский юридический журнал [Электронный ресурс]. – Режим доступа: https://eurasialaw.ru/nashi-rubriki/yuridicheskie-stati/istoriya-razvitiya-i-perspektivy-vnedreniya-sistemy-sotsialnogo-kredita-rejtinga-v-kitajskoj-narodnoj-respublike-i-rossijskoj-federatsii (дата обращения 29.03.2022).

4. Информационные технологии Городская система видеонаблюдения // Официальный сайт Мэра Москвы [Электронный ресурс]. – Режим доступа: https://video.dit.mos.ru (дата обращения 15.04.2022).
5. Кириллов А. Как работает система социального доверия в Китае // ИТАР-ТАСС [Электронный ресурс]. – Режим доступа: http:// https://tass.ru/opinions/5225841 (дата обращения 22.03.2022).
6. Королев Н. Говорит и показывает контракт // Коммерсантъ [Электронный ресурс]. – Режим доступа: https://www.kommersant.ru/doc/4465890 (дата обращения 10.04.2022).
7. Разумов Е. А. Цифровое диктаторство: особенности системы социального кредита в Китайской Народной Республике // Национальная безопасность. – 2020. – № 3. – С. 86–96.
8. Сенаторы одобрили антитеррористический пакет Яровой // Право.ru [Электронный ресурс]. – Режим доступа: https://pravo.ru/news/view/130772 (Дата обращения: 10.04.2022).
9. Совет безопасности обсудит отключение России от глобального интернета // Ведомости [Электронный ресурс]. – Режим доступа: https://www.vedomosti.ru/politics/articles/2014/09/19/suverennyj-internet (дата обращения 10.04.2022).
10. Цифровые пропуска – какие решения предлагаются в регионах // Национальная Ассоциация нефтегазового сервиса [Электронный ресурс]. – Режим доступа: https://nangs.org/news/it/tsifrovye-propuska-kakie-resheniya-predlagayutsya-v-regionah (дата обращения 12.04.2022).
11. Coleman S., Blumler J. G. The Wisdom of Which Crowd? // The Political Quarterly. – 2007. – No 82 (3). – P. 355–364.
12. Hacker K. L., Janvan D. What Is Digital Democracy? // Digital Democracy: Issues of Theory and Practice. – CA: SAGE Publications, 2000. – P. 1–9.
13. Phones Could Track the Spread of Covid-19. Is It a Good Idea? [Электронный ресурс] // Wired. – Режим доступа: https://www.wired.com/story/phones-track-spread-covid19-good-idea (дата обращения 01.04.2022).
14. Sloane M., Cahn A. F. Today's COVID-19 // The Daily Beast [Электронный ресурс]. – Режим доступа: https://www.thedailybeast.com/todays-covid-19-data-will-be-tomorrows-tools-of-oppression (дата обращения 01.04.2022).
15. Tracking the Global Response to COVID-19 // Privacy International [Электронный ресурс]. – Режим доступа: https://privacyinternational.org/examples/tracking-global-response-covid-19 (дата обращения 01.03.2022).