УДК 32 **DOI: 10.34670/AR.2020.49.76.011**

Цифровые технологии на службе человека и государства: поиск приоритетов

Баранов Николай Алексеевич

Доктор политических наук, профессор,
профессор кафедры международных отношений,
Северо-Западный институт управления,
Российская академия народного хозяйства и государственной службы при Президенте РФ,
199178, Российская Федерация, Санкт-Петербург, Средний пр., 57/43;
профессор кафедры политических институтов и прикладных политических исследований,
Санкт-Петербургский государственный университет,
191124, Российская Федерация, Санкт-Петербург, ул. Смольного, 1/3;
e-mail: nicbar@mail.ru

Аннотация

Современные технологии расширяют возможности для развития человека: повышается динамика жизни, создаются цифровые платформы в образовательных, научных, а также политических целях, возникают новые возможности для контроля за органами власти, совершенствуются коммуникативные практики. В то же время возникают новые опасности, которым подвержен человек. В докладе, подготовленном к началу работы Давосского экономического форума в 2019 г., акцентируется внимание на технологической неустойчивости и вводится понятие «Цифровой паноптикум», под которым понимаются новые формы социального контроля - распознавание лиц, анализ походки, микрочипирование, цифровое чтение по губам. Цифровые технологии обеспечивают невиданный прежде уровень контроля над обществами. В общественно-политической практике появился термин «цифровой тоталитаризм», под которым понимается тотальный цифровой контроль с помощью видеокамер, гаджетов, цифровых приложений, программ искусственного интеллекта за поведением и действиями человека для дальнейшего выстраивания его рейтинга в обществе. Опасность вторжения государства и общества в частную жизнь человека в условиях цифровизации не уменьшается, а напротив, возрастает. Всевластие органов безопасности и связанные с этим ограничения прав и свобод человека является проблемой не только авторитарных обществ, но и демократических государств. Выход видится в сочетании безопасного информационного пространства, создаваемого в решающей степени усилиями государства, и максимального использования возможностей цифровых технологий с пользой для человека посредством предоставления широких информационных прав.

Для цитирования в научных исследованиях

Баранов Н.А. Цифровые технологии на службе человека и государства: поиск приоритетов // Теории и проблемы политических исследований. 2020. Том 9. № 3А. С. 117-127. DOI: 10.34670/AR.2020.49.76.011

Ключевые слова

Информационное общество, цифровизация, цифровые права, цифровой паноптикум, цифровой тоталитаризм.

Введение

Мир настолько быстро изменяется, что человечество, зачастую, вынуждено просто запоздало рефлексировать на происходящие перемены, не вникая глубоко в суть происходящего. Технологические инновации, по мнению основателя и президента Всемирного экономического форума в Давосе Клауса Шваба, «находятся на грани активизации эпохального глобального изменения, и это совершенно неизбежно» [Шваб, 2019, 19]. Темпы развития инноваций оказываются беспрецедентно быстрыми, однако игнорировать высокую динамику изменений без негативных последствий невозможно. Как утверждает петербургский нейролингвист Татьяна Черниговская, «цифровая реальность уже признак отбора в социум. Если представить себе некую страну, которая не может себе позволить войти в цифровой мир, можно считать, что ее вообще нет» [В мире…, www]. Действительно, соответствие современным инновационным требованиям – это веление времени, а не просто модное увлечение технологиями.

Современные технологии востребованы как человеком, так и государством, которое, обладая широкими ресурсными возможностями, может навязать обществу свое понимание безопасности и административно ограничить свободу в интернете. Для человека новые технологии расширяют границы возможного, используемые в целях собственного развития и жизненного комфорта. Граждане используют технологии для контроля за властью и решения общественных проблем. Как справедливо отмечает А.А. Косоруков, «цифровые миры правительства и граждан все еще остаются обособленными друг от друга: государство может отставать от актуальных тенденций в сфере развития цифровых технологий, а общество может недооценивать вызовы и угрозы цифровому суверенитету государства» [Косоруков, 2019, 142-143].

Сближению человека и государства может способствовать четвертая промышленная революция, о которой пишет К. Шваб, обосновывая ее наступление тремя факторами: 1) темпами развития, которые характеризуются экспоненциальным ростом; 2) широтой и глубиной, основанной на цифровой революции и сочетающей разнообразные технологии, обусловливающие возникновение беспрецедентных изменений парадигм в экономике, бизнесе, социуме, в каждой отдельной личности; 3) системном воздействии, предусматривающем целостные внешние и внутренние преобразования всех систем по всем странам, компаниям, отраслям и обществу в целом [Шваб, 2019, 11].

Высокую актуальность приобретает адаптация новейших информационно-коммуникационных технологий к потребностям человека, общества, государства. Причем возможности инноваций могут быть использованы как в интересах индивида, так и в интересах государства, которые далеко не всегда идентичны. Если у человека технологические новшества расширяют возможности для развития, совершенствования, реализации своих планов в экономической, социальной или гуманитарной сферах, то для государства появляются новые возможности по контролю за обществом, за отдельными гражданами, несанкционированному доступу в приватную сферу. Поиск оптимальных взаимоотношений между государством и

гражданами в инновационной среде – важнейшая задача, стоящая перед социальными науками, в том числе перед политологией.

Плюсы и минусы современных технологий

Первой технологией, которая проникла в жизнь граждан быстрее, чем в государственные структуры, оказалась сеть Интернет. Общественная активность стала сопровождать различные технологические новшества, например, движение за открытые данные, возникшее в середине 2000-х гг., в рамках которого были выработаны принципы открытых данных, лежащих в основе модели цифрового управления: доступность, полнота, первичный характер, высокая оперативность, машиночитаемый формат, недискриминационный характер, незапатентованный формат, а также распространение данных на основе лицензии [Open…, www]. Такие движения стимулируют властные структуры к созданию атмосферы информационной открытости и прозрачности принимаемых решений, и способствуют демократизации политического процесса.

В 2014 году в Эстонии была запущена система электронного гражданства, которая поддерживает соединение между правительством и распределенным хранением данных на многочисленных серверах. На сайте «E-Estonia» констатируется, что в Эстонии создано «самое передовое цифровое общество в мире» [E-Estonia, www] с эффективной, безопасной и прозрачной экосистемой, помогающей гражданам и государству решать возникающие проблемы.

Роль граждан в производстве государственных услуг возрастает: они теперь рассматриваются не только как получатели, но и сопроизводители этих благ, что подразумевает более высокую ответственность в сфере производства и оказания государственных услуг. Резко возросло число мобильных приложений, позволяющих гражданам удовлетворять свои потребности в системе здравоохранения, образования, предоставления социальных услуг.

Составной частью цифрового управления и взаимодействия стала технология «больших данных», которые определяются как «наборы данных, размер которых превышает возможности стандартных программных средств по их сбору, хранению, управлению и анализу» [Big data…, 2011, www].

Технология «больших данных», ставшая возможной благодаря появлению новых технических и программных элементов распределенных систем обработки данных, широко используется правительственными органами, экспертными сообществами и мозговыми центрами, образовательными структурами, гражданским обществом, бизнесом. Однако они несут в себе опасность злоупотребления возможностями по контролю за гражданами, вмешательства в частную жизнь, использования персональных данных в преступных целях. История с частной английской компанией Cambridge Analytica, использовавшей технологию анализа «больших данных» для разработки стратегической коммуникации в интернете в ходе избирательной кампании в США и при проведении референдума о выходе Великобритании из Евросоюза, свидетельствует о широких возможностях влияния на избирателей и участников голосования.

В мире широко распространено недоверие к информации, причем не только частной, но и официальной, в том числе исходящей из независимых источников. Эпоха «постправды» и Fake News настолько дискредитировало информационное поле, что люди начинают верить лишь в

то, что подтверждает их позицию и не расходится с их точкой зрения. Подстраивание под мнение людей стало трендом в новостной повестке дня, даже касающейся нейтральных новостей. А люди, не научившиеся свободно ориентироваться в этом потоке информации, предпочитают либо ничему не верить, либо доверять своим смысловым приоритетам. «Мы должны сформировать способность жить в цифровом мире и не потерять человечность» [В мире…, www], - небезосновательно полагает Т. Черниговская.

Можно констатировать, что с одной стороны, «современные технологии, выстроенные в «цифре», позволяют быстро реагировать на повседневные проблемы жителей, отвечать на их инициативы, на их обращения, реагировать соответствующим образом, а значит, эффективнее и быстрее решать проблемы, с которыми люди сталкиваются в повседневной жизни» [Заседание…, 2020, www]. С другой стороны, возникает этический аспект использования больших данных. Государство и крупные корпорации получают доступ к персональным данным, делая это без явного согласия граждан или в обход законов. Более того, применяемые технологии анализа больших данных в сфере безопасности могут допускать ошибки, например, в процессе идентификации преступников или террористов, что приводит к дополнительным проверкам простых граждан или применению насилия к ним со стороны правоохранительных органов [Косоруков, 2019, 153].

Проблематика безопасности в контексте развития инновационных технологий

Секьюритизация проблематики безопасности предполагает повышенный интерес экспертного сообщества к вопросам ограничения прав и свобод человека, функционирования демократических институтов и практик. Цифровизация наряду с возможностями для расширения демократических процедур несет с собой опасность уязвимости программного и аппаратного обеспечения, повышение конфликтности в киберпространстве, ограничения в обеспечении защиты цифровых прав и цифрового суверенитета как государства, так и граждан. Доступ к сети Интернет на международном уровне признан одним из базовых прав человека и закреплен в международном праве, что явилось основанием для создания в некоторых странах движений в защиту «цифровых прав». Так, Генеральная Ассамблея ООН «признает глобальный и открытый характер Интернета и стремительное развитие информационно-коммуникационных технологий в качестве одной из движущих сил ускорения прогресса на пути развития в его различных формах» [Резолюция, 2013, www]. Вместе с тем, этим же документом подтверждается право на неприкосновенность личной жизни.

Угрозы, исходящие из киберпространства, затрагивают интересы бизнеса и каждого отдельного человека, использующего современные технологии. В России, как и во многих странах мира, новые технологии часто воспринимаются через призму порождаемых ими новых угроз и вызовов, а не создаваемых ими новых возможностей. Однако только от людей зависит, с какими целями будут применяться информационные технологии - во благо или во зло [Баранов, 2019, 31]. В условиях пандемии COVID-19 проблема безопасности актуализируется, на что обращает внимание заместитель председателя Совета Безопасности Российской Федерации Д.А. Медведев. В своей статье «Сотрудничество в сфере безопасности в период пандемии нового коронавируса» он пишет: «Цифра», несомненно, станет важнейшим фактором экономического, социального и политического развития в постпандемийном мире. Но

критически важно провести чёткое разграничение между благами, которые даёт цифровизация, и угрозой появления «цифрового Большого Брата», ограничения фундаментальных прав и свобод человека. Экономическая эффективность, которую несёт цифровизация, не может быть куплена ценой «цифрового тоталитаризма» [Медведев, 2020, www].

Опасности, на которые акцентируют внимание ученые, эксперты и политики, уже реализуются в нашей жизни. В общественно-политической практике появился термин «цифровой тоталитаризм», под которым понимается тотальный цифровой контроль с помощью видеокамер, гаджетов, цифровых приложений, программ искусственного интеллекта за поведением и действиями человека для дальнейшего выстраивания его рейтинга в обществе.

Генеральный секретарь ООН Антонио Гуттериш, выступая в начале 2020 года с обращением к Генеральной Ассамблее, выделил четыре угрозы, нависшие перед человечеством: геополитическая напряженность, климатический кризис, глобальное недоверие и «темная сторона цифрового мира», которая заключается в том, что, несмотря на огромные преимущества, новые технологии используются для совершения преступлений, разжигания ненависти, поддельной информации, угнетения и эксплуатации людей и вторжения в частную жизнь» [Guterres, 2020, www].

Выступая в Давосе на Всемирном экономическом форуме в январе 2020 г. израильский футуролог Юваль Ной Харари назвал три главные угрозы человечеству в XXI веке: ядерная война, экологический кризис и разрушительная сила технологий, особенно выделив последнюю проблему, как еще неизведанную. Технологии, по его мнению, несут массу рисков, среди которых он считает важнейшими появление большого количества «бесполезных» людей ввиду уничтожения многих специальностей; неравенство между странами, связанного с доступом к технологии искусственного интеллекта; цифровую диктатуру, осуществляющую контроль за гражданами; переход власти от людей к алгоритмам, вырабатываемым технологическими гигантами (Facebook, Google, Netflix, Amazon, Alibaba); уничтожение человечности, под которым подразумеваются технологии, разрушающие не только экономику, политику и жизненную философию, но и наше биологическое устройство [Футуролог, www]. Об этой же проблеме пишет Ф. Лукьянов - об утрате «контроля над информационными технологическими гигантами, которые способны вмешиваться в жизнь людей и диктовать им, как себя вести» [Свобода…, 2020, www].

В Докладе, подготовленном к началу работы Давосского экономического форума в 2019 г., акцентируется внимание на технологической неустойчивости (technological instabilities) и вводится понятие «Цифровой паноптикум» («Digital Panopticon»), под которым понимаются новые формы социального контроля: «Распознавание лиц, анализ походки, цифровые приложения, аффективные вычисления, микрочипирование, цифровое чтение по губам, датчики, считывающие отпечатки пальцев – благодаря распространению этих технологий, мы движемся в мир, в котором все данные о нас собраны, хранятся и подвергаются проверке через алгоритмы искусственного интеллекта» [The Global, 2019, www]. Искусственный интеллект (ИИ) уже рассматривается в качестве новой реальности электронного правосудия [Numa, www], что может привести в дальнейшем к цифровой диктатуре ИИ.

Отечественные политологи тоже анализируют проблемы, связанные с цифровизацией. Так, Д. Тренин пишет о новейшем инструменте, который освоили современные государства - «цифровые технологии, обеспечивающие невиданный прежде уровень контроля над обществами». По его мнению, «противоположение демократии и авторитаризма все больше

уходит на второй план, заменяется различиями в качестве и эффективности управления. Права граждан балансируются их обязанностями, выполнение которых обеспечивается системой всеохватного контроля. Наиболее успешные страны — те, где выше уровень общественной солидарности и взаимной ответственности правящих элит и обществ» [Тренин, 2020, www].

Наиболее известная практика цифрового тоталитаризма – это система социального кредита в Китае, которая была введена в действие Госсоветом КНР в 2014 г. Под «социальным кредитом» понимается «система оценки отдельных лиц или категорий граждан, а также юридических лиц и организаций по установленным государственным органом нормам и правилам, которые формируют определённые параметры, собираемые через инструменты массового наблюдения и технологии «больших данных» [Разумов, 2019, 88].

Проект полномасштабно заработал в 2014 году после публикации «Программы создания системы социального кредита (2014–2020)», согласно которой к 2020 г. все компании и каждый житель материкового Китая будут отслеживаться и оцениваться этой системой в режиме реального времени. Главная задача Программы: «оправдавшие доверие пользуются всеми благами, а утратившие доверие не смогут сделать ни шагу» [Уведомление…, 2014, www]. Китайская система социального кредита (SCS — Social Credit Score) — это социальная концепция, в основе которой лежит дифференциация граждан в отношении возможности получения социальных и экономических услуг в зависимости от индивидуального «рейтинга». Рейтинг определяется баллами, которые могут как начисляться, так и вычитаться в зависимости от поступков гражданина, его социального статуса, круга общения и различных других факторов. О китайской SCS в российской научной периодике имеется немало публикаций [Ларина, Овчинский, 2019, www; Авсеенко, 2019, www; Галиуллина…, 2018, 114-121], что свидетельствует об интересе со стороны научного сообщества новых цифровых практик, распространенных в мире.

Аналоги системы социального кредита применяются в разных вариантах и в других странах, например, в США или в ряде европейских государств – Великобритании, Германии, Франции. В США каждому резиденту присваивается индивидуальный номер социальной защиты (SSN - Social Security Number), с которым соотносятся как его личные данные, так и некоторые другие сведения, например, о платёжеспособности гражданина.

Специфика европейской системы сбора и обработки личной информации заключается в акцентировании внимания на формирование кредитного рейтинга гражданина или организации посредством его регуляции через связку экономического блока правительства с Европейским центральным банком. В некоторых странах, например в Германии, сбором и обработкой кредитной информации занимаются частные агентства.

Российская Федерация также находится в аналогичном цифровом тренде. Федеральным законом от 24 апреля 2020 года №123-ФЗ в городе Москве с 1 июля начинается эксперимент по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта [Федеральный закон…, 2020, www]. В соответствии с законом в Москве сроком на пять лет устанавливается экспериментальный правовой режим, целями которого являются: обеспечение повышения качества жизни населения, повышение эффективности государственного и муниципального управления, повышение эффективности деятельности хозяйствующих субъектов, а также формирование комплексной системы регулирования общественных отношений в ходе внедрения технологий искусственного интеллекта. Несмотря на то, что результатом

установления экспериментального правового режима не может быть ограничение конституционных прав и свобод граждан, введение для них дополнительных обязанностей, нарушение единства экономического пространства на территории Российской Федерации, о чем свидетельствует пятая статья закона, тем не менее для граждан вполне очевидно ужесточается правовой контроль. Поэтому будет ли польза для людей от экспериментального правового режима покажет будущее.

Заключение

Технологические переломные моменты в современном глобальном мире, называемые К. Швабом глубинными изменениями, оказывают противоречивое социальное воздействие, сопровождаемое как положительными, так и отрицательными эффектами. Среди негативных сторон кардинальных перемен отмечаются такие, как нарушение частной жизни, возможности наблюдения за человеком, обеспокоенность сохранностью личной информации, увеличение числа манипуляций, нарушение конфиденциальности и даже экзистенциональная угроза человечеству [Шваб, 2019, 141-190]. Больше половины глубинных изменений подвержены негативным эффектам, связанным с возможным вторжением в частную жизнь человека со стороны как государственных, так и корпоративных структур. Бюрократия всегда готова скорее запрещать, чем разрешать, однако пандемия продемонстрировала неожиданную тенденцию – согласие государственных структур на снятие некоторых регуляторных барьеров на пути цифровых технологий.

Тем не менее, контроль за обществом усиливается. Как утверждают специалисты, ни одно наше действие в интернете не остается незамеченным. Российский интернет-предприниматель, руководитель международной компании Reputation House Дмитрий Сидорин, размышляя о больших данных, пишет: «Растущее количество данных дает возможность прогнозировать развитие событий. На основе сведений из соцсетей строят модели эволюции потребительского спроса, поведения фондовых рынков, модели распространения эпидемий, прогнозы общественной активности по тому или иному поводу, включая митинги, и многое другое. Умение прогнозировать порождает желание менять ход событий и вмешиваться в интернет-пространство. Поэтому анализ данных интересен крупным мировым компаниям и государственным структурам» [Кризис…, 2020, www].

В политико-культурный контекст современных стран вплетаются потребности общества в создании безопасной цифровой среды, в которой заинтересованы и граждане, и государство. Возникает коллизия, связанная с поиском баланса полномочий государственных органов по обеспечению безопасности личности, общества и государства, с одной стороны, и недопустимостью их вторжения в частную сферу - с другой стороны. Данное противоречие актуально практически для всех современных государств независимо от политического режима и идеологических приоритетов. Выход видится в сочетании безопасного информационного пространства, создаваемого в решающей степени усилиями государства, и максимального использования возможностей цифровых технологий с пользой для человека посредством предоставления гражданам широких информационных прав.

Таким образом, у современного человека возникает дихотомия выбора между безопасностью и свободой, причем каждая из этих составляющих является одинаково важной для человека. Приоритет же будет определяться гражданами, исходя из их представлений о предполагаемом желаемом завтра, наложенном на политико-культурные особенности восприятия существующих проблем.

Библиография

1. Авсеенко И. Социальный кредит сформирует неравенство равных // Информационно-аналитическое агентство «Восток России». 10.04.2019. URL: https://www.eastrussia.ru/material/sotsialnyy-kredit-sformiruet-neravenstvo-ravnykh/ (дата обращения: 04.07.2020).
2. Баранов Н.А. Открытость vs безопасность: приоритеты для государства и гражданского общества в условиях цифровизации // Управленческое консультирование. 2019. № 10. С. 28-36.
3. «В мире рухнуло сразу всё». Татьяна Черниговская о цивилизации праздности и недоверии к информации // Центр стратегических оценок и прогнозов. 08.05.2020. URL: http://csef.ru/ru/nauka-i-obshchestvo/445/v-mire-ruhnulo-srazu-vsyo-tatyana-chernigovskaya-o-czivilizaczii-prazdnosti-i-nedoverii-k-informaczii-9165 (дата обращения: 04.07.2020).
4. Галиуллина С. Д., Бреслер М. Г., Сулейманов А. Р., Рабогошвили А. А., Байрамгулова Н. Н. Система социального кредитования в Китае как элемент цифрового будущего // Вестник УГНТУ. Наука, образование, экономика. Серия: Экономика. 2018. № 4 (26). С. 114-121.
5. Заседание Совета по развитию местного самоуправления. 30 января 2020 года. URL: http://www.kremlin.ru/events/president/news/62701 (дата обращения: 04.07.2020).
6. Косоруков А. А. Модель цифрового управления: открытые и большие данные // Политика и управление государством: Новые вызовы и векторы развития: Сборник статей / Под ред. А.И. Соловьева, Г.В. Пушкаревой. М.: Издательство «Аспект Пресс», 2019. С. 142-159.
7. Кризис сломал границы приватности. Дмитрий Сидорин — о том, как анализ больших данных из инструмента продаж стал инструментом большой политики. Июнь 2020. URL: http://plus-one.vedomosti.ru/blog/krizis-slomal-granicy-privatnosti (дата обращения: 01.07.2020).
8. Ларина Е., Овчинский В. Китайская система социального кредита: традиции и технологии // Завтра. 04.09.2019. URL: http://zavtra.ru/blogs/kitajskaya_sistema_sotcial_nogo_kredita_traditcii_i_tehnologii (дата обращения: 04.07.2020).
9. Медведев Д.А. Сотрудничество в сфере безопасности в период пандемии нового коронавируса // Россия в глобальной политике. 17.06.2020. URL: https://globalaffairs.ru/articles/bezopasnost-v-period-pandemii/ (дата обращения: 01.07.2020).
10. Разумов Е. А. Цифровое диктаторство: особенности системы социального кредита в Китайской Народной Республике // Труды ИИАЭ ДВО РАН. 2019. Т. 24. № 3. С. 86-97.
11. Резолюция Генеральной Ассамблеи ООН от 18 декабря 2013 г. № 68/167 «Право на неприкосновенность личной жизни в цифровой век». URL: https://undocs.org/pdf?symbol=ru/A/RES/68/167 (дата обращения: 04.07.2020).
12. Свобода — это рабство. Федор Лукьянов — об итогах всемирного экономического форума в Давосе // Коммерсантъ. 24.01.2020. URL: https://www.kommersant.ru/doc/4228069 (дата обращения: 04.07.2020).
13. Тренин Д. Вирус и миропорядок // Коммерсантъ. 2020. 29 марта. URL: https://www.kommersant.ru/doc/4307968?utm_referrer=https%3A%2F%2Fpulse.mail.ru&utm_source=pulse_mail_ru (дата обращения: 04.07.2020).
14. Уведомление Госсовета КНР о Программе создания системы социального кредита (2014—2020 гг.). URL: http://www.gov.cn/zhengce/content/2014-06/27/content_8913.htm (дата обращения: 04.07.2020).
15. Футуролог Харари назвал три главные угрозы человечеству в 21 веке // РБК. URL: https://www.rbc.ru/trends/futurology/5e2ef4499a79474925acdf08 (дата обращения: 04.07.2020).
16. Шваб К. Четвертая промышленная революция: пер. с англ. М.: Эксмо, 2019. 209 с.
17. Big data: The next frontier for innovation, competition and productivity. McKinsey Global Institute. May 1, 2011. Report. URL: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/big-data-the-next-frontier-for-innovation (дата обращения: 04.07.2020).
18. E-Estonia. URL: https://e-estonia.com (дата обращения: 04.07.2020).
19. Guterres Antonio. Remarks to the General Assembly on the Secretary-General's priorities for 2020. January 22, 2020. URL: https://www.un.org/sg/en/content/sg/speeches/2020-01-22/remarks-general-assembly-priorities-for-2020 (дата обращения: 04.07.2020).
20. Numa A. Artificial intelligence as the new reality of e-justice. URL: https://e-estonia.com/artificial-intelligence-as-the-new-reality-of-e-justice/ (дата обращения: 04.07.2020).
21. Open Government Data Principles. URL: https://public.resource.org/8_principles.html (дата обращения: 04.07.2020).
22. The Global Risks Report 2019. 14th Edition. Geneva: World Economic Forum, 2019. 107 p. URL: http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf (дата обращения: 04.07.2020).

Digital technologies at the service of man and the state: search for priorities

Nikolai A. Baranov

Doctor of political science, Professor,
Professor of the Department of international relations,
North-West Institute of management,
Russian Presidential Academy of National Economy and Public Administration,
199178, 57/43 Sredny av., Saint Petersburg, Russian Federation;
Professor of the Department of political institutions and applied political research,
Saint Petersburg State University,
191124, 1/3, Smolny str., Saint Petersburg, Russian Federation;
e-mail: nicbar@mail.ru

Abstract

Modern technologies expand opportunities for human development: the dynamics of life are increasing, digital platforms are being created for educational, scientific, and political purposes, new opportunities are emerging for monitoring government authorities, and communication practices are being improved. At the same time, there are new dangers that people are exposed to. The report, prepared for the start of the Davos economic forum in 2019, focuses on technological instability and introduces the concept of "Digital PANOPTICON", which refers to new forms of social control - facial recognition, gait analysis, microchipping, digital lip reading. Digital technologies provide an unprecedented level of control over societies. In socio-political practice, the term "digital totalitarianism" has appeared, which means total digital control by means of video cameras, gadgets, digital applications, and artificial intelligence programs over human behavior and actions to further build its rating in society. The danger of the state and society invading a person's private life in the context of digitalization does not decrease, but on the contrary, increases. The omnipotence of security agencies and related restrictions on human rights and freedoms is a problem not only for authoritarian societies, but also for democratic States. The way out is seen in the combination of a secure information space, created to a decisive extent by the efforts of the state, and the maximum use of the opportunities of digital technologies for the benefit of people through the provision of broad information rights.

For citation

Baranov N.A. (2020) Tsifrovye tekhnologii na sluzhbe cheloveka i gosudarstva: poisk prioritetov [Digital technologies at the service of man and the state: search for priorities]. *Teorii i problemy politicheskikh issledovanii* [Theories and Problems of Political Studies], 8 (3A), pp. 117-127. DOI: 10.34670/AR.2020.49.76.011

Keywords

Information society, digitalization, digital rights, digital PANOPTICON, digital totalitarianism.

References

1. Avseenko I. (2019) Social'nyj kredit sformiruet neravenstvo ravnyh [Social Credit Will Form Equal Inequality]. In: Informacionno-analiticheskoe agentstvo «Vostok Rossii» [Information and analytical agency "East of Russia"].

10.04.2019. URL: https://www.eastrussia.ru/material/sotsialnyy-kredit-sformiruet-neravenstvo-ravnykh/ (accessed: 04.07.2020).
2. Baranov N.A. (2019) Otkrytost' vs bezopasnost': prioritety dlja gosudarstva i grazhdanskogo obshhestva v uslovijah cifrovizacii [Openness vs Security: Priorities for the State and Civil Society in the Context of Digitalization] In.: Upravlencheskoe konsul'tirovanie [Management Consulting], №10, pp. 28-36.
3. Big data: The next frontier for innovation, competition and productivity. McKinsey Global Institute. May 1, 2011. Report. URL: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/big-data-the-next-frontier-for-innovation (accessed: 04.07.2020).
4. E-Estonia. URL: https://e-estonia.com (accessed: 04.07.2020).
5. Futurolog Harari nazval tri glavnye ugrozy chelovechestvu v 21 veke [Futurologist Harari named three main threats to humanity in the 21st century]. In.: RBK [RBC]. URL: https://www.rbc.ru/trends/futurology/5e2ef4499a79474925acdf08 (accessed: 04.07.2020).
6. Galiullina S. D., Bresler M. G., Sulejmanov A. R., Rabogoshvili A. A., Bajramgulova N. N. (2018) Sistema social'nogo kreditovanija v Kitae kak jelement cifrovogo budushhego [China's social credit system as part of a digital future]. In: Vestnik UGNTU. Nauka, obrazovanie, jekonomika. Serija: Jekonomika [Bulletin of USTU. Science, education, economics. Series: Economics], № 4 (26), pp. 114-121.
7. Guterres Antonio. Remarks to the General Assembly on the Secretary-General's priorities for 2020. January 22, 2020. URL: https://www.un.org/sg/en/content/sg/speeches/2020-01-22/remarks-general-assembly-priorities-for-2020 (accessed: 04.07.2020).
8. Kosorukov A. A. (2019) Model' cifrovogo upravlenija: otkrytye i bol'shie dannye [Digital Management Model: Open and Big Data]. In.: Politika i upravlenie gosudarstvom: Novye vyzovy i vektory razvitija: Sbornik statej / Pod red. A.I. Solov'eva, G.V. Pushkarevoj. [Politics and State Administration: New Challenges and Development Vectors: Collection of Articles]. Moscow: Izdatel'stvo «Aspekt Press», pp. 142-159.
9. Krizis slomal granicy privatnosti. Dmitrij Sidorin — o tom, kak analiz bol'shih dannyh iz instrumenta prodazh stal instrumentom bol'shoj politiki (2020) [The crisis has broken the boundaries of privacy. Dmitry Sidorin - about how big data analysis from a sales tool has become a big policy tool]. URL: http://plus-one.vedomosti.ru/blog/krizis-slomal-granicy-privatnosti (accessed: 01.07.2020).
10. Larina E., Ovchinskij V. (2019) Kitajskaja sistema social'nogo kredita: tradicii i tehnologii [The Chinese Social Credit System: Traditions and Technologies]. In.: Zavtra [Tomorrow]. URL: http://zavtra.ru/blogs/kitajskaya_sistema_sotcial_nogo_kredita_traditcii_i_tehnologii (accessed: 04.07.2020).
11. Medvedev D.A. (2020) Sotrudnichestvo v sfere bezopasnosti v period pandemii novogo koronavirusa [Security Collaboration during the New Coronavirus Pandemic]. In.: Rossija v global'noj politike [Russia in global politics]. URL: https://globalaffairs.ru/articles/bezopasnost-v-period-pandemii/ (accessed: 01.07.2020).
12. Numa A. Artificial intelligence as the new reality of e-justice. URL: https://e-estonia.com/artificial-intelligence-as-the-new-reality-of-e-justice/ (accessed: 04.07.2020).
13. Open Government Data Principles. URL: https://public.resource.org/8_principles.html (accessed: 04.07.2020).
14. Razumov E.A. (2019) Cifrovoe diktatorstvo: osobennosti sistemy social'nogo kredita v Kitajskoj Narodnoj Respublike [Digital dictatorship: features of the social credit system in the People's Republic of China] In.: Trudy IIAJe DVO RAN, T. 24, № 3, pp. 86-97.
15. Rezoljucija General'noj Assamblei OON ot 18 dekabrja 2013 g. № 68/167 «Pravo na neprikosnovennost' lichnoj zhizni v cifrovoj vek» (2013) [Resolution of the UN General Assembly of December 18, 2013 No. 68/167 “The right to privacy in the digital age”]. URL: https://undocs.org/pdf?symbol=ru/A/RES/68/167 (accessed: 04.07.2020).
16. Shvab K. (2019) Chetvertaja promyshlennaja revoljucija: per. s angl. [Schwab K. Fourth Industrial Revolution: Per. from English]. Moscow: Jeksmo, 209 p.
17. Svoboda — jeto rabstvo. Fedor Luk'janov — ob itogah vsemirnogo jekonomicheskogo foruma v Davose (2020) [Freedom is slavery. Fedor Lukyanov - on the results of the World Economic Forum in Davos]. In.: Kommersant [Kommersant]. URL: https://www.kommersant.ru/doc/4228069 (accessed: 04.07.2020).
18. The Global Risks Report 2019. 14th Edition. Geneva: World Economic Forum, 2019. 107 p. URL: http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf (accessed: 04.07.2020).
19. Trenin D. Virus i miroporjadok (2020) [Virus and world order]. In.: Kommersant [Kommersant]. URL: https://www.kommersant.ru/doc/4307968?utm_referrer=https%3A%2F%2Fpulse.mail.ru&utm_source=pulse_mail_ru (accessed: 04.07.2020).
20. Uvedomlenie Gossoveta KNR o Programme sozdanija sistemy social'nogo kredita (2014—2020 gg.) [Notification of the State Council of the PRC on the Program for creating a social credit system (2014–2020)]. URL: http://www.gov.cn/zhengce/content/2014-06/27/content_8913.htm (accessed: 04.07.2020).
21. «V mire ruhnulo srazu vsjo». (2020) Tat'jana Chernigovskaja o civilizacii prazdnosti i nedoverii k informacii ["Everything collapsed in the world at once." Tatyana Chernigovskaya on the civilization of idleness and distrust of information]. In.: Centr strategicheskih ocenok i prognozov [Center for Strategic Assessments and Forecasts]. URL: http://csef.ru/ru/nauka-i-obshchestvo/445/v-mire-ruhnulo-srazu-vsyo-tatyana-chernigovskaya-o-czivilizaczii-

prazdnosti-i-nedoverii-k-informaczii-9165 (accessed: 04.07.2020).
22. Zasedanie Soveta po razvitiju mestnogo samoupravlenija (2020) [Local Government Development Council meeting]. URL: http://www.kremlin.ru/events/president/news/62701 (accessed: 04.07.2020).