ИНСТИТУЦИОНАЛИЗАЦИЯ УПРАВЛЯЕМОСТИ И ПРОБЛЕМА КОНТРОЛЯ В ПРОСТРАНСТВЕ ЦИФРОВЫХ КОММУНИКАЦИЙ[1]

Л.В. Сморгунов

Сморгунов Леонид Владимирович, Санкт-Петербургский государственный университет, Университетская наб. 7/9, Санкт-Петербург, 199034, Россия.
E-mail: 1.smorgunov@spbu.ru.
ORCID 0000-0002-2581-2975

Аннотация. В статье ставится проблема публичной управляемости в условиях современных средств информации, порождающих возможность контроля сверху и снизу, по горизонтали. Современная цифровизация многих областей общественной жизни вызывает как положительные эффекты, так и угрозы. Развивая условия управляемости, она в то же самое время порождает угрозу чрезмерного контроля сверху и снизу. Раскрываются особенности контроля сверху и снизу. Контроль сверху порождает возможность управляемости как дисциплинируемости внешнего пространства жизнедеятельности человека. Управляемость в этом контексте предстает, с одной стороны, как способность больших организационных систем на основе обработки больших массивов данных о гражданах не просто их контролировать, а использовать в нужном для этих систем направлениях, т.е. управлять поведением больших масс людей. Контроль снизу возникает на основе потребности принадлежности к Сети и порождает форму управляемости в виде самоцензуры. Противостоит данным видам управляемости гражданское участие в публичном управлении, обеспеченное современными цифровыми технологиями. Цифровое публичное управление базируется на алгоритмах, обеспечивающих такие институциональные нормы взаимодействия, как анонимность, справедливость и взаимность. Управляемость на основе участия является результатом сетевой координации взаимодействия, создающей эффект сотрудничества, а не конкуренции. Анализируется как форма управляемости тенденция «суверенизации Интернета», которая выражается в современной регуляторной политике государств по созданию условий, обеспечивающих достаточные национальные гарантии контроля над интернет-пространством. Подчеркивается значение правовой институционализации современных форм управляемости, возникающих в условиях развития контроля сверху и снизу.

Ключевые слова: публичная управляемость, контроль сверху, контроль снизу, суверенный интернет, институционализация

Введение

Внедрение цифровых технологий в государственное управление и политику сопровождается дискуссиями о преимуществах, проблемах и рисках цифрового мира. Современное цифровое управление требует адаптивности, мобильности, гибкости, чувствительности и скорости реагирования на возникающие проблемы. Все это влияет на преобразования в сфере управленческих институтов и культуры. Оно включает в себя требования к данным, в том числе принципы сотрудничества, прозрачности и открытости, инноваций и совместного производства. В то же время цифровые технологии обострили проблемы контроля сверху (surveillance), вызвав обеспокоенность населения по поводу «Большого брата» (после Джорджа Оруэлла), «Паноптикума» (после Джереми Бентама и Мишеля Фуко) или Всевидящего ока (древний стереотип) (Chalmers, 2005; Borradori, 2016). Опасность для свободы и неприкосновенности частной жизни со стороны цифровых технологий связи вызвали ответный контроль снизу, или

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

по горизонтали («sousveillance») (Ganascia, 2010; Bakir et al., 2017), который сам по себе создает угрозу вертикальной интеграции и координации публичного пространства, но одновременно порождает социальный контроль и самоцензуру, ограничивая свободу и личное пространство. Дискуссии о свободе, доминировании и вмешательстве сопровождаются надеждой на бесконфликтную стратегию взаимодействия цифрового управления и отношений между гражданами, которая базируется на сотрудничестве, прозрачности и честности, которые основаны на алгоритмах цифровых технологий. Многие убеждены, что алгоритмическое управление устранит опасность неэффективности и недоверия, возложив часть ответственности на безличные процедуры.

Исторически трансформация государственной политики в эпоху цифровой революции в XXI в. уже сдерживается традициями, заложенными практикой внедренного электронного правительства, в которой значительное внимание уделяется услугам, информации и реагирующему поведению. Электронное правительство становится «узким» для развития цифровых технологий, предоставляя новые возможности для государственного управления и политики не только по форме, но и по содержанию и культуре. В то же время набирает обороты движение за «электронное правительство 3.0», которое ломает старые привычные формы взаимодействия между государством и обществом. Некоторые исследователи говорят, что, по-видимому, необходимо отказаться от прилагательного «электронный» при описании структуры и деятельности государственных органов и говорить либо просто о «правительстве 3.0», либо сосредоточиться на его новых механизмах и культуре взаимодействия с гражданами, используя термин «гражданское правительство». Этот переход связан с технологической и политической основой современных структур координации взаимодействия. В частности, следует отметить понятие «платформа», которое подчеркивает не только важность открытых и нейтральных средств коммуникации, но и публичную основу для формирования новой административно-институциональной конфигурации.

В процессе трансформации электронного правительства с порталов на платформы проявился политический характер возможного использования государства в качестве платформы. Узко технологический подход к платформам позволил только повысить эффективность предоставления услуг. В более широком толковании говорилось об изменении идеологии государственной политики, которое стало характеризоваться такими особенностями, как ориентация на включение граждан, сотрудничество основных заинтересованных сторон в разработке общественных решений, дискурсивная практика определения повестки дня, и так далее. И здесь сотрудничество может теперь привести к новой роли государства: государства, которое, скорее, обеспечивает и усиливает социальное создание стоимости своими гражданами. Он защищает инфраструктуру P2P-сотрудничества и создания общин и совместной административной культуры.

В этих условиях возникает вопрос о том, как трансформируется управляемость систем в условиях цифровизации общества и политики. Можем ли мы просто поговорить о его адаптации к меняющимся требованиям цифровизации? Или мы наблюдаем какую-то политику цифрового управления, которая радикально меняет принципы, методы, подходы и нормы управленческой деятельности? Какова эта политика цифрового управления и как цифровая культура формирует ее институциональную культуру? Какую роль играют процессы гражданского участия на основе сотрудничества, взаимности и взаимной ответственности в этом процессе формирования / адаптации управляемости?

Опасности управляемости как контроля сверху (surveillance) и контроля снизу (sousveillance)

Одной из центральных проблем релевантности политического дизайна внедрения цифрового публичного управления выступает соотношение в нем процессов и технологий контроля сверху (surveillance) и контроля снизу, по горизонтали и между (sousveillance) участниками взаимодействия. В этой связи основной задачей является исследование взаимодействия информационных компаний и государства в процессах формирования новой экономической и политико-административной логики управления. Подобные изменения могут привести к эрозии основ функционирования демократических политических режимов. Под угрозой оказывается пространство частной жизни и сама автономия индивида. Соединение материала «больших данных» с техниками поведенческой экономики, многими исследователями оценивается как новый эффективный инструмент коммерческого и политического манипулирования.

Управляемость в этом контексте предстает, с одной стороны, как способность больших организационных систем (государства, ТНК, монополистических частных платформ совместной экономики и торговли, новые социальные медиа) на основе обработки больших массивов данных о гражданах (их идентификациях, предпочтениях, коммуникациях) не просто их контролировать, а использовать в нужном для этих систем направлениях, т.е. управлять поведением больших масс людей. Основным методом управляемости при таком контроле выступает дисциплинирование пространства жизнедеятельности человека, а, следовательно, и самой жизни. Эту идею в концепции Паноптикума развивал Мишель Фуко.

Но и контроль снизу и по горизонтали (sousveillance), с другой стороны, позволяет усилить управляемость посредством самонаблюдения, социального контроля и самоцензуры. В этом отношении гражданская свобода попадает под контроль безличных сил цифровой общественности, умело ориентированных техно-социальных ассамбляжей, подчиняющихся логике господства и подчинения. Контроль снизу включает в себя не только выставление на всеобщее обозрения персональной информации о себе в социальных сетях, но и возможность предоставления такой информации, записанной современными средствами аудио- и видеонаблюдения. Как пишет Жан-Габриель Ганасия, «здесь понятие контроля снизу (sousveillance) стало включать лиц, которые делятся личными данными и анонимными записями, сгенерированными автоматическими устройствами, т.е. системами камер безопасности, видеоконтроля, системами закрытой трансляции телевидения и т.д. Соответственно, контроль снизу зависит не только от произвольных индивидуальных стремлений, но и от правил, согласно которым устройства автоматической записи публично доставляют информацию, которую они записывают (Ganascia, 2010, p. 493–494). Сутью управляемости здесь выступает программирование поведения человека посредством сетевой идентификации как принадлежности.

Исследователями отмечено, что в основе нового типа идентичности лежит способность быть видимым. Видимость (visibility)[2] характерна для контроля сверху,

[2] Видимость (visibility) следует отличать от появления (appearance). Хотя коннотативно эти термины похожи, однако видимость означает выставление образа, тогда как появление связано с позиционированием человека, а не его образа. Диалектика видимости связана с тем, что она есть одновременно выставление образа и сокрытие человека от контроля. Несчастье человека как раз и связано с его неспособностью стать публичным (политическим) в условиях современного господства средств контроля.

а также для контроля снизу. Если для первой формы контроля видимость распространяется на объект вне власти (власть невидима), и управляемость здесь становится формой организации деятельности посредством организации дисциплинарного пространства для контроля, то видимость во втором случае является общей задачей равных участников-образов. Не случайно в качестве основных признаков контроля снизу являются следующие особенности: полная прозрачность общества; фундаментальное равенство, которое дает всем возможность наблюдать — и, следовательно, контролировать — всех остальных; тотальное общение, которое позволяет каждому обмениваться со всеми остальными (Ganascia, 2010, p. 497). «Быть видимым» становится существенным фактором идентификации; присутствие в пространстве видимого выражает экзистенциальную потребность человека в век современной коммуникационной революции. Оба вида наблюдения «позволяют и способствуют формированию действенных идентичностей, поскольку их создание зависит от серии повторений и изложений в форме обмена контентом и повторной текстуализации информации каждый раз, когда кто-то делится ею, ставит лайки, комментирует или пишет в Твиттере. Игра на видимость / невидимость является фундаментальным аспектом онлайн существования, который ставит перед пользователем неудобную дилемму: быть увиденным и, следовательно, быть или не быть увиденным и, следовательно, не быть» (Xinaris, 2016, p. 67).

Условиями, определяющими потребность вертикального и горизонтального контроля, выступают безопасность и эффективность. Война с террором выступила первым способом оформления режима безопасности, который в условиях новой информационной революции стал опираться на технологический прорыв в области контроля над большими данными. Потребность возвратить доверие к государству посредством экономии публичных финансов и эффективности предоставления публичных услуг стала вторым фактором опоры на новые технологии. Не следует, однако, упускать из виду и то, что новые сетевые медиа шли в ногу с эффективностью услуг, так как они предоставляли более продуктивные способы общения, подтверждая возможность более экономного способа субъективации человека в виртуальном публичном пространстве без заботы о приватном.

Ясно, что эти виды контроля и управляемости проявляются во всех современных высокотехнологичных обществах независимо от демократических или авторитарных режимов. Демократические режимы не могут противостоять экспансии техно-социальных ассамбляжей контроля из-за потребностей безопасности и эффективности. Авторитарные режимы легитимизируют свои намерения господства той же технократической аргументацией безопасности и эффективности, обеспеченных новой промышленной революцией. Трансформация прежних разделений режимов на демократические и авторитарные сначала выражается в смешении их свойств (гибридные режимы), а чем дальше, тем больше приводит к новой их констелляции на основе степени возможного популизма и виртуальности. Прагматически это выражается в том, что, когда нужно, режим может быть любым; он не фиксирует своих свойств в стабильных институтах; он становится подвижным.

Гарантиями, позволяющими обеспечить нормальные условия управляемости для союза граждан в современном государстве, выступают ряд условий и механизмов, обеспеченных современным развитием. Радикальной формой борьбы с контролем сверху выступает сама цифровизация с ее условиями создания цифровых программ с использованием криптографических протоколов. Джулиан Ассанж, кто первый

позволил открыто противостоять мощным силам контроля сверху, писал, что «информацию легче зашифровать, чем расшифровать. Мы видели, что можем использовать это странное свойство для создания законов нового мира. Абстрагировать наше новое платоническое царство от его базовых основ спутников, подводных кабелей и их контроллеров. Чтобы укрепить наше пространство за криптографической завесой. Создавать новые земли запрещено для тех, кто контролирует физическую реальность, потому что для того, чтобы следовать за нами в них, потребовались бы бесконечные ресурсы. И таким образом объявить независимость» (Assange et al., 2012, p. 4). Важным средством противостояния контролю является его ограничение правом — совокупностью нормативных институтов, регулирующих физическое и социальное пространство использования контроля и правовой надзор над ним. Здесь же следует отметить и актуальную сегодня тему — формирование цифровых прав человека, обеспечивающих его свободу, приватность и деятельность. Нельзя не отметить и то, что в современных условиях открытость политического пространства сопровождается формированием системы возможностей для прямой демократии. Цифровизация позволяет восстановить прямые формы активности в условиях кризиса политической репрезентации.

Управляемость, цифровизация и гражданское участие

Эти новые проблемы и возможности определяются как трансформацией политических и административных институтов под влиянием противоречивой политики, так и появлением нового технологического ядра — электронного, а затем и цифрового управления. ИКТ первого, второго и третьего поколений определяли управляемость государства с функциональной (услуги электронного правительства), организационной (электронное участие) и коммуникативной (мониторинг демократии) позиций. Сетевая теория государственного управления сформировала радикальную концепцию «управления без правительства». В четвертом поколении ИКТ стала развиваться технология распределенных баз данных (регистров) — блокчейн, основанный на способности выполнять прямые транзакции между пользователями распределенных сетей на основе криптографических протоколов и алгоритмов, практически без доверия и в обход третьих сторон, включая состояние, был развит. С теоретической точки зрения анализ цифровых технологий в управлении их неоспоримыми преимуществами отмечает децентрализованное проектирование Сети, снижение эксплуатационных расходов, прозрачность операций и конфиденциальность, повышение скорости текущих процессов, надежность и безопасность, а также повышение «осведомленности» о решениях по отслеживанию на всех этапах, цикл офисной работы, что особенно важно для государственного сектора на современном этапе. В разных странах эти преобразования стали общими мотивами политических и административных реформ. В этом случае основным направлением политических и административных реформ является переход от электронного правительства, ориентированного на предоставление услуг и реализацию функций, к цифровому правительству, ориентированному на услуги, функции и управление посредством участия граждан. Организация экономического сотрудничества и развития (ОЭСР) в своих рекомендациях формирования цифрового правительства в 2014 г. поставила проблему гражданского участия на первое место, определив три основных задачи: (1) обеспечить большую прозрачность, открытость и инклюзивность правитель-

ственных процессов и операций; (2) поощрять вовлечение и участие публичных, частных и гражданских стейкхолдеров в разработке политики, дизайнов публичных услуг и их предоставления; (3) создать в публичном секторе культуру, ориентированную на информационные данные (Recommendation…, 2014, p. 6–7).

В этом отношении степень и качество участия граждан в сетях управления становится фактом, который необходимо изучать эмпирически, а не простым элементом, который соответствует этой парадигме партисипаторного управления (Parés et al., 2012). Концепция управляемости на основе участия не может быть отделена от понимания управляемости в целом. Управляемость — это способность системы реагировать на изменение внешнего контекста, сохраняя при этом ее природу и назначение. Управляемость на основе участия является результатом сетевой координации взаимодействия, создающей эффект сотрудничества, а не конкуренции. Ориентация на сотрудничество и совместное производство в государственной политике означает, что разработка политики строится с упором на граждан, а не на учреждения; возникает сотрудничество, а не просто внешнее партнерство; взаимодействие в процессе государственной политики основано на общих ценностях, а не только на заключении договоров; расширяются общественные арены для сотрудничества; основное внимание уделяется обсуждению общественных ценностей и реальных потребностей; управление осуществляется через суждения, а не нормы (Сморгунов, 2016); большое внимание уделяется реальному контексту жизни заинтересованных сторон государственной политики (потребностям и интересам, выбору места и времени); существует контекстуализация процесса государственной политики вместо его типизации; обеспечивается прозрачность управления и политики, формируются ориентированные на граждан данные, а цифровые ресурсы используются для государственной политики. Цифровизация играет важную роль в обеспечении управляемости на основе участия.

Цифровизация государственного управления — это процесс трансформации культуры, организации и взаимоотношений органов государственной власти с бизнесом и обществом посредством использования новых цифровых технологий (большие данные, Интернет, искусственный интеллект). Понимание процесса цифровизации как способа преобразования пространства государственного управления определяется не только ориентацией на большую чувствительность и подотчетность, но и ориентированной на граждан правительственной организацией. Она часто понимается как процесс использования новых ИКТ и, в частности, электронных технологий для организации и обеспечения эффективного функционирования публичной сферы. Кроме того, подчеркивается, что цифровизация в политическом смысле является способом расширения политических форм взаимодействия общества и государства, что делает государственное управление совместным (Asgarkhani, 2005). В то же время важно отметить, что участие граждан способствует развитию «подвижной демократии» в местных общинах — когда политические субъекты выбирают и голосуют по важным вопросам — и это указывает на то, что этот вопрос начинает фигурировать в политической повестке дня. Этот тип демократии позволяет не только принимать непосредственное участие в процессах принятия решений, но и создает условия, при которых представительство интересов приобретает характер «связанной репутации», обеспечиваемой участием в выработке политических решений.

Ценность цифровизации выходит далеко за рамки простого управления. Нормативная база, используемая цифровыми технологиями, позволяет решать ряд проблем, возникающих в связи с кризисом представительной демократии, подотчетности и контроля. Анализ технологии блокчейна показывает, что она создает условия для чистой процессуальной справедливости, обеспечивая возможность честного решения общественных вопросов (Scott et al., 2017). Этот пример демонстрирует огромные возможности оцифровки процессов управления для формирования его новой организации, которая выходит за рамки простого общественного выбора между левиафаном и анархией. Предыдущий выбор был основан на минимизации издержек взаимозависимости (внешние издержки и транзакционные издержки), тогда как государственное управление основывалось на способности системы обеспечивать безопасность и учитывать основные интересы. Цифровизация не уменьшает эти требования, но идет дальше, обеспечивая управляемость без посредников через сетевой технологический алгоритм с криптографическими протоколами, обеспечивающими анонимность и справедливость участия. Технология блокчейна универсальна настолько, что обеспечивает процессы международного общения государств в условиях децентрализации принятия решений современного плюрализма мировой политики (Салин, 2017) и необходимости защиты национальных больших данных. Действительно «криптография может защищать не только гражданские свободы и права отдельных лиц, но и суверенитет и независимость целых стран» (Assange et al., 2012, p. 60). Управляемость как сетевой эффект оцифровки государственного управления основана как на количестве участников взаимодействия, так и на интенсивности публичного общения. Она поддерживается процедурой справедливого консенсуса, основанного на взаимности, равенстве, безразличии и автономной организации децентрализованных решений.

Суверенный Интернет и цифровая управляемость

В последнее десятилетие управление Интернетом со стороны государства стало явным фактом глобальной организации коммуникационных потоков. Особенно этот процесс усилился после разоблачений последних лет о неправомерном использовании интернет-информации как специальными службами, так и коммерческими структурами. Потребность в регулировании интернет-пространства извне стала рассматриваться как важный способ сохранения национального суверенитета над информацией и коммуникацией. Притом, что данное пространство характеризовалось тенденцией глобализации, однако его организационно-технологическое обеспечение либо концентрировалось в руках некоторых государств, либо монополизировалось частными компаниями. С одной стороны, например, США сосредоточили у себя огромное количество гипермасштабируемых дата-центров, через которые осуществлялся интернет-трафик и хранилась информация как частная, так и публичная. По некоторым подсчетам их оказалось до 45% от общего количества в мире. И, например, Канада обеспокоилась прохождением от 25 до 60% своего интернет-трафика через США и возможностью использования соответствующих данных американскими спецслужбами (Clement, 2019). С другой стороны, «большая часть трафика в нём [Интернете] проходит по частным сетям мегакорпораций. Amazon, Microsoft, Facebook и Google развертывают свои сети доставки контента (CDN) такими темпами, что через 5 лет по ним будет проходить 70% всего трафика»

(Мрачное…, 2019). В этом государства увидели вызов для своей безопасности и суверенитета. К тому же назрела потребность регулирования совместной экономики и интернет-торговли. Все государства так или иначе стали как-то отвечать на это, пытаясь поднять уровень цифровой управляемости.

В данном случае под цифровой управляемостью мы понимаем способность государства влиять на контент, трафик и присутствие в сети Интернет различных сайтов с помощью регулирования сетевой техно-организации, контроля и допуска. С различной степенью интенсивности государство всегда регулировало интернет-пространство. Приведем пример такого регулирования в Соединенных Штатах. Хотя это описание не относится непосредственно к теме «суверенного Интернета», однако позволяет увидеть, что и в стране, выступившей против данной системы по понятным причинам, на деле регулирование Интернета является довольно разнообразным и тщательным, обеспечивающим национальный суверенитет над сетевыми потоками и их контентом.

В США существует ряд законов, обеспечивающих контроль над Интернетом. Назовем только наиболее значимые из них. В 1986 г. был принят Закон о компьютерном мошенничестве и злоупотреблениях в качестве поправки к существующему закону о компьютерном мошенничестве, который был частью Закона о всеобъемлющем контроле за преступностью 1984 г. Данный закон регулировал доступ к компьютерам. В 1996 г. в США был принят Закон о приличии в общении, который пытался регулировать как непристойность (если она доступна для детей), так и непристойность в киберпространстве. Не все нормы данного закона считаются конституционными по решению Верховного Суда, однако те, которые действуют, регулируют этот момент контента. Закон о защите авторских прав в цифровую эпоху 1998 г. предусматривает уголовную ответственность за производство и распространение технологий, которые могут быть использованы для нарушения авторских прав. Закон о защите конфиденциальности детей в Интернете вступил в силу в апреле 2000 г. Он применяется к онлайновому сбору персональных данных от детей в возрасте до 13 лет лицами или организациями, находящимися под юрисдикцией США. Он же регулирует ряд вопросов доступа в сеть, в том числе для школ и библиотек. Особое значение для контроля над Интернетом имеет Закон о патриотизме, подписанный президентом Дж. Бушем мл. в 2001 г. после событий 11 сентября. В частности этот закон позволял расширить рамки контроля информации, если они касались национальной безопасности, что позволяло Федеральному бюро расследований (ФБР) осуществлять поиск такой информации по телефону, электронной почте и финансовым документам без постановления суда; закон позволял также расширенный доступ правоохранительных органов к деловой документации, включая библиотечную и финансовую документацию. Эти и другие нормы закона подверглись большой критике и часть из них была признана неконституционными. Закон просуществовал до 2015 г. и был заменен в этом же году Законом о свободе, который восстановил ряд норм предыдущего закона и наложил некоторые ограничения на массовый сбор телекоммуникационных метаданных граждан США американскими спецслужбами, в том числе Агентством национальной безопасности. Он также восстановил разрешение на прослушивание телефонных разговоров и отслеживание террористов-одиночек. В США Управление по контролю за иностранными активами, которое было образовано в соответствии с Законом о торговле с врагом

1917 г., по этому и другим федеральным законам публикует списки лиц и организаций (как североамериканских, так и зарубежных), с которыми по различным причинам американским компаниям запрещено иметь дело. Публикация этого списка означает, что регистраторы доменных имен в США должны блокировать соответствующие веб-сайты. Закон об обмене информацией о кибербезопасности 2015 г. разрешает обмен информацией об интернет-трафике между правительством США и технологическими и производственными компаниями. Эти и другие законы позволяют правительству США эффективно обеспечивать цифровую управляемость Интернетом с учетом доминирующего положения данной страны в вопросе размещения техноорганизационных условий работы Глобальной сети на собственной территории. В 2015–2019 гг. здесь развернулась борьба вокруг так называемого «сетевого нейтралитета» (запрет для провайдеров использовать свое положение для регулирования контента и трафика путем монетизации), предполагающего регулирование действий компаний — поставщиков Интернета. Еще при президенте Б. Обаме был принят Порядок открытого Интернета, который устанавливал регулирующие правила для провайдеров по обеспечению «сетевого нейтралитета». При администрации Д. Трампа в 2017 г. этот порядок был отменен. В апреле 2019 г. Палата представителей большинством демократов приняла проект закона «Акт о сохранении Интернета», отменяющий прежний порядок. В настоящее время данный проект находится на рассмотрении в Сенате. Но он вряд ли пройдет через вторую палату Конгресса и будет подписан президентом.

США были той страной, которая в декабре 2012 г. в Дубае наряду с Великобританией, Канадой и Австралией не подписала итоговый документ Международного телекоммуникационного союза ООН. Прежде всего эти страны возражали против призывов ко всем государствам иметь равные права на управление Интернетом. С таким предложением вышли представители России, Китая, Саудовской Аравии, Алжира и Судана. Оно заключалось в том, чтобы правительства всех стран имели равные права управлять «ресурсами нумерации, именования, адресации и идентификации в Интернете» (US and UK refuse…, 2012). С этого исторического факта начинается фактическая история «суверенного Интернета», которая сегодня охватывает не только те страны, которые были инициаторами соответствующего предложения, но и другие развитые и развивающиеся страны. Конечно, вопрос о национальных условиях существования Интернета возникал и до 2012 г. (Shen, 2016), однако в качестве политической стратегии действий по созданию условий, обеспечивающих национальный контроль над Интернетом, вопрос обострился именно во втором десятилетии нынешнего века.

Термин «суверенитет Интернета» может означать в общем виде как достаточно высокий уровень самообеспеченности и технологической независимости страны в данной сфере. Этот термин чаще всего используется применительно к трем областям интернет-политики: экономический протекционизм (использование национального аппаратного и программного обеспечения и поддержка национальных ИТ-компаний в их экспансии на зарубежные рынки); безопасность национальной интернет-инфраструктуры, обеспечивающих национализацию интернет-трафика; национальная организация использования больших данных и их локализация на территории страны (Brokeš, 2018).

Наиболее последовательными сторонниками подобной суверенизации выступают Китай и Россия, где принята соответствующая политика и обеспечивающие

их законы. Однако и другие страны в условиях растущих вызовов (экономических, финансовых, безопасности, политических) все более склоняются к «суверенному Интернету». В апреле 2019 г. правительство Великобритании опубликовало «Белую книгу о вреде в онлайн пространстве», предусматривающую создание независимого регулятора для оценки онлайн контента сайтов (Online Harms White Paper, 2019). По некоторым экспертным подсчетам Интернет-трафик Канады на 25–60% проходит по территории США, что, по мнению некоторых, создает угрозу национальной безопасности страны, учитывая разоблачение Сноудена относительно контроля разведки США над зарубежными информационными потоками (Clement, 2019). В данной ситуации разрастания национального контроля над интернет-пространством Глобальные сети вынуждены учесть значимость государственного регулирования ряда вопросов и заявить о его поддержке. Так, Фейсбук прямо заявил о необходимости государственного регулирования, а Гугл проводит дифференцированную политику, учитывая эту тенденцию. Как пишет обозреватель ББС Селли Эди, «отдельный Интернет для одних, опосредованный Фейсбуком суверенитет для других: независимо от того, разграничены ли информационные границы отдельными странами, коалициями или глобальными интернет-платформами, ясно одно — открытый Интернет, о котором мечтали его первые создатели, уже исчез» (Adee, 2019). Фридомхаус (Freedomhouse) в своем исследовании свободы в Интернете за 2018 г. отмечает явную тенденцию усиления контрольных функций государства, назвав доклад «Свобода в сети 2018. Рост цифрового авторитаризма» (Freedom on the Net 2018. The Rise of Digital Authoritarianism). Данные оценочные суждения, как бы к ним не относиться, фиксируют озабоченность разрастанием контроля со стороны государства. Частью правомерная, частью выходящая за рамки разумности, данная политика является отражением потребности организации и порядка в пространстве глобальных сетей. Эта политика является в какой-то мере отражением общей политики государств в условиях современных вызовов безопасности и устойчивого развития.

Заключение

Процессы цифровизации публичного управления сопровождаются как положительными эффектами, так и рисками и вызовами. Политический эффект цифровизации и одновременно вызов связан с управляемостью современными системами. С одной стороны, цифровизация создает условия для более устойчивой управляемости на основе возможных трансформаций институциональной структуры публичного управления и перехода от иерархических, бюрократических структур к горизонтальным, сетевым отношениям, построенным на правилах сотрудничества и справедливости. С другой стороны, современные технические средства создают угрозу управляемости, когда она строится на основе дисциплинирования (контроль сверху и контроль снизу) как внешнего, так и внутреннего пространства жизнедеятельности современного человека. Внешний надзор и самоцензура создают условия для манипулирования, популизма и постправды. Сторонники цифровизации делают акцент на ее положительных сторонах, оппоненты подчеркивают возникающие риски и угрозы. По-видимому, начало четвертой промышленной революции пока не может оформиться в какие-то четкие положительные или отрицательные эффекты. Одновременно присутствует оптимизм и тревога. Потенциал гражданского участия и совместного публичного управления ограничивает

возможность неправомерного контроля и надзора. Стремление к суверенизации Интернета решает эту проблему применительно к международной системе, вместе с тем создавая угрозу открытости и прозрачности социальных коммуникаций. Многие видят выход в праве, в создании системы норм и регуляторов, которые не позволили бы нарушить границы свободы и приватности. Может быть оно и так; цифровые права личности и гарантии поставят предел контролю сверху и создадут условия для участия (Wagner et al., 2019). Однако способны ли современные техносоциальные системы, ассамбляжи вещей, технологий и людей приводиться в порядок правом? «Не было случая,— писал Бруно Латур,— чтобы установление правового государства облегчало жизнь тех, кто привык к простоте государства полицейского» (Латур, 2018, с. 245).

Библиографический список

Латур, Б. (2018). *Политики природы*. М.: Ад Маргинем Пресс.

Мрачное будущее интернета: неравенство и несвобода. (2017, 4 августа). *Хабр*. Режим доступа https://habr.com/ru/company/asus/blog/405783/

Салин, П. (2017). Иерархия равных. Как преодолеть кризис системы международных отношений. *Россия в глобальной политике*, 5, 129–140.

Сморгунов, Л. В. (2016). Знание и публичное управление: от утверждения нормы к суждению. *Политическая наука*, 2, 181–197.

Adee, S. (2019, 15 May). The Global Internet is Disintegrating. What Comes Next? *BBC: Future Now*. Retrieved from http://www.bbc.com/future/story/20190514-the-global-internet-is-disintegrating-what-comes-nex

Asgarkhani, M. (2005). Digital Government and Its Effectiveness in Public Management Reform. *Public Management Review*, 7(3), 465–487.

Assange, J., Appelbaum, J., Muller-Maguhn, A. & Zimmermann, J. (2012). *Cypherpunks: Freedom and the Future of the Internet*. N.Y., L.: OR Books.

Bakir, V. (2013). *Torture, Intelligence and Sousveillance in the War on Terror*. Ashgate: Farnham, Surrey.

Bakir, V., Feilzer, M. & McStay, A. (2017). Introduction to Special Theme Veillance and Transparency: A Critical Examination of Mutual Watching in thePost-Snowden, Big Data era. *Big Data & Society*, 4(1), 1–5. DOI: 10.1177/2053951717698996

Brokeš, F. (2018, 24 September). Russia's Sovereign Internet. *Central European Financial Observer*. Retrieved from https://financialobserver.eu/cse-and-cis/russias-sovereign-internet/

Borradori, G. (2016). Between Transparency and Surveillance: Politics of the Secret. *Philosophy and Social Criticism*, 42(4–5), 456–464. doi: 10.1177/0191453715623321

Chalmers, R. (2005). Orwell or All Well? The Rise of Surveillance Culture. *Alternative Law Journal*, 30(6), 258–261.

Clement, A. (2018, 26 March). *Canadian Network Sovereignty: A Strategy for Twenty-First-Century National Infrastructure Building*. Retrieved from https://www.cigionline.org/articles/canadian-network-sovereignty

Ganascia, J.-G. (2010). The Generalized Sousveillance Society. *Social Science Information*, 49(3), 489–507. DOI: 10.1177/0539018410371021

Online Harms White Paper. (2019, 8 April). Retrieved from https://www.gov.uk/government/consultations/online-harms-white-paper

Parés, M., Bonet-Martí, J. & Martí-Costa M. (2012). Does Participation Really Matter in Urban Regeneration Policies? Exploring Governance Networks in Catalonia (Spain). *Urban Affairs Review*, 48(2), 238–271. DOI:10.1177/1078087411423352

Recommendation of the Council on Digital Government Strategies. Adopted by the OECD Council on 15 July 2014. (2014). *OECD*. Retrieved from https://www.oecd.org/gov/digital-government/Recommendation-digital-government-strategies.pdf

Scott, B., Loonam, J. & Kumar, V. (2017). Exploring the Rise of Blockchain Technology: Towards Distributed Collaborative Organizations. *Strategic Change*, 26(5), 423–428. DOI: 10.1002/jsc.2142

Shen, Y. (2016). Cyber Sovereignty and the Governance of Global Cyberspace. *Chinese Political Science Review*, 1(1), 81–93. DOI: 10.1007/s41111-016-0002-6

US and UK Refuse to Sign UN's Communications Treaty. (2012, 10 December). BBC News. Retrieved from https://www.bbc.com/news/technology-20717774

Xinaris, Ch. (2016). The individual in an ICT world. *European Journal of Communication*, 31(1), 58–68. DOI: 10.1177/0267323115614487

Wagner, B., Kettemann, M. & Veith, K. (Eds.). (2019). *Research Handbook on Human Rights and Digital Technology. Global Politics, Law and International relations*. Cheltenham, UK; Northampton, MA, USA: Edward Elgar Publishing.

Статья поступила в редакцию 14.08.2019
Статья принята к публикации 30.08.2019

Для цитирования: Сморгунов Л.В. Институционализация управляемости и проблема контроля в пространстве цифровых коммуникаций.— *Южно-российский журнал социальных наук*. 2019. Т. 20. № 3. С. 62-75.

INSTITUTIONALIZATION OF GOVERNABILITY AND THE PROBLEM OF VEILLANCE IN THE SPACE OF DIGITAL COMMUNICATIONS

L.V. Smorgunov

Leonid V. Smorgunov, St. Petersburg State University, Universitetskaja nab., 7/9, St. Petersburg, 199034, Russia. E-mail: 1.smorgunov@spbu.ru.
ORCID 0000-0002-2581-2975

Acknowledgement. The research was carried out through the financial support of the Russian Science Foundation, grant No 19-18-00210 "Political ontology of digitalization: Study of institutional bases for digital forms of governability".

Abstract. The article raises the problem of public governability in modern media which entail surveillance and sousveillance. Digitalization in the sphere of public life entails both positive effects and threats. Improving conditions for governability, digitalization simultaneously generates the threat of surveillance and sousveillance. The paper dwells upon the specificity of both. Oversight can result in turning governability into the instrument of ordering people's life. In this context, governability is a data-intensive instrument that uses the data array processed by large operational systems about citizens. It allows not only to control them but also to use the data to govern and control the behavior of large masses of people. Sousveillance is the result of the need for network belonging and it generates self-censorship as a form of governability. Yet, the citizens' participation in public administration, backed by modern digital technologies, is opposed to surveillance and sousveillance. Digital public governance is based on algorithms that ensure such institutional norms of interaction as anonymity, justice and reciprocity. Participatory governability is the result of network-based coordination of interaction that creates the effect of collaboration rather than contest. The tendency of "Internet sovereignty" is analyzed as a form of governability, which is expressed in modern regulatory policies of states aimed at creating conditions to provide sufficient national guarantees of control over the Internet space. The paper emphasizes the importance of legal institutionalization of modern forms of governability arising in the context of the development of control from above and from below.

Keywords: public governability, surveillance, sousveillance, sovereign Internet, institutionalization.

DOI: 10.31429/26190567-20-3-62-75

References

Adee, S. (2019, 15 May). The Global Internet is Disintegrating. What Comes Next? *BBC: Future Now*. Retrieved from http://www.bbc.com/future/story/20190514-the-global-internet-is-disintegrating-what-comes-nex

Asgarkhani, M. (2005). Digital Government and Its Effectiveness in Public Management Reform. *Public Management Review*, 7(3), 465–487.

Assange, J., Appelbaum, J., Muller-Maguhn, A. & Zimmermann, J. (2012). *Cypherpunks: Freedom and the Future of the Internet*. N.Y., L.: OR Books.

Bakir, V. (2013). *Torture, Intelligence and Sousveillance in the War on Terror*. Ashgate: Farnham, Surrey.

Bakir, V., Feilzer, M. & McStay, A. (2017). Introduction to Special Theme Veillance and Transparency: A Critical Examination of Mutual Watching in thePost-Snowden, Big Data era. *Big Data & Society*, 4(1), 1–5. DOI: 10.1177/2053951717698996

Borradori, G. (2016). Between Transparency and Surveillance: Politics of the Secret. *Philosophy and Social Criticism*, 42(4–5), 456–464. doi: 10.1177/0191453715623321

Brokeš, F. (2018, 24 September). Russia's Sovereign Internet. *Central European Financial Observer*. Retrieved from https://financialobserver.eu/cse-and-cis/russias-sovereign-internet/

Chalmers, R. (2005). Orwell or All Well? The Rise of Surveillance Culture. *Alternative Law Journal*, 30(6), 258–261.

Clement, A. (2018, 26 March). *Canadian Network Sovereignty: A Strategy for Twenty-First-Century National Infrastructure Building*. Retrieved from https://www.cigionline.org/articles/canadian-network-sovereignty

Ganascia, J.-G. (2010). The Generalized Sousveillance Society. *Social Science Information*, 49(3), 489–507. DOI: 10.1177/0539018410371021

Latour, B. (2018). *Politiki pryrody* [Politics of Nature]. M.: Ad Marginem Press.

Mrachnoe budushchee interneta: neravenstvo i nesvoboda [The dark future of the Internet: inequality and the absence of freedom]. (2017, 4 August). *Habr* [Habr]. Retrieved from https://habr.com/ru/company/asus/blog/405783/

Online Harms White Paper. (2019, 8 April). Retrieved from https://www.gov.uk/government/consultations/online-harms-white-paper

Parés, M., Bonet-Martí, J. & Martí-Costa M. (2012). Does Participation Really Matter in Urban Regeneration Policies? Exploring Governance Networks in Catalonia (Spain). *Urban Affairs Review*, 48(2), 238–271. DOI:10.1177/1078087411423352

Recommendation of the Council on Digital Government Strategies. Adopted by the OECD Council on 15 July 2014. (2014). *OECD*. Retrieved from https://www.oecd.org/gov/digital-government/Recommendation-digital-government-strategies.pdf

Salin, P. (2017). Ierarkhiia ravnykh. Kak preodolet' krizis sistemy mezhdunarodnykh otnoshenii [The Hierarchy of Equals. How to Overcome the Crisis in the System of International Relations]. *Rossia v globalnoi politike* [Russia in Global Affairs], 5, 129–140.

Scott, B., Loonam, J. & Kumar, V. (2017). Exploring the Rise of Blockchain Technology: Towards Distributed Collaborative Organizations. *Strategic Change*, 26(5), 423–428. DOI: 10.1002/jsc.2142

Shen, Y. (2016). Cyber Sovereignty and the Governance of Global Cyberspace. *Chinese Political Science Review*, 1(1), 81–93. DOI: 10.1007/s41111-016-0002-6

Smorgunov, L.V. (2016). Znanie I publichnoe upravlenie: ot utverzdenia normy k suzdeniyu [Knowledge and Public Administration: From Ordered Rule to Judgment]. *Politicheskaya nauka* [Political Science], 2, 181–197.

US and UK Refuse to Sign UN's Communications Treaty. (2012, 10 December). *BBC News*. Retrieved from https://www.bbc.com/news/technology-20717774

Wagner, B., Kettemann, M. & Veith, K. (Eds.). (2019). *Research Handbook on Human Rights and Digital Technology. Global Politics, Law and International relations*. Cheltenham, UK; Northampton, MA, USA: Edward Elgar Publishing.

Xinaris, Ch. (2016). The Individual in an ICT World. *European Journal of Communication*, 31(1), 58–68. DOI: 10.1177/0267323115614487

Received 14.08.2019
Accepted 30.08.2019

For citation: Smorgunov L.V. Institutionalization of Governability and the Problem of Veillance in the Space of Digital Communications.— *South-Russian Journal of Social Sciences*. 2019. Vol. 20. No. 3. Pp. 62-75.