УДК 330:004.9

ЦИФРОВЫЕ ТЕХНОЛОГИИ УПРАВЛЕНИЯ И КОНТРОЛЯ – ВОЗМОЖНОСТИ И ВЫЗОВЫ

Соколов Л.А.

Московский городской университет управления Правительства Москвы имени Ю.М. Лужкова, Москва, e-mail: sokolovla@mos.ru

Пандемия COVID-19 оказала серьезное влияние как на предприятия и организации, так и на общество в целом. Противопандемические ограничения и массовый переход на удаленную работу значительно ускорили внедрение цифровых технологий взаимодействия, управления и контроля. Данные технологии, с одной стороны, предоставляют большие возможности, но, с другой стороны, создают и серьезные угрозы. Среди угроз – опасность злоупотреблений со стороны владельцев и операторов данных систем, а также со стороны киберпреступников. Реальностью может стать и тоталитарный контроль над сотрудниками, если речь идет об организациях, и над гражданами, если речь идет о государствах. Как на уровне корпораций, так и на государственном уровне уже внедряются системы автоматизированного контроля над людьми и предиктивной аналитики, используемой в целях «социального мониторинга». Ситуация осложняется отсутствием реальных возможностей общественного контроля использования цифровых технологий и собираемых ими данных, непрозрачность принятия решений. Решением мог бы стать «зеркальный» цифровой контроль над действиями руководства организаций или должностными лицами органов государственного управления со стороны граждан. Однако это потребует создания совершенно нового типа «общественного договора».

Ключевые слова: удаленная работа, цифровые технологии, ИКТ, тотальный контроль, цифровое рабство

DIGITAL TECHNOLOGIES IN MANAGEMENT AND CONTROL – OPPORTUNITIES AND CHALLENGES

Sokolov L.A.

Moscow Metropolitan Governance Yury Luzhkov University, Moscow, e-mail: sokolovla@mos.ru

The COVID-19 pandemic has had a major impact on both businesses and organizations and society as a whole. Anti-pandemic restrictions and the massive transition to telecommuting have significantly accelerated the introduction of digital technologies of interaction, management and control. These technologies, on the one hand, provide great opportunities, but, on the other hand, they also pose serious threats. Among the threats is the danger of abuse by the owners and operators of these systems, as well as by cybercriminals. Totalitarian control over employees, when it comes to organizations, and over citizens, when it comes to states, can also become a reality. Systems of automated control over people and predictive analytics used for the purposes of «social monitoring» are already being implemented both at the corporate level and at the state level. Systems of automated control over people and predictive analytics used for the purposes of «social monitoring» are already being implemented both at the corporate level and at the state level. The situation is complicated by the lack of real opportunities for public control over the use of digital technologies and the data they collect, and the lack of transparency in decision-making. The solution could be a «mirror» digital control over the actions of the management of organizations or officials of government bodies by citizens. However, this will require an entirely new type of «social contract».

Keywords: telecommuting, digital technologies, total control, surveillance capitalism

Эпидемии и пандемии случались на протяжении всей истории человечества. Но последняя пандемия коронавируса оказала, пожалуй, сильнейшее влияние не только на организации, но и на общество в целом. Интересно, что это влияние связано не столько с летальностью, сколько с теми изменениями, которые произошли в результате действий правительств и руководителей организаций, направленных на противодействие пандемии.

Пандемия и последовавшие в результате ограничения наглядно продемонстрировали, что режим удаленной работы как в случае его применения на регулярной основе в обычных условиях, а особенно при вынужденном его применении в условиях вводимых властями ограничений, требует соответствующих изменений в самых различных сферах – законодательной, организационно-управленческой, технической и т.д. В данной работе мы рассмотрим вопросы, связанные с использованием цифровых технологий управления, контроля и взаимодействия.

Целью данного исследования является осмысление тех реалий, которые возникли в сфере цифровых технологий управления как в рамках отдельных организаций, так и в рамках общества в целом, определение возникающих возможностей и вызовов, поиск наиболее эффективных решений.

Материалы и методы исследования

В процессе исследования были использованы как данные из открытых источников, так и материалы собственных исследований, применялись методы качественного и количественного анализа.

Результаты исследования и их обсуждение

В режиме удаленной работы с использованием информационно-коммуникационных технологий (ИКТ) особую актуальность приобретают вопросы защиты информации, в частности персональных данных. Примечателен тот факт, что в первое полугодие 2020 г., т.е. непосредственно в начале действия противопандемических ограничений и массового перехода на «удаленку», количество киберпреступлений в России выросло на 92 %, т.е. фактически удвоилось [1]. С одной стороны, ряд вопросов здесь лежит в технической плоскости. Но с другой – и в правовой тоже. Нельзя не отметить, например, тот факт, что в настоящее время получение согласия гражданина на обработку его персональных данных носит, по сути, принудительный характер. Персональные данные человека собираются на различных носителях, включая электронные. При этом возможность отказаться от предоставления персональных данных или ограничить их использование у гражданина фактически отсутствует. А вот необходимость сбора тех или иных персональных данных различными структурами и отдельными лицами вызывает большие вопросы. Конечно, когда речь идет, например, о персональных данных, которые работник предоставляет работодателю или клиент банка предоставляет банку, то необходимость этого сомнений не вызывает. Но возьмем, например, широко распространенную ситуацию с пропуском в разного рода офисные и общественные здания. Практически в каждом офисном центре, начиная от гигантов типа «Москва Сити» и заканчивая даже небольшими офисами, охранники или дежурные администраторы на входе фиксируют паспортные данные каждого посетителя. При этом сама целесообразность сбора этих данных вызывает большие сомнения. Можно понять, что предъявление документа, удостоверяющего личность, необходимо сотрудникам охраны или дежурным для того, чтобы удостовериться, что в качестве посетителя в некую организацию пришел именно тот человек, встреча с которым запланирована. Это логично. И это можно объяснить в том числе интересами обеспечения безопасности. Однако для этого достаточно простого предъявления документа, удостоверяющего, что «я это я». Но с какой целью фиксируются все данные паспорта гражданина, включая номер, серию, дату выдачи и остальную информацию, которая содержится в документе? И где гарантии, что эти данные не будут в дальнейшем использоваться в противоправных целях?

Даже не собирая, в формальном смысле этого слова, персональные данные, исключительно по «цифровому следу» в сети Интернет можно узнать о человеке очень много. Известный социолог Шошана Зубофф в этой связи еще в 2014 г. ввела в оборот термин «капитализм слежки» [2].

В контексте взаимоотношений работодателя и работника, а также государства и гражданина развитие современных технологий все острее ставит проблему тотального контроля. В современном языке уже прижились словосочетания «цифровое рабство» и даже «цифровой концлагерь». Под «цифровым рабством» понимается тотальный контроль над сотрудником, если речь идет об организации, или же за гражданином, если речь идет о государственных и других структурах, с помощью цифровых и инфокоммуникационных технологий. Типичные варианты такого контроля были продемонстрированы во время пандемических ограничений. Это, например, блокировка транспортных и социальных карт отдельным категориям людей. Но наиболее ярким примером здесь является приложение «Социальный мониторинг». Оно определяет местоположение мобильного телефона и периодически присылает запросы, требуя от человека сделать фото (или, как теперь часто говорят, «сэлфи»), чтобы убедиться, что человек находится рядом с телефоном [3]. Только за первый месяц работы это приложение выписало москвичам 54 тыс. штрафов [4]. Некоторые работодатели с началом пандемических ограничений также активно заинтересовались возможностями контролировать удаленную работу сотрудников. В настоящее время существует целый ряд различных приложений, способных фиксировать в буквальном смысле каждое движение сотрудника. И не просто фиксировать, но и выдавать соответствующую аналитику. Также существует определенный опыт использования предиктивной аналитики для определения вероятности того, что сотрудник теряет лояльность организации и в скором времени может ее покинуть.

Нет сомнений в том, что технологии, позволяющие собирать всевозможную информацию о человеке, накапливать ее и анализировать, будут развиваться и дальше. Возможности для тотального наблюдения и контроля над большинством людей, по крайней мере за теми, кто имеет смартфон и пользуется интернетом, существуют уже сейчас. Их массовое использование

государственными и бизнес-структурами – это лишь вопрос времени.

Серьезная угроза заключается в том, что ни отдельный человек, ни даже общество в целом, озаботься оно такой проблемой, не в состоянии это проконтролировать. Если раньше можно было (по крайней мере теоретически) проконтролировать, скажем, уничтожение бумажных документов, хранящихся в некоем архиве, то проконтролировать удаление данных с электронных носителей, гарантированно убедившись, что не осталось более ни одной электронной копии, практически невозможно. Аналогично человек не в состоянии как-либо проконтролировать и то, ведется ли за ним круглосуточная слежка с использованием «умных» устройств, таких как компьютеры, смартфоны или другая техника. Единственный возможный на данный момент способ избежать этого – полностью исключить из своей жизни использование таких устройств. Но в современном мире для огромного количества людей это означает не просто лишить себя определенного уровня комфорта, но также лишиться и возможностей работы, перемещения, доступа даже к самым необходимым благам цивилизации.

С 1 января 2021 г. новый гражданский кодекс официально узаконил систему социального кредита в Китае. [5] Технически в настоящее время вполне возможно реализовать подобные системы и в отдельно взятых организациях.

Как и любая другая технология, эта технология сама по себе не плоха и не хороша. Если говорить, например, о контроле над персоналом, то у данной технологии есть совершенно очевидные преимущества, когда речь идет, например, о контроле доступа на различные объекты в целях обеспечения производственной безопасности. В этом случае система автоматически распознает ситуацию, когда, например, сотрудник без соответствующего допуска приближается к опасному объекту или просто находится там, где ему не положено находиться. Аналогично уже достаточно давно существуют системы, позволяющие, например, контролировать местоположение и скорость передвижения транспортных средств, что также используется как в целях обеспечения безопасности, так и в целях предотвращения других нарушений, таких как хищения или просто несанкционированные отклонения от маршрута, приводящие к повышенному расходу топлива. В ряде случаев использование систем тотального контроля с помощью «умных» устройств представляется вполне оправданным.

Но с течением времени все более остро будет стоять вопрос о том, где находится та грань, за которой заканчивается действительно необходимый и оправданный контроль и начинается вторжение в личную жизнь человека и возникает опасность жесткого тоталитарного контроля вплоть до описанных некогда Оруэллом санкций за «мыслепреступления». В настоящее время это уже звучит отнюдь не так фантастично. В области управления персоналом давно используется оценка организационного климата, вовлеченности, удовлетворенности организацией и т.п. С появлением современных систем распознавания образов, машинного зрения и достаточно мощных нейросетей регулярно звучат запросы на то, чтобы иметь возможность оценивать вовлеченность и удовлетворенность организацией, анализируя выражение лиц сотрудников с помощью камер в автоматическом режиме. Совершенно очевидно, что как только появится техническое решение, способное сколько-нибудь эффективно решать данную задачу, то очень многим руководителям неминуемо придет в голову «простое и логичное» решение типа «довольных поощрять, а от недовольных избавляться».

Показательной в этом плане является существующая уже сегодня практика владельцев и руководства социальных сетей по блокировке аккаунтов и удалению информации тех пользователей, которые по каким-либо причинам их не устраивают. Причем данные меры принимаются даже к таким людям, как президент (ныне уже экс-президент) США Дональд Трамп. Если даже всемирно известные люди, обладающие весьма значительным влиянием и капиталами, подвергаются цензуре в информационном пространстве социальных сетей, то что говорить об обычных гражданах?

Подобная практика не нова. Достаточно вспомнить демонстративное сожжение в нацистской Германии книг, содержание которых противоречило идеологии национал-социализма, ретуширование фотографий с целью удаления с них определенных персонажей или уничтожение архивов. То же самое можно сказать о кампаниях по дезинформации, которые в наше время, в частности, приняли форму распространения ложных, или на интернет-сленге фейковых новостей. Но у цифровой эпохи есть свои особенности. Поскольку соответствующие системы управляются централизованно, то информация может быть удалена или искажена практически без каких-либо следов. В распоряжении обычного человека практически отсутствуют какие-либо средства, дающие возможность хотя

бы проверить подлинность той или иной информации или документа или доказать, что удаленная информация вообще когда-либо существовала. И это при том, что практически неограниченные объемы информации на электронных носителях могут быть удалены или изменены, что называется, одной кнопкой. Таким образом, снова получается, что весьма узкий круг лиц, являющихся владельцами или операторами разного рода информационных ресурсов, получают практически неограниченные возможности для оказания информационного влияния в глобальном масштабе при том, что контроль со стороны общества за ними невозможен чисто технически.

В этой связи ключевыми становятся вопросы: как контролировать владельцев информационных ресурсов? Как обеспечить достоверность информации и ее защиту от преднамеренного удаления или искажения в интересах тех или иных лиц? Кто и каким образом будет программировать системы типа «социального рейтинга»? Что именно будет считаться заслугой, а что – нарушением? Кто будет принимать эти решения? Каким образом граждане смогут это контролировать и влиять на это? Каким образом будут выявляться и пресекаться злоупотребления, например понижение рейтинга в качестве мести или для оказания давления на какого-либо человека или группу людей?

Эффективной мерой мог бы быть «зеркальный» цифровой контроль со стороны сотрудников, если речь идет об организациях, или жителей, если речь идет о городах, регионах или странах. В г. Москве давно уже используется практика получения обратной связи от жителей через городские порталы, основным среди которых является портал Mos.ru. Также в г. Москве на выборах в Мосгордуму, а затем уже и на выборах высших должностных лиц субъектов Российской Федерации было применено дистанционное электронное голосование на цифровых избирательных участках [6].

Технически в настоящее время вполне возможна реализация цифрового контроля над деятельностью органов власти со стороны населения или же цифрового контроля и обратной связи со стороны сотрудников в организации. По сути, это позволило бы реализовать идею «цифровой демократии», в рамках которой сотрудники организации или жители города, региона или страны могли бы в режиме реального времени напрямую оценивать действия должностных лиц. И в случае, когда количество отрицательных оценок превышало бы определенный порог, поднимался бы вопрос о принятии соответствующих мер. В рамках организации это мог бы быть дополнительный анализ деятельности руководителя, в рамках государственного и муниципального управления таким образом мог бы решаться вопрос, например, об отзыве депутата, не выполняющего свои функции или о принятии мер к руководителям соответствующих органов власти.

Однако очевидно, что основная проблема лежит вовсе не в технической плоскости. Основная проблема лежит в области, если так можно выразиться, общественного договора. Только если традиционно общественный договор подразумевает отказ людей от суверенных прав в пользу государства, то описанная выше специфика цифровых технологий управления и контроля ставит противоположную задачу: государство (или руководство организаций, если речь идет об организациях) должно добровольно ограничить себя в возможностях использования цифровых технологий и предоставить гражданам возможности контроля над их использованием. В реальности трудно предположить, что те, в чьих руках сосредотачиваются практически неограниченные возможности для контроля и для манипулирования данными в свою пользу, добровольно пойдут на такие самоограничения. По крайней мере, это сделают далеко не все. Поэтому уже сейчас необходимо проводить определенную работу «снизу», чтобы люди, зная о возможных рисках, уже сейчас обращали внимание руководства на всех уровнях на необходимость совместного решения данной проблемы. В организациях это могут быть профсоюзы, в обществе – партии, общественные движения, объединения граждан и даже отдельные лица.

В этой связи видятся целесообразными определенные законодательные ограничения и введение мер «аналогового» контроля в целях недопущения злоупотреблений возможностями цифровых технологий. Это может быть, например, сохранение традиционных «бумажных» технологий выборов, проведение очных опросов, голосований и т.п. Такой подход, с одной стороны, дает людям возможность выбора, а выбор – это всегда важно. С другой стороны, параллельное использование цифровых и традиционных, «аналоговых», технологий позволяет верифицировать информацию подобно тому, как в настоящее время данные экзитполов сравниваются с официальными результатами выборов.

Выводы

Цифровые технологии, с одной стороны, создают видимость свободы рас-

пространения информации, прозрачности и доступности ее для каждого, но, с другой стороны, это оборачивается риском тотального контроля и манипуляций со стороны владельцев и операторов соответствующих систем, а также со стороны киберпреступников или даже государственных структур недружественных государств.

Поэтому использование цифровых технологий ставит перед организациями и перед обществом в целом задачу формирования совершенного нового типа «общественного договора», который если не исключал бы полностью подобные злоупотребления, то, по крайней мере, предусматривал бы механизмы общественного контроля и общественной оценки деятельности власти, если речь идет о государственном и муниципальном управлении, и руководства организаций в данной сфере.

Список литературы

1. Генпрокуратура Российской Федерации [Электронный ресурс]. URL: http://www.genproc.gov.ru/smi/news/genproc/news-1884166/ (дата обращения: 11.03.2021).

2. Shoshana Zuboff. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. Public Affairs; 1st edition. 2019. 704 p.

3. Социальный мониторинг [Электронный ресурс]. URL: https://www.mos.ru/city/projects/monitoring/ (дата обращения: 11.03.2021).

4. Васильчук Т. Антисоциальный мониторинг // Новая газета. № 57. 03.06.2020.

5. Социальный рейтинг в Китае. TADVISER [Электронный ресурс]. URL: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A1%D0%BE%D1%86%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9_%D1%80%D0%B5%D0%B9%D1%82%D0%B8%D0%BD%D0%B3_%D0%B2_%D0%9A%D0%B8%D1%82%D0%B0%D0%B5 (дата обращения: 11.03.2021).

6. Центральная избирательная комиссия Российской Федерации. Цифровые избирательные участки [Электронный ресурс]. URL: http://www.cikrf.ru/analog/ediny-den-golosovaniya-2019/tsifrovye-izbiratelnye-uchastki/ (дата обращения: 11.03.2021).