

Социология: теоретические и эмпирические исследования

УДК 316.77

DOI: 10.28995/2073-6401-2020-4-57-71

Есть ли место личным данным в цифровом будущем?

Виктор К. Левашов

*Институт социально-политических исследований ФНИСЦ РАН,
Москва, Россия, levachov@mail.ru*

Оксана В. Гребняк

*Институт социально-политических исследований ФНИСЦ РАН,
Москва, Россия, oksanapov@yandex.ru*

Аннотация. Авторы рассматривают зарубежный практический опыт (в первую очередь на примере КНР) в вопросах применения цифровых технологий и искусственного интеллекта для решения практических задач, продиктованных, в числе прочего, необходимостью контроля за распространением COVID-19. Сравнение методов борьбы с коронавирусом Китая и европейских стран демонстрирует акцент на разнополярных возможностях цифрового развития и их разницу с точки зрения эффективности борьбы с заболеванием и с точки зрения прав и свобод личности. Внимание уделено также особенностям сбора информации для bigdata, реальности и перспективам внедрения инновационных цифровых технологий и искусственного интеллекта на территории Российской Федерации. Ввод новейших цифровых технологий и систем искусственного интеллекта требует равновесия со стороны адаптированного под новинки законодательства и усилий, направленных на обеспечение безопасности частной жизни граждан в результате усиливающейся цифровизации всех систем государства. Подчеркивается важность ликвидации цифровой неграмотности как императива цифровых практик во всех сферах: как практического пользования приложениями, так и безопасности и функционирования технологий с целью создания комфортной цифровой среды для граждан всех поколений.

Ключевые слова: цифровизация, сбор данных, bigdata, безопасность личных данных, COVID-19, борьба с пандемией

© Левашов В.К., Гребняк О.В., 2020

Для цитирования: Левашов В.К., Гребняк О.В. Есть ли место личным данным в цифровом будущем? // Вестник РГГУ. Серия «Философия. Социология. Искусствоведение». 2020. № 4. С. 57–71. DOI: 10.28995/2073-6401-2020-4-57-71

Is there a place for personal data in the digital future?

Viktor K. Levashov

*Institute of Socio-Political Research of FCTAS RAS,
Moscow, Russia, levachov@mail.ru*

Oksana V. Grebnyak

*Institute of Socio-Political Research of FCTAS RAS,
Moscow, Russia, oksananov@yandex.ru*

Abstract. The authors consider foreign practical experience (primarily on the example of the PRC) in the application of digital technologies and artificial intelligence to solve practical tasks dictated, among other things, by the need to control the spread of COVID-19. A comparison of the methods used to combat the coronavirus in China and European countries demonstrates an emphasis on the heteropolar possibilities for digital development and their difference in the effectiveness of the fight against the disease and in terms of individual rights and freedoms. Attention is also paid to the specifics of collecting the information for Big Data, as well as the reality and prospects of implementing innovative digital technologies and artificial intelligence in the Russian Federation. The introduction of the latest digital technologies and artificial intelligence systems requires a balance between legislation adapted to new developments, and efforts aimed at ensuring the security of citizens' private lives as a result of the increasing digitalization in all state systems. It emphasizes the importance of digital illiteracy in all areas: both the practical use of applications, and the security and functioning of technologies in order to create a comfortable digital environment for citizens of all generations.

Keywords: digitalization, data collection, Big Data, personal data security, COVID-19, fighting the pandemic

For citation: Levashov, V.K. and Grebnyak, O.V. (2020), "Is there a place for personal data in the digital future?", *RSUH/RGGU Bulletin. "Philosophy. Sociology. Art Studies" Series*, no. 4, pp. 57–71, DOI: 10.28995/2073-6401-2020-4-57-71

Цифровизация и технологии искусственного интеллекта (ИИ) становятся стратегическим транснациональным трендом в рамках шестого технологического уклада. Их стремительное развитие и внедрение в повседневную жизнь обусловлено естественным развитием науки, техники, цивилизации и протимулировано мировым кризисом пандемии COVID-19. Являясь новым двигателем экономического роста, цифровизация и ИИ становятся основным предметом соперничества между крупнейшими мировыми державами. Не в меньшей степени, чем уровень технического развития, важно разумное встраивание новейших технологий в функционирование государства и обыденную жизнь. Меняются не только устройства и предметы, но и уклад жизнедеятельности общества, его культура, коммуникационная структура, уровень воздействия на окружающую среду. От соразмерной и бесконфликтной трансформации государства и общества под влиянием технологий зависит, насколько устойчивой будет дальнейшая коэволюция человека, общества и природы. На сегодняшний день говорить о соразмерности сложно, учитывая растущее цифровое неравенство. Равновесие имеет спорный формат: «цифра» и искусственный интеллект в равной степени подразумевают полярные понятия свободы слова в Интернете и жестких штрафов за обширный перечень тем; возможности использования анонимайзеров и сбор данных с возможностью их дешифрации и т. д. Иными словами, это в равной степени свобода и тотальный контроль, вопрос в том, готовы ли мы к такому равенству.

Актуальные цифровые практики

Способность оперативно применять новейшие технологии в соответствии с требованиями момента не менее важна, чем сам по себе уровень технологического развития. Эта способность, наравне с готовностью жертвовать личным пространством и личными удобствами для достижения общей цели стали необходимостью в 2020 г. в связи с распространением вируса COVID-19. Наилучшим образцом здесь может послужить пример Китайской народной республики.

В период коронавирусной пандемии на контроль за передвижением и контактами населения в Китае были брошены все системы видеонаблюдения и сбора гео- и идентификационных данных. Это немалая сеть: в 2020 г. общее число видеорекамер с системой автоматического распознавания лиц в КНР должно было достигнуть 626 млн. Контроль за перемещениями осуществлялся и мобильными

операторами. Оперативно была внедрена система «Код здоровья»: на основе базовых сведений о здоровье, перемещении, контактах каждому человеку присваивался QR-код определенного уровня (зеленый – свободное передвижение, желтый – самоизоляция на 7 дней, красный – самоизоляция на 14 дней). Коды считывались при посадке в такси, входах в крупные здания, вокзалы. Благодаря этому при обнаружении заболевших круг возможных зараженных оперативно выявлялся. Строжайшее выполнение всех карантинных требований, ношение масок в общественных местах и прочие санитарно-гигиенические меры привели к быстрому сокращению числа болеющих в период «первой волны». Устойчивое положение сохраняется и осенью 2020 г.: по данным Национальной комиссии здравоохранения КНР, 21 ноября было выявлено всего 17 новых случаев заболевания: из них 14 считаются «привозными» и лишь 3 случая «внутреннего» заражения¹. Для сравнения: в России по данным на 22 ноября за сутки был выявлен 24 581 новый случай заболевания²; во Франции за тот же период – свыше 13 тысяч³.

Справедливости ради отметим, что и государственное устройство, и менталитет населения Китая способствуют развертыванию более полной и быстрой системы цифрового контроля по сравнению с европейскими странами. В чрезвычайных ситуациях необходимость в централизованном регулировании и соблюдении жесткой дисциплины вырастает в разы. Успех Китая на первых же этапах борьбы с COVID-19 легко объясняется тем, что строгость выполнения предписаний и навык постоянного контроля является для местного социума нормой как элемент политической культуры, и для получения доступа к личным данным не нужны внештатные ситуации. В то же время правительства ряда европейских стран (в частности, Италии, Франции, Германии и др.), внедряя контроль за передвижениями зараженных граждан, вынуждены были экстренно принимать дополнительные законы и делать специальные заявления о возможности передачи личных данных без согласия лица, которому эти данные принадлежат. Действия эти были впоследствии раскритикованы судом Европейского союза, считающим незаконным массовый сбор и хранение данных через мобильных

¹Daily briefing on novel coronavirus cases in China // National Health Commission of the PRC. 22.11.2020. URL: http://en.nhc.gov.cn/2020-11/22/c_82218.htm (дата обращения 22.11.2020).

²Сайт «Стопкоронавирус». URL: <https://стопкоронавирус.рф>

³Во Франции за сутки выявили свыше 13 тыс. носителей SARS-CoV-2 // ИА REGNUM: [сайт]. 22.11.2020. URL: <https://regnum.ru/news/society/3121920.html> (дата обращения 22.11.2020).

и интернет-провайдеров под предлогом обеспечения национальной безопасности. Подобные меры, согласно резолюции суда ЕС, должны быть жестко ограничены во времени и проводиться исключительно под надзором судов или независимых административных органов⁴.

Подчеркнем оперативность Китая, ставшего очагом распространения нового заболевания. Китай первым ввел жесткие карантинные меры: часть населенных пунктов была заблокирована, в ряде городов было приостановлено движение общественного транспорта, проводилось массовое тестирование на наличие вируса, миллионам граждан было запрещено покидать дома. США и Европа начали подключать ограничительные меры значительно позднее, до последнего стремясь минимизировать потери для экономик из-за закрытия границ (для туристов, мигрантов, товаров), промышленных и культурно-развлекательных предприятий и пр.

Важно отметить, что меры по борьбе с коронавирусом – не единственный пример внедрения Китаем в обыденную реальность цифровых технологий. Так, с 2014 г. запущен пилотный проект системы социального кредита (social credit system), выстраивающего рейтинг индивида исходя из соблюдения им законов и правовых норм. За отсутствие противоправных действий, за общественную деятельность, своевременную оплату счетов и кредитов начисляются баллы, за нарушения и проступки – вычитаются. Зачисление/ списание происходит автоматически на основе данных систем контроля, наблюдений, сведений о графике выплаты налогов, штрафов и прочих баз цифровых данных, то есть благодаря тотальной цифровизации деятельности социальных, коммунальных, полицейских служб. Высокий социальный рейтинг гарантирует доступ к скидкам и льготам (например, снижение стоимости коммунальных услуг или процента по кредиту). Нежелание придерживаться правил понижает социальный рейтинг и, соответственно, закрывает доступ к социальным благам: неблагонадежным гражданам могут запретить занимать должности на госслужбе, отказать в продаже комфортных мест на поезд/самолет и, в некоторых случаях, вообще запретить пользоваться поездами и самолетами⁵. Согласно

⁴Пресс-релиз Суда ЕС от 06.10.2020. URL: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-10/cp200123en.pdf> (дата обращения 01.10.2020).

⁵China to bar people with bad “social credit” from planes, trains // REUTERS. 16.03.2018. URL: [/https://www.reuters.com/article/us-china-credit/china-to-bar-people-with-bad-social-credit-from-planes-trains-idUSKCN1GS10S](https://www.reuters.com/article/us-china-credit/china-to-bar-people-with-bad-social-credit-from-planes-trains-idUSKCN1GS10S) (дата обращения 01.10.2020).

программе, к 2020 г. каждый гражданин Китая будет оцениваться в режиме реального времени [Самусева 2019]. По оценке всемирной правозащитной организации Human Rights Watch, Китай выстроил «сеть тотальной государственной электронной слежки и изощренную систему интернет-цензуры»⁶. Даже работа местного Интернета построена в рамках «Великого китайского файервола», позволяющего властям ограничивать доступ к зарубежным ресурсам и фильтровать результаты запросов в поисковых сетях.

Близкие по функциям цифровые технологии, вводимые на территории РФ, как правило, вызывают отторжение в социуме [Белова, Великая 2020]. Камеры с функцией распознавания лиц, социальный мониторинг передвижений для больных коронавирусом, цифровые пропуска и т. д. – в первую очередь воспринимаются и обозначаются как первые шаги к цифровому концлагерю и тотальной слежке.

Цифровой след

Реакция российских граждан на установку камер с функцией распознавания личности и создание облачных баз данных для госучреждений создает впечатление, что это первые и уникальные для нашей страны технологии по сбору и хранению личной информации. Это ошибочное впечатление. Интернет давно перестал быть информационно-коммуникационной технологией, он превратился в полноценное социальное пространство, в котором каждый индивид уже оставил цифровой след (его называют также отпечатком и даже цифровой тенью), растущий с каждым днем – уникальный набор прослеживаемых действий в интернете. «Следы» оставляют смартфоны, ноутбуки, фитнес-трекер, проездные билеты, банковские карты. Информация о пользователе и его действиях сохраняется в глобальном массиве больших данных (bigdata). Рост объемов циркулирующей информации колоссальный: по прогнозам, глобальная инфосфера к 2025 г. может вырасти до 175 зетабайт⁷ (для справки 1 Зетабайт = 1 триллион Гигабайт). Очевидна

⁶ *Пом К.* Китай как источник глобальной угрозы правам человека: Всемирный доклад 2020 / HumanRightsWatch: [сайт]. URL: <https://www.hrw.org/ru/world-report/2020/country-chapters/337324> (дата обращения 30.09.2020).

⁷ The Digitization of the World – From Edge to Core. Исследование International Data Corporation при поддержке Seagate Technology. URL: <https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf> (дата обращения 30.09.2020).

ее коммерческая ценность, что приводит к постоянному совершенствованию технологии обработки больших данных и извлечения из них прибыли.

В Интернете источниками сведений становятся запросы поисковых систем, переписка и контакты социальных сетей, данные от «умных» вещей и многое другое. Подавляющее большинство маркетинговых стратегий и избирательных программ строится на изучении информации о потребителе/избирателе и подборе максимально эффективных методик влияния на него. Свою выгоду находят злоумышленники: из размещенных фотографий, комментариев, по результатам банковских транзакций и проставляемых «лайков» можно составить общую картину о месте жительства и работы, уровне дохода, политических и религиозных взглядах, совершаемых покупках и использовать их в мошеннических схемах. Как отмечает израильский ученый Юваль Ной Харари (Yuval Noah Harari), личные данные сместили землю и технологии, возглавив рейтинг ценных ресурсов: «Сегодня информация является самым ценным активом в мире, потому что с её помощью можно завладеть и манипулировать людьми. ...Ваши данные – самый важный актив, который у вас есть»⁸.

Совокупность следов можно условно разделить на две категории. *Идентификационные данные* – паспорт, адрес, телефон, место работы, личные фотографии, номер банковской карты и пр., что позволяет установить личность гражданина. Получение таких сведений открывает мошенникам широчайшие возможности для афер как в киберпространстве, так и оффлайн. *Пассивные данные* – совокупность сведений, собираемых из поисковых систем, мобильными операторами, технические файлы от посещенных ресурсов и др. Это отпечаток личности человека: в нем явно видны интенции человека, его интересы, потребности, социальный и интеллектуальный уровень. Это именно тот набор информации, который можно анализировать в обезличенном (то есть без использования идентификационных данных о гражданине) виде для статистики, бизнеса, маркетинга и пр.

Подчеркнем, что разделение совокупностей данных именно условное. Это важно учитывать, так как в действительности обязательства операторов по конфиденциальности, обезличиванию и прочие меры не являются гарантией анонимности персональных данных.

⁸Программа «Познер»: гость Юваль Ной Харари // 1TV. Выпуск от 24.06.2019. URL: <https://youtu.be/cr2o6EWdq9A?t=2327> (дата обращения 30.09.2020).

На сегодняшний день основной правовой преградой от злоупотреблений при обработке bigdata является Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных». Однако, как отмечают специалисты по информационному праву, технологии bigdata несовместимы с рядом базовых принципов, лежащих в основе законодательства о персональных данных [Савельев 2015]. К примеру, 152-ФЗ ограничивает использование собранных данных конкретными, заранее сформулированными целями (ст. 5, пункт 2), в то время как суть и смысл bigdata в многократном использовании. Также ст. 5, пункт 3 запрещает объединение баз данных, что выносит за рамки правового поля ряд аналитических преимуществ технологии работы с bigdata.

Что же касается обезличивания анализируемых данных, приказ Роскомнадзора от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных» формулирует однозначные требования. В частности, должны использоваться обратимые методики, то есть должна оставаться «возможность преобразования, обратного обезличиванию (деобезличивание), которое позволит привести обезличенные данные к исходному виду, позволяющему определить принадлежность персональных данных конкретному субъекту, устранить анонимность», а также «возможность косвенного деобезличивания (возможность проведения деобезличивания с использованием информации других операторов)»⁹.

Итак, понятно, что обезличивание не сможет обеспечить защиту и неприкосновенность личных данных и частной жизни граждан. Тем временем внедряются все новые технологии, направленные на сбор и анализ новых объемов информации, в том числе носящих изначально идентификационный характер.

Цифровизация в России и отношение к ней граждан

В настоящее время практические разработки в сфере ИИ и нейросетей идут полным ходом и постепенно включаются в различные отрасли экономики и общественных отношений. Пока сохраняется выраженная неравномерность цифровой оснащенности центра-

⁹Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных». URL: <https://base.garant.ru/70451476/> (дата обращения 11.11.2020).

ной области страны и отдаленных регионов, столичный регион используется как «песочница» для отработки цифровых систем, планируемых к распространению по мере сокращения цифрового неравенства.

Так, московский метрополитен с 2018 г. тестирует систему распознавания лиц. Современные камеры способны «узнать» человека, чье фото есть в базе, даже в маске, очках и головном уборе, что повышает шанс поимки преступников, находящихся в федеральном розыске. При наличии базы данных, сопряженной с медицинскими сведениями, в чрезвычайных ситуациях наподобие пандемии COVID-19 камеры могли бы предупреждать о входе в метро граждан с подтвержденным диагнозом, нарушивших карантин. В перспективах обыденного использования таких камер – подключение возможности оплаты «лицом».

Есть еще множество интересных наработок отечественного производства. К примеру, российский разработчик средств информационной безопасности «Сёрч Информ» выпустил систему Profile Center с уникальным алгоритмом анализа текста по общей тональности, длине предложений, преобладанию тех или иных слов. По результатам составляется психологический портрет пользователя на основе более чем трех десятков личностных качеств: базовые эмоции, психотип, уровень самооценки и амбиций, возможное взаимодействие с коллективом, риски правонарушений. Помимо статичного психологического портрета модуль способен выполнять прогностические функции.

В ходе совместной работы специалистов Научного центра психологического здоровья, Психологического института РАО и Института русского языка им. В.В. Виноградова разрабатывается сервис, позволяющий диагностировать склонность к депрессии, обнаружить признаки агрессии или иного пограничного состояния по активности человека в социальных сетях. В ходе конференции Open Talks AI-2020 о сервисе рассказал заведомом «Интеллектуальный анализ информации» Института проблем искусственного интеллекта ФИЦ ИУ РАН Иван Смирнов: «Мы получаем информацию из профиля, информацию о социальных связях: друзья, подписчики, сообщества. И анализируем изображения, которые публикует пользователь. Например, невротизм и экстраверсия очень хорошо определяются только на основе информации из профиля и матрицы репостов»¹⁰.

¹⁰ *Ядуха В.* Искусственный интеллект ставит диагнозы пользователям соцсетей // Журнал «Компания». 05.03.2020. URL: <https://ko.ru/articles/iskusstvennyu-intellekt-stavit-diagnozy-polzovatelyam-sotssetey/> (дата обращения 11.11.2020).

В 2020 г. в России активизировался и прямой сбор личных данных: 8 июня 2020 г. подписан ФЗ-№ 168 «О едином федеральном информационном регистре, содержащем сведения о населении Российской Федерации». В документе будут зафиксированы все идентификационные номера, сведения об образовании, работе, родителях, супругах и детях, долгах, состоянии здоровья. Запущенный несколько ранее перевод медицинских карт и трудовых книжек в цифровой формат отлично вписывается в процесс пополнения ЕФИР (единый федеральный информационный регистр), как и запущенный 1 июля 2020 г. эксперимент по созданию и (в дальнейшем) использованию приложения «Мобильный идентификатор» вместо гражданского паспорта. По совокупности фактов, граждане сразу провели параллели между созданием единого регистра, активизации проекта цифрового паспорта, вспомнили QR-коды для цифровых пропусков в период самоизоляции и сравнили всю эту совокупность с китайскими QR-кодами. За опасение перспектив тотальной цифровой диктатуры легко зацепились и длительное время муссировались в обществе конспирологические теории о чипировании через вакцинацию, включающие в себя возможность прямой манипуляции носителями.

Еще одним крупнейшим и одним из самых неоднозначно воспринятых пилотным проектом текущего года можно назвать закон об искусственном интеллекте, принятый для скорейшего усовершенствования комплекса технологических решений, имитирующего когнитивные функции человека. Эксперимент, начавшийся в июне 2020 г., расширит правительственные базы данных новыми объемами изображений, голосов и т. д. «Можно сказать, что новый закон подразумевает официальное оформление тотального контроля над гражданами, что чревато нарушением их права на неприкосновенность частной жизни, а также, имея в виду слабую защиту персональных данных, усиление мошеннических схем», – отмечает М. Игнатъев (руководитель адвокатского бюро «Михаил Игнатъев и партнеры»¹¹. Не осталось в стороне от критики электронное голосование, проводимое в период пандемии COVID-19 и обнаружившее целый ряд недоработок и технических накладок, связанных как с процессом выборов, так и затруднениями доступа к нему.

В целом, что касается экстренного введения цифровых практик в период самоизоляции, основная заслуга – на взгляд рядовых

¹¹ Изменения в закон «О персональных данных» – контроль над гражданами // ИА REGNUM. 04.05.2020. URL: <https://regnum.ru/news/polit/2938192.html> (дата обращения 30.09.2020).

граждан – лежит на представителях бизнеса (торговые сети, зарубежные платформы видеоконференций), а неудачные инициативы и тревожные ожидания ассоциируются с действиями правительства, что, на взгляд автора, выстраивает негативное совокупное отношение граждан к цифровизации [Новожедина, Гребняк 2020]. Общую тенденцию можно наблюдать по итогам проведенного в декабре 2018 г. Институтом социально-политических исследований ФНИСЦ РАН 48-го этапа мониторинга «Как живешь, Россия?». Резкий рост пользователей цифровых технологий, вызванный пандемией, еще не начался, что объясняет большое количество граждан, затруднившихся с оценкой влияния цифровых технологий на нашу жизнь (см. табл. 1). Но вектор становления отношения к эффектам «цифры» уже можно проследить.

Таблица 1

Мнение респондентов о том, к каким результатам приводит внедрение цифровых технологий в нашу жизнь (РФ, декабрь 2018. N = 1605)

<i>Вопрос: «Прочитайте суждения о том, к каким результатам приводит внедрение цифровых технологий в нашу жизнь, и в каждой из пяти пар отметьте то суждение, с которым Вы согласны»</i>	%
К повышению уровня и качества жизни всех граждан страны	37
К снижению уровня и качества жизни, увеличению количества бедных граждан	21
Затруднились ответить	42
К участию граждан в управлении обществом и государством	26
К снижению уровня прав, свобод и безопасности граждан	24
Затруднились ответить	50
К укреплению суверенитета и безопасности страны	21
К ослаблению суверенитета и к росту зависимости извне	26
Затруднились ответить	53
К расширению свободного доступа к мировому культурному наследию, научному знанию и сохранению природы	34
К навязыванию стандартов и ценностей массового потребления товаров и услуг, к деградации природы	34

Окончание табл. 1

<i>Вопрос: «Прочитайте суждения о том, к каким результатам приводит внедрение цифровых технологий в нашу жизнь, и в каждой из пяти пар отметьте то суждение, с которым Вы согласны»</i>	%
Затруднились ответить	32
К здоровому образу жизни и укреплению нравственности	17
<i>К разрушению нравственности и моральной деградации</i>	33
Затруднились ответить	50

Источник: Левашов В.К., Афанасьев В.А., Новоженина О.П., Шушанова И.С. Экспресс-информация: Как живешь, Россия? XLVIII этап социологического мониторинга, ноябрь–декабрь 2018 г. / Под общ. ред. В.К. Левашова [Электронное издание]. М.: Перспектива, 2019. 59 с. URL: <https://goo.gl/2ZAze1>

Респондентам предлагалось выбрать ответы в пяти парах альтернативных суждений¹². Этот индикатор позволяет получить информацию о том, как оценивается гражданами реализация цифровых технологий с пяти разных сторон нашей жизни. Как видно из таблицы, лишь в отношении последствий для уровня и качества жизни граждан респонденты настроены оптимистично. По двум индикаторам из пяти («Ослабление суверенитета и безопасности страны» и «Разрушение нравственности и моральная деградация») негативные ожидания преобладают. В отношении прав и свобод граждан, а также доступа к мировому культурному наследию и культуре потребления мнение респондентов почти в равной степени разделилось на оптимистичное и пессимистичное.

Заключение

РФ обладает технологическими и интеллектуальными возможностями для дальнейшей разработки собственных и внедрения зарубежных технологий. Сложность состоит в преодолении кри-

¹² *Левашов В.К., Афанасьев В.А., Новоженина О.П., Шушанова И.С. Экспресс-информация: Как живешь, Россия? XLVIII этап социологического мониторинга, ноябрь–декабрь 2018 г. / Под общ. ред. В.К. Левашова [Электронный ресурс]. М.: Перспектива, 2019. 59 с. URL: <https://goo.gl/2ZAze1>*

тического отношения со стороны граждан и повышении цифровой грамотности. Ключевым фактором успешного функционирования систем искусственного интеллекта, технологий отслеживания контактов заболевших граждан, маркетинговых и новостных алгоритмов и пр. является сбор и анализ личной информации. Исторически это имеет отрицательную социально-политическую коннотацию в восприятии россиян и воспринимается как слежка, вездесущий глаз условного «большого брата», создавая ощущение поднадзорности и вызывая чувство протеста. На наш взгляд, для реализации программы Цифровой экономики РФ в целом и внедрения технологий, способных сыграть роль в борьбе с ситуациями, аналогичными тем, что сложились в период пандемии COVID-19 в частности, необходимо усилить работу по двум направлениям.

Первое – это обеспечение безопасности хранения, передачи и доступа к полученным от граждан идентификационным сведениям. На сегодняшний день слишком часты утечки из баз данных, содержащих паспортные данные, финансовую информацию, номера телефонов и пр. Согласно аналитике Info Watch, за 2019 г. объем утечки персональных данных в России вырос более чем на 40% по сравнению с 2018 г. В итоге количество скомпрометированных персональных составило более 170 млн¹³. Безопасность хранения должна предоставляться по умолчанию, а не являться дополнительной платной функцией. Чувство защищенности остается одной из базовых потребностей человека, без которой невозможно стабильное, устойчивое гражданское общество [Немировский, Немировская 2012]. Потеря контроля над приватностью делает невозможным ощущение социальной защищенности. Дополнительным подтверждением вышесказанному служит тот факт, что, несмотря на невысокую общую оценку важности нацпроекта «Цифровая экономика» (8-е место из 13 проектов для респондента лично и 11-е место из 13 для всего общества), 16% опрошенных в августе–сентябре 2020 г. респондентов считают «защиту цифровой информации и персональных данных» самой необходимой из внесенных в Конституцию РФ поправок¹⁴.

Второе направление – комплексное – касается повышения доверия к действиям властей. Из вышеизложенного видно, что

¹³ Урманцева А. Переход на личное: в 2019 г. утекло вдвое больше персональных данных // Известия. 2019. 27 дек. № 247 (30477). С. 1.

¹⁴ Экспресс-информация: Как живешь, Россия? 50-й этап социологического мониторинга, август–сентябрь 2020 года / В.К. Левашов, Н.М. Великая, И.С. Шушпанова [и др.]; отв. ред. В.К. Левашов; ФНИСЦ РАН. М.: Перспектива, 2020 [Электронный ресурс]. URL: <http://испи.рф/wp-content/uploads/2020/12/экспресс-информация-как-живёшь-россия.pdf>

большинство пессимистичных ожиданий напрямую связано с опасениями граждан, что полученные данные будут использоваться для манипуляций, контроля, дополнительных финансовых сборов, пропаганды. Для принуждения, дополнительных ограничений или в иных, не раскрываемых заранее, целях. Без минимизации этих факторов в общественном сознании высока вероятность отторжения массового внедрения «умных» технологий. Целью и фундаментом цифрового всеобуча должно стать всеобщее повышение цифровой грамотности граждан не только в сфере практического владения конкретными приложениям, но и в усвоении научно-популярных представлений о принципах функционирования новейших технологий, что позволит повысить научно-критическое восприятие конспирологических теорий.

Литература

- Белова, Великая, Фадеева 2020 – *Белова Н.И., Великая Н.М., Фадеева Е.В.* Социальные страхи россиян в условиях пандемии коронавирусной инфекции COVID-19 // I Российско-Иранский социологический форум: Сборник тезисов докладов участников форума / Отв. ред. С.В. Рязанцев, Т.К. Ростовская. М.: Перспектива, 2020. С. 186–196.
- Немировский, Немировская 2012 – *Немировский В.Г., Немировская А.В.* Чувство незащищенности от социальных опасностей как основа типологизации регионов // Мониторинг общественного мнения. 2012. № 1 (107). С. 113–127.
- Новоженкина, Гребняк 2020 – *Новоженкина О.П., Гребняк О.В.* Особенности реализации проекта «Цифровая экономика» в условиях пандемической реальности // X Международная социологическая Грушинская конференция «Жить в России. Жить в мире. Социология повседневности»: Материалы конференции / Отв. ред. А.В. Кулешова. М.: ВЦИОМ, 2020. С. 139–144.
- Савельев 2015 – *Савельев А.И.* Проблемы применения законодательства о персональных данных в эпоху «Больших данных» (BigData) // Право: Журнал Высшей школы экономики. 2015. № 1. С. 43–66.
- Самусева 2019 – *Самусева О.А.* Социальный рейтинг как системная характеристика политической надежности в китайском обществе // Социально-гуманитарные знания. 2019. № 6. С. 349–361.

References

- Belova, N.I., Velikaya, N.M. and Fadeeva, E.V. (2020), “Socialnuyе strahi v usloviyah pandemii koronavirusnoi infekcii COVID-19” [Social fears of Russians in the context of the Covid-19 pandemic], in Ryazantsev, S.V. and Rostovskaya, T.K. (eds.),

- I Rossijsko-Iranskiy sociologicheskiiy forum, sbornik tezisev dokladov uchastnikov foruma* [Proceedings of the 4th International Conference on I Russian Iranian sociological Forum], Perspektiva, Moscow, Russia, pp. 186–196.
- Nemirovsky, V.G. and Nemirovskaya, A.V. (2012), “*Chuvstvo nezashchishchemosti ot sotsial'nykh hopasnostey kak osnova tipologizatsii regionov*” [Sense of unprotectedness against social dangers as a basis of the regions typology], The public opinion monitoring, no. 1 (107), Russia, pp. 113–127.
- Novozhenina, O.P. and Grebnyak, O.V. (2020), “Features of the Digital Economy project implementation in the context of pandemic reality”, in Kuleshova, A.V. (ed.), *Proceedings of the X international sociological Grushin conference “Living in Russia. Living in peace. Sociology of everyday life”*, Vserossiiskii tsentr izucheniya obshchestvennogo mneniya, Moscow, Russia, pp. 139–144.
- Savelyev, A.I. (2015), “The Issues of Implementing Legislation on Personal Data in the Era of Big Data”, *Pravo. Zhurnal Vysshey shkoly ekonomiki*, no. 1, pp. 43–66.
- Samuseva, O. (2019), “Social rating as a system mark of political reliability in the Chinese society”, *Sotsial'no-gumanitarnye znaniia*, no. 6, pp. 349–361.

Информация об авторах

Виктор К. Левашов, доктор социологических наук, Институт социально-политических исследований ФНИСЦ РАН, Москва, Россия; 119333, Россия, Москва, ул. Фотиевой, д. 6, корп. 1; levachov@mail.ru

Оксана В. Гребняк, Институт социально-политических исследований ФНИСЦ РАН, Москва, Россия; 119333, Россия, Москва, ул. Фотиевой, д. 6, корп. 1; oksananov@yandex.ru

Information about the authors

Viktor K. Levashov, Dr. of Sci. (Sociology), Institute of Socio-Political Research of FCTAS RAS, Moscow, Russia; bldg. 1, bld. 6, Fotieva Str., Moscow, Russia, 119333; levachov@mail.ru

Oksana V. Grebnyak, Institute of Socio-Political Research of FCTAS RAS, Moscow, Russia; bldg. 1, bld. 6, Fotieva Str., Moscow, Russia, 119333; oksananov@yandex.ru