Демаркация публичного и приватного при взаимодействии государства и граждан на цифровых сетевых платформах

УДК 316.776 DOI https://doi.org/10.26425/2658-347X-2021-4-3-16-26

Получено 15.06.2021 Доработано после рецензирования 09.07.2021 Принято 21.07.2021

Зотов Виталий Владимирович

Д-р социол. наук, проф., ФГАОУ ВО «Московский физико-технический институт (национальный исследовательский университет)», г. Москва, Российская Федерация

ORCID: https://orcid.org/0000-0003-1083-1097

E-mail: Om_zotova@mail.ru

АННОТАЦИЯ

Цифровые сетевые платформы построены на социотехническом взаимодействии между акторами и актантами. Создание и развитие государственных сервисов на основе цифровых платформ неминуемо ведет к трансформации взаимоотношений государства и граждан. Привлекательность государственных цифровых платформ для граждан повышается при разрешении противоречия между возможностями новых форм социального взаимодействия и угрозой неправомерного использования персональных данных, риском причинения вреда или преследований.

В статье представлены результаты анализа границ публичного и приватного при взаимодействии государства с гражданами на цифровых сетевых платформах. Метод исследования – сравнительный анализ, который базируется на дихотомии публичного и приватного, отраженной в концепции приватного и публичного Х. Арендт, концепции публичной сферы Ю. Хабермаса, нормативно-правовой концепции приватности Р. Гависона. Эмпирическую базу составили социологическое исследование, проведенное с целью получения информации о границах приватности и публичности персональных данных в цифровом сетевом пространстве (n = 1 000 среди населения старше 18 лет, проживающего в столичных мегаполисах и медианных по уровню информатизации регионах в 2020 г.), и результаты опросов Лаборатории Касперского, проведенные в 2019 г. и 2020 г.

Проведенное исследование позволяет утверждать, что практически 2/3 граждан сталкивались с неправомерным использованием в сети «Интернет» конфиденциальных сведений. Большинство опрошенных осведомлены о том, что сайты, социальные сети и поисковые системы могут собирать данные для веб-аналитики. При этом граждане считают возможным передачу персональных данных органам власти в обобщенном виде для принятия управленческих решений. Половина опрошенного населения не возражает против осуществления цифрового контроля за действиями и перемещениями граждан. Таким образом, несмотря на имеющийся негативный опыт, явное сопротивление при организации сбора персональной информации на цифровых сетевых платформах маловероятно.

Ключевые слова

Цифровизация, цифровая трансформация, приватная сфера, публичная сфера, взаимодействие государства и общества, цифровые сетевые платформы, государственные платформы, персональные данные

Для цитирования

Зотов В.В. Демаркация публичного и приватного при взаимодействии государства и граждан на цифровых сетевых платформах//Цифровая социология. 2021. Т. 4, № 3. С. 16–26.

Благодарности

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 20-011-00694 «Публичное управление как конфигурирование релятивных сетей в публичном пространстве цифрового общества».

Demarcation of the public and private in the interaction of the state and citizens on digital network platforms

DOI https://doi.org/10.26425/2658-347X-2021-4-3-16-26

Received 15.06.2021 Revised 09.07.2021 Accepted 21.07.2021

Vitaliy V. Zotov

Dr. Sci. (Soc.), Prof., Moscow Institute of Physics and Technology, Moscow, Russia

ORCID: https://orcid.org/0000-0003-1083-1097

E-mail: Om_zotova@mail.ru

ABSTRACT

Digital network platforms are built on sociotechnical interaction between actors and actors. The creation and development of new public services based on digital platforms inevitably leads to the transformation of the relationship between the state and citizens. The attractiveness of state digital platforms for citizens increases when resolving the contradiction between the possibilities of new forms of social interaction and the threat of misuse of personal data, the risk of harm or persecution.

The article presents the results of the analysis of the boundaries of the public and private in the interaction of the state with citizens on digital network platforms. The research method is a comparative analysis, which is based on the dichotomy of public and private, reflected in the concept of private and public X. Arendt, concepts of the public sphere J. Habermas, regulatory and legal concepts of privacy by R. Gavison. The empirical base was made up of a sociological study conducted to obtain information about the boundaries of privacy and publicity of personal data in the digital network space (n = 1 000 among the population over 18 years old living in metropolitan megacities and median regions by the level of informatization, 2020) and the results of Kaspersky Lab surveys conducted in 2019–2020.

The conducted research allows us to assert that almost 2/3 of citizens have faced the misuse of confidential information on the Internet. Most of the respondents are aware that websites, social networks and search engines can collect data for web analytics. At the same time, citizens consider it possible to transfer personal data to the authorities in a generalized form for making managerial decisions. Half of the surveyed population does not object to the implementation of digital control over the actions and movements of citizens. Thus, despite the existing negative experience, it is unlikely that there will be any obvious resistance to organizing the collection of personal information on digital network platforms.

Keywords

Digitalization, digital transformation, private sphere, public sphere, interaction of the state and society, digital network platforms, state platforms, personal data

For citation

Zotov V.V. (2021) Demarcation of the public and private in the Interaction of the state and citizens on digital network platforms. *Digital sociology*, vol. 4, no. 3, pp. 16–26. DOI: 10.26425/2658-347X-2021-4-3-16-26

Acknowledgements

The study was performed with the financial support of the Russian Foundation for Basic Research within the framework of the scientific project No. 20-011-00694 "Public administration as configuration of relational networks in the public space of a digital society".

ВВЕДЕНИЕ

Если в эпоху первоначального проникновения информационно-телекоммуникационных технологий в повседневную жизнь, виртуальный мир сети «Интернет» (далее – Интернет) воспринимался как место для развлечений, игры, «бегства» от бытовых невзгод, временного ухода от повседневности, то на сегодняшний день использование Интернета является жизненно необходимым: отказаться полностью от использования электронной почты, социальных медиа, мессенджеров означает уйти из жизни общества, стать своего рода отшельником. Сейчас онлайн-жизнь становится неотъемлемой частью офлайн-жизни, однако и индивиды, и общество в целом еще не успели перестроиться на этот новый, взаимопроникающий формат отношений офлайн- и онлайн-миров, что провоцирует конфликты, возникающие во многом из-за отсутствия демаркации между общественным и личным. В последнее десятилетие баланс между публичностью и приватностью радикально меняется. Например, обычный вход в аккаунт социальной сети Facebook, Twitter или Instagram, можно рассматривать и как выход в публичное пространство для презентации себя, своих мыслей, и как пребывание в узком приватном круге друзей и знакомых.

Новый этап информатизации – цифровизация – не просто сопровождается увеличением объема хранимой, передаваемой и обрабатываемой информации, но и ведет к созданию цифровых сетевых платформ, которые обладают аналитическими и прогностическими функциями. Суть платформы в том, что она создает не сервис по продаже и/или оказанию услуг, а экосистему, с помощью которой удобнее организовать взаимодействие между заинтересованными сторонами. А цифровизация публичного управления формирует концепцию платформенного государства [Сморгунов, 2019]. Цифровые сетевые платформы создают условия для объединения концепций «электронного правительства» и «электронной демократии». Они способствуют развитию гражданского участия в повседневных делах государства так же, как и повышению качества предоставляемых услуг [Зотов и др., 2021]. При этом успех цифровизации публичного управления определяется следующими техническими условиями: формированием платформ, облегчающих привлечение граждан к принятию решений; использованием методов автоматизированного принятия решений (на базе искусственного интеллекта) с минимальной возможностью участия человека, для снижения рисков; открытием информационных данных для принятия решений [Лихтин, 2021]. Именно организация цифровых сетевых платформ позволяет обеспечить поставленные Л.А. Василенко задачи перед системой публичного управления, а именно, создание: механизмов выполнения управленческих функций каждым ее актором (органами власти, институтами гражданского общества); алгоритмов согласования интересов всех субъектов и координации их последующих действий; инструментов для выражения интересов акторов, включая мониторинг и реализацию прав и обязанностей участников, а также механизмы урегулирования разногласий [Vasilenko, 2021].

Создание и развитие новых государственных сервисов на основе цифровых платформ неминуемо влечет за собой изменения формата взаимодействия государства и гражданами, формируя новые технологии управления. Платформы при этом становятся пространством для взаимодействия объединенных в сеть участников и позволяют правительству координировать эти взаимодействия, а также мотивировать сотрудников и поддерживать принципы бережливого правительства (англ. Lean Government) [Стырин, Дмитриева, 2021]. Теперь государственные структуры перестают быть главным субъектом управления: эту функцию выполняет набор алгоритмов и программных инструментов, которыми управляет платформа, контролируя и развивая децентрализованную сеть представителей заинтересованных сторон [Моазед, Джонсон, 2019].

Однако, наступления «прекрасного» будущего публичного управления в ближайшей перспективе ожидать не стоит, поскольку цифровизация имеет определенные границы, связанные с безопасностью персональных данных, а также сведений о личной жизни, финансовом благополучии, здоровье, взглядах и убеждениях человека. Уже не секрет, что цифровой след человека – это ценная информация для маркетологов, политтехнологов и иных социальных технологов. С завидным постоянством происходят намеренные или случайные утечки персональной информации. В качестве примера можно привести публикацию на форуме данных более 500 млн пользователей Facebook[1] или преднамеренное опубликование в Интернете персональных данных сторонников Алексея Навального накануне апрельских протестов[2].

Также очевидно, что претензии по вопросу конфиденциальности данных чаще всего затрагивают социальные сети Facebook, Twitter, Instagram, YouTube и TikTok, которые собирают информацию о пользователе напрямую. Хотя в последнее время в их число добавились и иные цифровые сетевые платформы: Google, Amazon Uber и др. Вокруг этих платформ уже функционирует обширная сеть компаний, которые занимаются сбором персональных данных и зарабатывают на их продаже.

[1] *BBC* (2019). Data on 540 million Facebook users exposed. Режим доступа: https://www.bbc.com/news/technology-47812470 (дата обращения: 12.06.2021).

[2] *Филипенок А., Скобелев В.* (2021). Роскомнадзор начнет проверку из-за утечки данных сторонников Навального // РБК. Режим доступа: https://www.rbc.ru/politics/20/04/2021/607ecf5b9a7947353f644f54 (дата обращения: 12.06.2021).

Они собирают, покупают, сортируют и продают данные, полученные в ходе фиксации цифровых следов повседневного взаимодействия граждан. Сегодня крайне опасным для развития российского социума могут стать две крайности: неправомерное распространение информации, приносящее ущерб интересам человека, семьи, общества и государства; изъятие из оборота ценной информации, способной стимулировать прогрессивное развитие государства [Василенко и др., 2010].

Сегодня крайне важно государственные платформы сделать достаточно привлекательными для граждан, чтобы последние активно присоединялись и поддерживали их. Для этого необходимо разрешить существующее противоречие между возможностями новых форм социального взаимодействия и угрозой неправомерного использования персональных данных, риском причинения вреда или преследований. В этом контексте особый смысл приобретает анализ границ публичного (то, что происходит во взаимодействии с другими людьми) и приватного (то, что защищается от выдачи другим) использования персональной информации в общественном сознании.

МЕТОДЫ

Основным методом исследования выступает сравнительный анализ, который опирается на дихотомию публичного и приватного. Исследование этой дихотомии имеет сложную историю, породившую многочисленные формулировки противопоставления публичного и частного, большинство из которых до сих пор определяют современное понимание терминов. Статья опирается на исследования классиков социально-гуманитарного познания, в частности на концепцию приватного и публичного Х. Арендт, концепцию публичной сферы Ю. Хабермаса, нормативно-правовую концепцию приватности Р. Гависона.

Эмпирической основой стало социологическое исследование, проведенное с целью получения достоверной и обоснованной информации о границах приватности и публичности персональных данных в цифровом сетевом пространстве. Генеральная совокупность исследования – население старше 18 лет, проживающее в столичных мегаполисах (Москва и Санкт-Петербург) и медианных по уровню информатизации регионах (Курская и Белгородская области, занимающие в рейтинге развития информационного общества 26 и 22 место соответственно). Выборочная совокупность в количестве n = 1 000 респондентов квотировалась по полу и возрасту (до 30 лет, от 30 до 60 лет, старше 60 лет). В связи с эпидемиологической ситуацией социологическое исследование проходило в форме массового анкетного опроса комбинированного типа: 1) онлайн-опрос с применением сервиса Google; 2) полевой опрос с использованием личных интервью с использованием бумажной анкеты. После проведения опроса в Google недостающие квоты были дополнены опросом среди населения. Из обработки были исключены анкеты, из которых было ясно, что респонденты не имеют компьютеров, не пользуются Интернетом, ничего не могут сказать о цифровых технологиях, поскольку они не связаны с их повседневной практикой. Данные опросов были дополнены результатами исследований Лаборатории Касперского, проведенных в 2019–2020 гг.[3,4].

ТЕОРЕТИКО-МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ

Практика разделения жизнедеятельности человека на публичное и приватное берет начало в работе Х. Арендт [Арендт, 2000]. Важная роль в данном исследовании отводится личностному аспекту публичного пространства. Х. Арендт рассматривает публику как совокупность личностей, способных лично контактировать друг с другом. В ее концепции публичная сфера – это пространство свободы равных индивидов. А личная свобода неотделима от публичности.

В контексте функционирования массмедиа к теме приватного и публичного обращался Ю. Хабермас, в работах которого понятия «публичное», «публичность» и, наконец, наиболее распространенное «публичная сфера» стали означать возможность существования пространства коммуникаций, в котором общественное мнение формируется в процессе совместной дискуссионной деятельности [Хабермас, 2017]. Публичная сфера выступает значимым фактором эволюции гражданского общества, поскольку именно она отвечает за актуализацию в общественном сознании вопросов, вызывающих озабоченность всех граждан и касающихся организации их совместной жизнедеятельности.

Публичная сфера предстает как неотъемлемая часть общества, формирующаяся на определенных этапах его развития. В рамках данной сферы открыто признается право граждан не только на свою позицию, но и возможность ее отстоять в соответствии с принятыми в обществе правилами демократической дискуссии. В отличии от Х. Арендт, которая выделяет личностный аспект в публичной сфере, у Ю. Хабермаса последняя предстает не ареной действий равных личностей, а внеличностным феноменом (местом осуществления коммуникации, обмена мнениями),

[3] *Блог Касперского* (2019). Цена приватности в Интернете: готовы ли пользователи рисковать личными данными? Режим доступа: https://www.kaspersky.ru/blog/privacy-report-2019-summary/22730/ (дата обращения: 12.06.2021).

[4] *Лаборатория Касперского* (2020). Опрос «Лаборатории Касперского»: 64% россиян пытались удалять информацию о себе с сайтов или из социальных сетей. Режим доступа: https://www.kaspersky.ru/about/press-releases/2020_opros-laboratorii-kasperskogo-64-rossiyan-pitalis-udalyat-informatsiyu-o-sebe (дата обращения: 12.06.2021).

возникающим из взаимодействия индивидов друг с другом. В работах Ю. Хабермаса понятие приватного практически не разрабатывается. Здесь приватная сфера выступает как условие личной автономии, по отношению к сфере публичной она играет служебную роль.

В. Кимличка предполагает, что на самом деле существует две различные дихотомии публичного и приватного: различие между общественно-доступным и личным и различие между государством и гражданским обществом [Kymlicka, 2001]. В рамках первой дихотомии личное выступает как приватное в том смысле, что оно представляет собой сферу жизнедеятельности, в которую можно отступить перед давлением общества и государства. В рамках второй – гражданское общество является приватным пространством, поскольку оно не управляется публичной властью государства. Вместе взятые эти дихотомии создают трехстороннее разделение совокупной жизнедеятельности человека по линии публичное/приватное: государство (публичное), гражданское общество (публично-приватное) и личность (приватное).

Понятно, что государство всегда позиционируется как публичное, личная жизнь индивида – как приватное. Как ни странно, гражданское общество предстает как приватное пространство, когда оно противопоставляется государству, и публичным, когда оно противопоставляется личному. В дальнейшем анализе будем исходить из данного соотношения, при этом исследовательское внимание сконцентрируем на приватной сфере личности.

Приватность предстает в аспекте непроницаемости для внешнего контроля, определенной сокрытости от общества и государства. Приватность подразумевает не только право человека на защиту своих персональных данных от посторонних, но и право на личное пространство и его защиту от вторжений. Израильский исследователь Р. Гависон в своем детальном анализе различных аспектов проблемы приватности отмечает, что приватность так или иначе связана с ограничением доступа других людей к индивиду, и выделяет три типа таких ограничений: 1) ограничение знаний других об индивиде; 2) ограничение физического доступа к индивиду; 3) ограничение внимания к индивиду со стороны других [Gavison, 1980]. Состояние полной приватности, где все вышеуказанные ограничения доведены до абсолюта, маловероятно и, более того, нежелательно. Но тем не менее, приватность должна находиться под защитой, поскольку нарушение ограничений Р. Гависона может стать серьезной проблемой для человека. Сохранение приватности предполагает запрет на действия, ее нарушающие, а также устранение вероятных посягательств на завоевание личного пространства человека [Шкудунова, 2007].

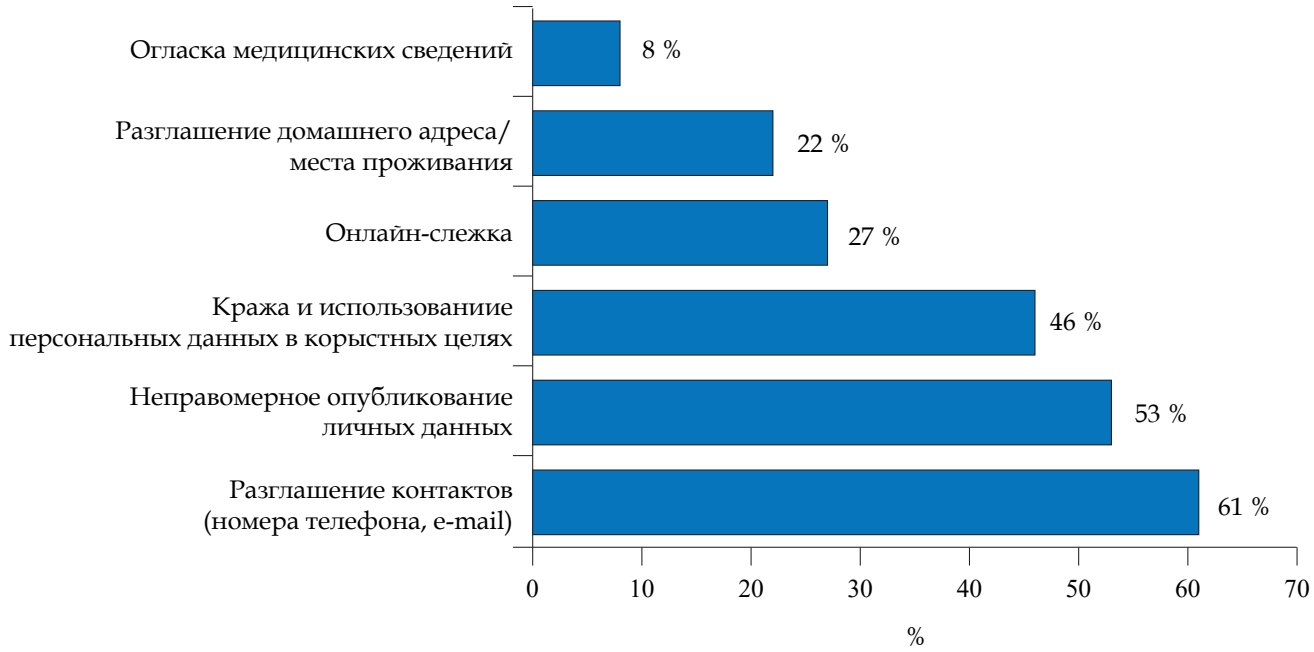
Развитие в начале XXI в. информационно-телекоммуникационных технологий, формирование информационно-коммуникационной среды, позволили публичной сфере стать пространством общественного диалога. Социальные медиа постепенно становятся одной из ключевых коммуникационных платформ, открытой и свободной для общественной активности индивида в рамках совещательной демократии [Саликов, 2018]. Но информационно-коммуникационная среда испытывает потребность в разработке механизма конфигурирования релятивной сети представителей заинтересованных сторон, который бы не нарушал приватности индивида.

АНАЛИЗ РЕЗУЛЬТАТОВ

Помимо очевидных плюсов Интернета существует и множество рисков его использования. В основу проводимого исследования было положено предположение о том, что граждане достаточно неохотно пускают государство в свою приватную сферу, поскольку это вызывает определенный дискомфорт, тревогу, опасение. Такая позиция формирует негативное отношение к государству, которое предстает как Левиафан, протягивающий свои щупальца в личную жизнь человека, в его приватное пространство.

В современном мире передача персональных данных через Интернет стала повседневной и абсолютно естественной практикой. Помимо очевидных плюсов Интернета существует и множество рисков «опубличивания» личной жизни пользователя сети. Однако онлайн-транзакции и общение в сети могут привести к утечке конфиденциальной информации. Чем больше информации можно найти о человеке в сетевом пространстве, тем выше для него риск столкнуться с различными угрозами, например, мошенничеством или кражей цифровой личности. Представленные на рисунке 1 результаты опроса показывают, что люди сталкиваются с определенными вещами, связанными с вторжением в их личное пространство в Интернете, охотой на их персональные данные.

Больше всего респонденты сталкивались с несанкционированным разглашением номера телефона, неправомерным опубликованием личных данных, кражей и использованием персональных данных в корыстных целях. Это подтверждает, что проблема вторжения в личную жизнь существует. Более половины опрошенных людей сталкивались с вторжениями в личное пространство, связанное с персональными данными. Особенно актуальна данная проблема для граждан с низким уровнем владения интернет-технологиями. Выход из данной ситуации видится в формировании компетентности, обеспечивающей возможность существования в цифровом обществе [Каргаполова и др., 2020; Проказина, 2020].



Составлено автором по материалам исследования / *Compiled by the author on the materials of the study*

***Рис. 1.* Распределение ответов на вопрос «Сталкивались ли Вы в сети «Интернет» со следующими ситуациями вторжения в личную жизнь?»**

Figure 1. Distribution of answers to the question "Have you encountered the following situations of invasion of privacy on the Internet?"

В ходе опроса о приватности в сети, проведенного Лабораторией Касперского при поддержке компании Toluna, выяснилось, что почти каждый пятый пользователь (18 %) находил в сети некую информацию о себе или своих близких, которую он бы предпочел не видеть в открытом доступе (n = 1 090 среди граждан Российской Федерации). По данным этого опроса 64 % россиян пытались удалять свои личные данные с сайтов или из социальных сетей[5].

Ежедневно социальные сети и другие электронные площадки аккумулируют широкий комплекс персональных данных пользователей, от личных переписок до данных банковских карт. Одновременно с этим растет вмешательство в частную жизнь человека, идет нарастание злоупотреблений данными о гражданине со стороны государства, использование «цифровой» личности в криминальных целях. Сюда включаются не только киберпреступность, но веб-мониторинг интернет-трафика пользователей, несанкционированное проникновение в личные гаджеты, расшифровка личных переписок граждан в мессенджерах, социальных сетях, игровых чатах и хищение приватной информации. Это несет угрозу конфиденциальности персональных данных пользователей. Поэтому следующий вопрос касался того, насколько люди понимают, что все те устройства, с которыми они работают, ведут сбор информации для веб-аналитики (см. рис. 2).

Опрос показал, что 46 % хорошо осведомлены о том, что идет процесс сбора информации, а 37 % что-то слышали об этом. Наибольший уровень полной осведомленности был зафиксирован среди жителей столичных мегаполисов – 70 %, значительно меньше в областных и районных центрах – 45 % и 46 % соответственно, в то время как в сельской местности показатель не превысил 31 %. Анализ возрастной структуры респондентов о осведомленности о возможности сбора данных веб-аналитики сайтами, социальными сетями и поисковыми системами показывает высокий уровень у молодежи по сравнению с пожилыми (51 % против 33 %).

Безусловно, когда человек заходит на сайт, устанавливает приложение, подсоединяет устройство, у него появляется предупреждение о том, что данные будут собираться. Поэтому осведомленность о сборе данных для веб-аналитики достаточно высокая. Отметим, что по данным опроса Лаборатории Касперского, в возможность обеспечить полную конфиденциальность личных данных в Интернете 56 % респондентов не верят (n = 11 000 пользователей из 21 страны)[6].

[5] *Лаборатория Касперского* (2020). Опрос «Лаборатории Касперского»: 64 % россиян пытались удалять информацию о себе с сайтов или из социальных сетей. Режим доступа: https://www.kaspersky.ru/about/press-releases/2020_opros-laboratorii-kasperskogo-64-rossiyan-pitalis-udalyat-informatsiyu-o-sebe (дата обращения: 12.06.2021).

[6] *Блог Касперского* (2019). Цена приватности в Интернете: готовы ли пользователи рисковать личными данными? Режим доступа: https://www.kaspersky.ru/blog/privacy-report-2019-summary/22730/ (дата обращения: 12.06.2021).

Составлено автором по материалам исследования / *Compiled by the author on the materials of the study*

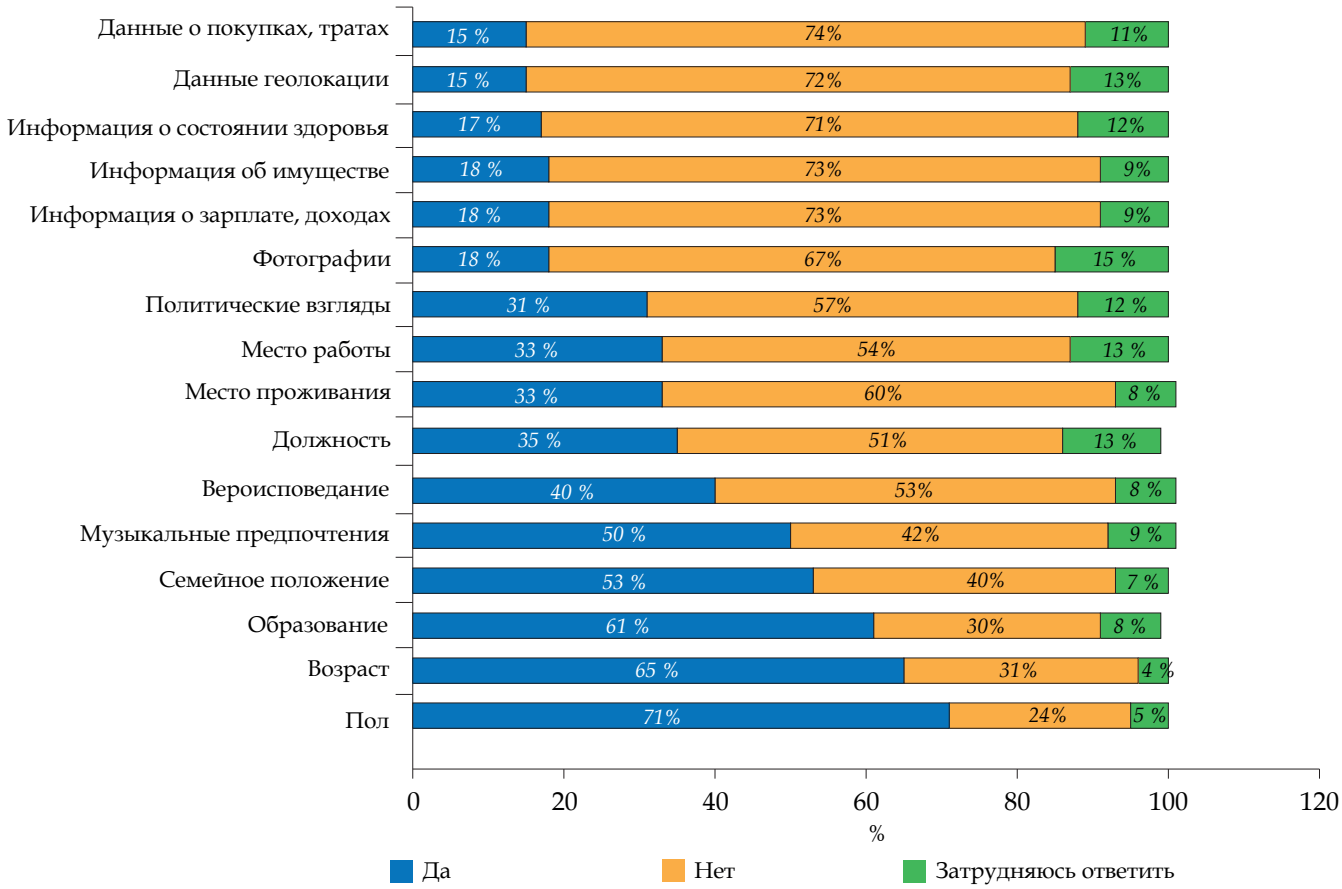
***Рис. 2.* Распределение ответов на вопрос «Интернет-сайты, социальные сети, поисковые системы могут собирать данные для веб-аналитики. Скажите, пожалуйста, Вы знаете, что-то слышали об этом или слышите сейчас впервые?»**

Figure 2. Distribution of answers to the question "Internet sites, social networks, search engines can collect data for web analytics. Tell me, please, do you know, have you heard something about this or are you hearing it now for the first time?"

Невзирая на все потенциальные угрозы, в данном опросе Лаборатории Касперского 18% пользователей ответили, что они готовы в обмен на бесплатные услуги, подарки или программные приложения поделиться личными данными. В рамках нашего исследования гораздо большая часть респондентов выказала готовность предоставлять государственным органам информацию о себе для использования обобщенном виде, анализа, принятия решений (см. рис. 3).

Представленные на рисунке данные показывают, что значительная часть людей готова предоставлять государству такие персональные данные, как пол, возраст, образование, семейное положение, то есть основные социально-демографические характеристики. В наименьшей мере люди готовы предоставлять информацию, связанную с личными доходами/расходами: информация об имуществе, информация о зарплате, информация о покупках, тратах. В этом же ряду находятся данные о геолокации, то есть о текущем местоположении. Здесь население не готово предоставлять эту информацию для использования даже в обобщенном виде. Хотя надо сказать, что значительная часть сервисов, например умные города, используют геолокацию для определения потоков пассажирооборота и т.п.

Очень долго человечество шло именно к приватности: своя квартира, своя комната, свой виртуальный мир. Сейчас же происходит возвращение к публичности. В городском пространстве появляются датчики движения и камеры видеонаблюдения, применяются программы распознавания лиц. В ближайшее время Правительство России планирует создать государственную информационную систему «Национальная платформа видеонаблюдения», которая возьмет на себя анализ видео со всех городских камер в стране. Сегодня каркас такой системы планируется создать только в городах-миллионниках и крупных краевых и областных центрах, на ключевых транспортных магистралях и самых критичных объектах городской инфраструктуры. Логику действий государства по аккумулированию всех данных понять можно, но в случае утечки данных в результате взлома, социальной инженерии или коррупции чиновников злоумышленник получит доступ к информации, которая очень чувствительна для любого гражданина. Он сможет не только предпринять попытку добраться до финансов гражданина, но и в перспективе анализировать его действия буквально пошагово, а это уже вторжение в приватное пространство человека не только со стороны государства, но и частных лиц.



Составлено автором по материалам исследования / *Compiled by the author on the materials of the study*

***Рис. 3.* Распределение ответов на вопрос «Согласны ли Вы предоставить органам власти следующие персональные данные для анализа и принятия решений?»**

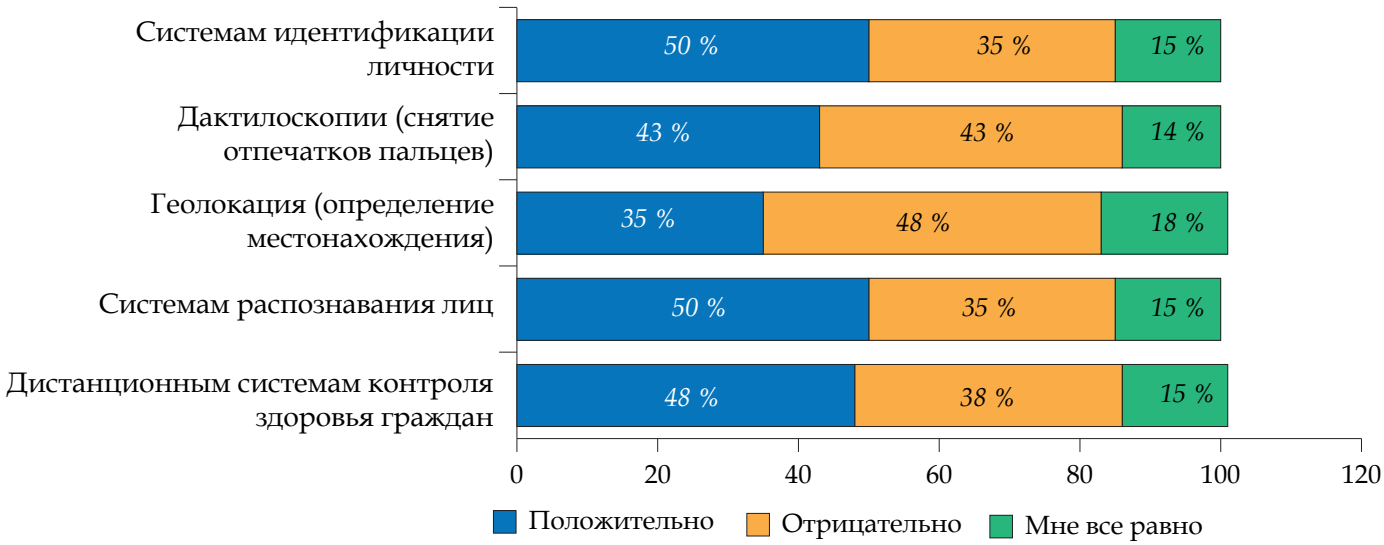
Figure 3. Distribution of answers to the question "Do you agree to provide the following personal data to the authorities for analysis and decision-making?"

В основе цифровых сетевых платформ лежит взаимодействие между акторами и актантами, которое реализуется благодаря не только прямому вводу информации человеком в стационарное или мобильное устройство, но и информации, получаемой со смарт-устройств и датчиков. Поэтому следующий вопрос затрагивал отношение респондентов к цифровым технологиям наблюдения и контроля за действиями и перемещениями граждан, данные которых используются на цифровых сетевых платформах.

Население в целом позитивно относится к отдельным системам наблюдения и контроля за действиями и перемещениями граждан (см. рис. 4). К системам распознавания лиц, а также к системам идентификации личности положительно относится 50 % респондентов, что на 15 п.п. больше отрицательного отношения к данным технологиям. Поровну распределись мнения респондентов относительно дактилоскопии (снятие отпечатков пальцев) – и положительно, и отрицательно к данной технологии относится по 43 % опрошенных. Скорее негативно население воспринимает только цифровые технологии определения геолокации (местонахождения) – 48 % опрошенных.

Распределение ответов населения согласно возрасту респондентов не позволило выявить существенных различий относительно восприятия отдельных инструментов наблюдения и контроля за действиями и перемещениями граждан. Тем не менее, старшее поколение наиболее положительно относится к технологиям распознавания лиц (55 %), респонденты среднего возраста – к системам идентификации личности (53 %), а молодежь – к дактилоскопии (45 %), геолокации (37 %) и дистанционным системам контроля здоровья граждан (52 %).

Распределение по типу населенного пункта, в котором проживают респонденты, позволило выявить тот факт, что жители сельских поселений в целом более позитивно относятся практически ко всем инструментам наблюдения и контроля за действиями и перемещениями граждан. Вероятно, это связано с тем, что данные инструменты не используются на уровне сельских поселений, тогда как жители мегаполисов и областных центров уже неоднократно сталкивались с ними.



Составлено автором по материалам исследования / *Compiled by the author on the materials of the study*

***Рис. 4.* Распределение ответов на вопрос: «Как Вы относитесь к следующим цифровым инструментам наблюдения и контроля за действиями и перемещениями граждан?»**

Figure 4. Distribution of the responses to the question: "How do you feel about the following digital tools for monitoring and controlling the actions and movements of citizens?"

ЗАКЛЮЧЕНИЕ

Если сделать промежуточные выводы, то можно утверждать о том, что с неправомерным использованием в сети «Интернет» конфиденциальных сведений сталкивались практически две трети опрошенных граждан. Большинство опрошенных осведомлены о том, что сайты, социальные сети и поисковые системы могут собирать данные для веб-аналитики. При этом граждане считают возможным передачу персональных данных органам власти в обобщенном виде для принятия управленческих решений. Половина опрошенного населения не возражает против осуществления цифрового контроля за действиями и перемещениями граждан.

Таким образом, несмотря на имеющийся негативный опыт население не возражает против вторжения в приватное пространство со стороны органов власти в рамках реализации публичного управления. И это свидетельствует о том, что при организации взаимодействия населения и государства на цифровых сетевых платформах не будет встречать ярого сопротивления. Да, здесь можно в какой-то мере говорить о цифровой некомпетентности населения, но футурофобии, страха будущего нет.

СПИСОК ЛИТЕРАТУРЫ

Арендт Х. (2000). Vita Activa, или О деятельной жизни / пер. с нем. и англ. В.В. Бибихина; под ред. Д.М. Носова. СПб.: Алетейя. 437 с.

Василенко В.И., Василенко Л.А., Рухтин М.В. и др. (2010). Трансформационные процессы в системе допуска к государственной тайне России: монография / под общ. ред. А.А. Прохожева. М.: Проспект. 591 с.

Зотов В.В., Захаров В.М., Сапрыка В.А. (2021). Цифровизация публичного управления: электронная демократия vs электронное правительство // NOMOTHETIKA: Философия. Социология. Право. Т. 46, № 3. С. 250–262. DOI: https://doi.org/10.52575/2712-746X-2021-46-2-250-262

Каргаполова Е.В., Каргаполов С.В., Давыдова Ю.А., Дулина Н.В. (2020). Информационные компетенции молодежи в условиях цифровизации общества // Экономические и социальные перемены: факты, тенденции, прогноз. Т. 13, № 3. С. 193–210. https://doi.org/10.15838/esc.2020.3.69.13

Лихтин А.А. (2021). Трансформация государственного управления в условиях цифровизации // Управленческое консультирование. № 4. С. 18–26. https://doi.org/10.22394/1726-1139-2021-4-18-26

Моазед А., Джонсон Н. (2019). Платформа: практическое применение революционной бизнес-модели / пер. с англ. А. Соломиной. М.: Альпина Паблишер. 288 с.

Проказина Н.В. (2020). Цифровая грамотность населения как ресурс развития информационного общества // Информационное развитие России: состояние, тенденции и перспективы: Сборник статей X всероссийской научно-практической конференции. Орел, 6 декабря 2020 г. / под ред. Ю.В. Каиры. Орел: Среднерусский институт управления – филиал РАНХиГС. С. 77–83.

Саликов А.Н. (2018). Ханна Арендт, Юрген Хабермас и переосмысление публичной сферы в эпоху социальных медиа // Социологическое обозрение. Т. 17, № 4. С. 88–102. https://doi.org/10.17323/1728-192X-2018-4-88-102

Сморгунов Л.В. (2019). Партисипаторная государственная управляемость: платформы и сотрудничество // Власть. Т. 27, № 5. С. 9–19. https://doi.org/10.31171/vlast.v27i5.6712

Стырин Е.М., Дмитриева Н.Е. (2021). Государственные цифровые платформы: ключевые особенности и основные сценарии развития: доклад к XXII Апрельской международной научной конференции по проблемам развития экономики и общества. Москва, 13–30 апреля 2021 г. М.: Изд. дом Высшей школы экономики. 32 с.

Хабермас Ю. (2017). Структурное изменение публичной сферы: исследования относительно категории буржуазного общества / пер. с нем. В.В. Иванова. М.: Весь Мир. 342 с.

Шкудунова Ю.В. (2007). Концептуальная основа «публичности» и «приватности» // Вестник Омского университета. № 4 (46). С. 65–68.

Gavison R.E. (1980). Privacy and the limits of law // The Yale Law Journal. V. 89, no. 3. Pp. 421–471. https://doi.org/10.2307/795891

Gavison R.E. (1992). Feminism and the public-private distinction // Stanford Law Review. V. 45, no. 1. Pp. 1–45. https://doi.org/10.2307/1228984

Kymlicka W. (2001). Contemporary political philosophy: an introduction. 2nd ed. New York: Oxford University Press, 2001. 512 p.

Vasilenko L.A. (2021). Public policy in digital society // KnE Social Sciences: XXIII International Conference Culture, Personality, Society in the Conditions of Digitalization: Methodology and Experience of Empirical Research Conference. V. 5, no. 2. Pp. 585–593. https://doi.org/10.18502/kss.v5i2.8404

REFERENCES

Arendt H. (2000), *Vita Activa oder Vom tätigen Leben* [*Vita Activa, or About active life*], translated from German and English by V.V. Bibikhin, Aleteya, St. Petersburg, Russia. (In Russian).

Gavison R. (1980), “Privacy and the limits of law”, *The Yale Law Journal*, vol. 89, no. 3, pp. 421–471. https://doi.org/10.2307/795891

Gavison R. (1992), “Feminism and the public-private distinction”, *Stanford Law Review*, vol. 45, no. 1, pp. 1–45.

Habermas J. (2017), *The structural transformation of the public sphere: An inquiry into a category of bourgeois society*, translated from German by V.V. Ivanov, Ves` Mir, Moscow, Russia. (In Russian).

Kargapolova E.V., Kargapolov S.V., Davydova Yu.A. and Dulina N.V. (2020), “Information competences of young people within digitalization of society”, *Economic and Social Changes: Facts, Trends, Forecast*, vol. 13, no. 3, pp. 193–210. (In Russian). https://doi.org/10.15838/esc.2020.3.69.13

Kymlicka W. (2001), *Contemporary political philosophy: an introduction*, 2nd ed, Oxford University Press, New York, USA.

Likhtin A.A. (2021), “Transformation of public administration in the digital era”, *Administrative Consulting*, no. 4, pp. 18–26. (In Russian). https://doi.org/10.22394/1726-1139-2021-4-18-26

Moazed A. and Johnson N. (2019), *Platform: practical application of a revolutionary business model*, translated from English by A. Solomina, Al`pina Publisher, Moscow, Russia. (In Russian).

Prokazina N.V. (2020), Digital literacy of the population as a resource for the development of the information society, *Information Development of Russia: State, Trends and Prospects: Proceedings of the X All-Russian Scientific and Practical Conference. Orel, December 6, 2020*, edited by Yu.V. Kaira, Central Russian Institute of Management – a branch of the Russian Presidential Academy of National Economy and Public Administration, Orel, Russia, pp. 77–83. (In Russian).

Salikov A. (2018), “Hannah Arendt, Jurgen Habermas, and rethinking the public sphere in the age of social Media”, *Russian Sociological Review*, vol. 17, no. 4, p. 88–102. (In Russian). https://doi.org/10.17323/1728-192X-2018-4-88-102

Smorgunov L.V. (2019), “Participatory governability: platforms and collaboration”, *Vlast’*, vol. 27, no. 5, pp. 9–19. (In Russian). https://doi.org/10.31171/vlast.v27i5.6712

Shkudunova Yu.V. (2007), “Conceptual framework of “publicity” and “privacy”, *Herald of Omsk University*, no. 4, pp. 65–68. (In Russian).

Styrin E.M. and Dmitrieva N.E. (2021), *State Digital Platforms: Key Features and Main Development Scenarios: Report to the XXII April International Scientific Conference on Problems of Economic and Social Development. Moscow, April 13–30, 2021*, Publishing House of the Higher School of Economics, Moscow, Russia. (In Russian).

Vasilenko V.I., Vasilenko L.A., Rukhtin M.V. et al. (2010), *Transformation processes in the system of access to state secret of Russia: monograph*, edited by of A.A. Prokhozhev, Prospekt, Moscow, Russia. (In Russian).

Vasilenko L.A. (2021), Public policy in digital society, *KnE Social Sciences: XXIII International Conference Culture, Personality, Society in the Conditions of Digitalization: Methodology and Experience of Empirical Research Conference*, vol. 5, no. 2, pp. 585–593. https://doi.org/10.18502/kss.v5i2.8404

Zotov V.V., Zakharov V.M. and Sapryka V.M. (2021), "Digitalization of public administration: electronic democracy vs electronic government", *NOMOTHETIKA: Philosophy. Sociology. Law*, vol. 46, no. 3, pp. 250–262. (In Russian). DOI: https://doi.org/10.52575/2712-746X-2021-46-2-250-262

TRANSLATION OF FRONT REFERENCES

[1] BBC (2019), "Data on 540 million Facebook users exposed". Available at: https://www.bbc.com/news/technology-47812470 (accessed 12.06.2021).

[2] Filipenok A. and Skobelev V. (2021), "Roskomnadzor will start checking due to the data leak of Navalny's supporters", *RBC*. Available at: https://www.rbc.ru/politics/20/04/2021/607ecf5b9a7947353f644f54 (accessed 12.06.2021).

[3] Kaspersky Blog (2019), "The price of privacy on the Internet: are users willing to risk their personal data?". Available at: https://www.kaspersky.ru/blog/privacy-report-2019-summary/22730/ (accessed 12.06.2021).

[4] Kaspersky Lab (2020), "Kaspersky Lab survey: 64 % of Russians tried to delete information about themselves from websites or from social networks". Available at: https://www.kaspersky.ru/about/press-releases/2020_opros-laboratorii-kasperskogo-64-rossiyan-pitalis-udalyat-informatsiyu-o-sebe (accessed 12.06.2021).

[5] Ibid.

[6] Kaspersky Blog (2019), "The price of privacy on the Internet: are users willing to risk their personal data?". Available at: https://www.kaspersky.ru/blog/privacy-report-2019-summary/22730/ (accessed 12.06.2021).