■ ■ ■ Баланс приватного и публичного в использовании персональных данных в цифровом сетевом пространстве[1]

Зотов В.В.[1], Губанов А.В.[2]

1. Московский физико-технический институт (национальный исследовательский университет) (МФТИ), Москва, Российская Федерация.
2. Белгородский государственный национальный исследовательский университет (НИУ БелГУ), Белгород, Российская Федерация.

Аннотация. Актуальность исследования определяется необходимостью обеспечения всесторонней защиты личных данных граждан, поскольку их разглашение может вести к нанесению ущерба репутации, а возможно и к финансовом потерям из-за действий криминального характера. В этом контексте особый смысл приобретает анализ границ публичного и приватного в общественном сознании. В ходе проведённого массового и экспертного опроса по данной проблематике было установлено, что с неправомерным использованием конфиденциальных сведений в сети Интернет сталкивались практически 2/3 граждан. Но большинство экспертов и участников массового опроса осведомлены о том, что Интернет-сайты, социальные сети и поисковые системы могут собирать данные для веб-аналитики. Одновременно с этим большинство участников исследования считают возможной передачу персональных данных органам власти в обобщённом виде для принятия управленческих решений, а именно сведений о месте проживания, возрасте, семейном положении, образовании и половой принадлежности. Наиболее закрытыми для анализа стали сведения о покупках и тратах, геолокации и состоянии здоровья. Режим приватности в социальных сетях зависит от уровня публичности человека: для государственных служащих, членов партий и общественных объединений, представителей науки и образования он выше, чем для рядовых граждан (для них он зависит от знания о такой возможности настроек соцсетей). Большинство экспертов и рядовых граждан поддержали возможность введения запрета на раскрытие в сети Интернет и социальных сетях информацию о службе для военнослужащих и полицейских, при этом аналогичные меры считают недопустимыми для государственных служащих, муниципальных служащих, представителей бюджетной сферы и депутатов; только относительно судей мнение населения и экспертов не совпало: первые считают не допустимым введение запрета, а вторые – необходимым. Можно предположить, что цифровизация общества не обостряет проблему демаркации приватного и публичного. Однако ключевым инструментом разграничения личного и общественного в медиа-пространстве является создание специальной нормативно-правовой базы.

Ключевые слова: цифровое сетевое пространство, публичное управление, пространство публичных коммуникаций, приватная сфера, публичная сфера, персональные данные

[1] Исследование выполнено при финансовой поддержке РФФИ и АНО ЭИСИ в рамках научного проекта № 20-011-31535 «Публичное управление в цифровом обществе: к новому общественному договору».

Для цитирования: Зотов В.В., Губанов А.В. Баланс приватного и публичного в использовании персональных данных в цифровом сетевом пространстве // Коммуникология. 2021. Том 9. № 2. С. 15-30. DOI: 10.21453/2311-3065-2021-9-2-15-30.

Сведения об авторах: Зотов Виталий Владимирович – доктор социологических наук, профессор, профессор департамента философии Московского физико-технического института (МФТИ), старший научный сотрудник Белгородского государственного национального исследовательского университета (НИУ БелГУ); Губанов Александр Владимирович – кандидат социологических наук, Белгородский государственный национальный исследовательский университет (НИУ БелГУ). *Адрес:* 141701, Россия, Московская область, г. Долгопрудный, пер. Институтский, 9. *E-mail:* zotov.vv@mipt.ru; aleksandrgubanov1@mail.ru.

Статья поступила в редакцию: 01.03.2021. *Принята к печати:* 21.03.2021.

Цифровизация как угроза персональным данным

Цифровизация общества предусматривает организацию органами власти деятельности, которая призвана способствовать созданию условий для развития общества знаний, повышению благосостояния и качества жизни граждан, их степени информированности и цифровой грамотности, формированию информационно-коммуникационного пространства с учётом потребностей граждан и общества в получении качественных и достоверных сведений, развитию новой технологической основы информационной инфраструктуры для социальной и экономической сферы. Но проникновение цифровых технологий в жизнедеятельность человека несёт не только новые возможности оптимизации процессов взаимодействия, но и сопровождается появлением новых угроз безопасности, которые в случае их игнорирования могут свести на нет потенциальные выгоды внедрения данных технологий.

Важно учитывать то обстоятельство, что в связи с развитием информационно-коммуникационных процессов и новых технологий общественный запрос на получение актуальной информации все чаще удовлетворяется в сети Интернет. Всё больший объём социальной активности человека перемещается в сетевое пространство, где приобретает виртуальный характер, что в свою очередь приводит к оцифровке её параметров в качестве компонента «цифрового профиля» [Горбунов]. Социальное пространство, характеризуемое высокими темпами цифровизации, для человека, актора информационного взаимодействия, превращается в цифровую сетевую среду. Наряду с перспективами, открывающимися благодаря цифровым технологиям, перед людьми, государственными органами, гражданским обществом, возникают серьёзные проблемы. Цифровизация сопровождается увеличением объёма хранимой, передаваемой и обрабатываемой информации, что несёт угрозу защите конфиденциальных данных, в частности персональных данных пользователей. Одновременно с этим нарастает вмешательство в частную жизнь человека, злоупотребления данными о человеке со стороны государства, использование новых технологических возможностей с криминальными целями. Сюда включаются и несанкционированное проникновение в личные

гаджеты, и хищение приватной информации, и информационная агрессия, а также киберпреступность, информационная война и информационный терроризм.

Надо понимать, что увеличение числа кибрепреступлений является естественным следствием цифровизации. И хотя цифровизация находится лишь на начальном этапе, а киберпреступность уже превратилась в одну из ключевых проблем цифрового сетевого пространства. По данным МВД в 2020 году число преступлений, совершаемых с применением информационно-телекоммуникационных технологий, возросло на 73%, в том числе с использованием сети Интернет – на 91%, при помощи средств мобильной связи – на 88%[1]. На рост числа киберпреступлений повлиял переход сотрудников российских компаний на удалённую работу, который способствовал снижению бдительности, а также увеличение потребности в онлайн-покупках. Отметим, что по мнению некоторых авторов, утечка персональных данных граждан России в последняя время носит политический подтекст, поскольку со стороны стран Запада развёрнута широкомасштабная информационная война против России, представляющая реальную опасность для национальной безопасности страны [Воронина].

Сегодня можно наблюдать сохранение актуальности проблемы обеспечения всесторонней защиты персональных данных граждан, поскольку их разглашение может привести к нанесению значительного репутационного или финансового ущерба. При этом стоит отметить, что данный вопрос регулярно поднимается на законодательном уровне. Так, с марта 2021 года вступил в силу Федеральный закон от 30.12.2020 № 519-ФЗ об изменении правил обработки общедоступных персональных данных, согласно которому операторы больше не смогут использовать полученные сведения о гражданах в режиме «по умолчанию» и им потребуется получить согласие на каждое конкретное действие по обработке и публичному распространению.

В этом контексте особый смысл приобретает анализ границ публичного (то, что происходит во взаимодействиях с другими людьми) и приватного (то, что защищается от выдачи другим) использования персональной информации в общественном сознании. Приватность подразумевает не только право на защиту персональных данных о человеке от посторонних, но и право на личное пространство и его защиту. Сохранение приватности предполагает табуирование действий её нарушающих, а также устранение возможных посягательств на завоевание личного пространства [Шкудунова].

Методы исследования границ приватности и публичности персональных данных

С методологической точки зрения текущее исследование будет основано на интуитивно-рациональном методе [Babintsev, Sapryka], который отдаёт прио-

[1] См. официальный сайт Министерства внутренних дел Российской Федерации: https://мвд.рф/reports/item/22678184/.

ритет эмпирическим данным и их интерпретации. Методологической базой исследования послужили труды зарубежных и российских авторов, раскрывающие проблему информационной безопасности личности в социально-философском и социологическом плане [Дементьев; Диев; Кривоухов, Зотов]. Эмпирической основой стало социологическое исследование, проведённое с целью получения достоверной и обоснованной информации о границах приватности и публичности персональных данных в цифровом сетевом пространстве. Социологическое исследование включало массовый и экспертный опросы. В связи с эпидемиологической ситуацией массовый опрос проводился как анкетный опрос комбинированного типа: (1) онлайн-опрос с применением сервиса Google; (2) полевой опрос с использованием личных интервью с использованием бумажной анкеты. Генеральная совокупность исследования – это население старше 18 лет, проживающее в столичных мегаполисах и медианных по уровню информатизации регионах (Курская, Белгородская области, которые в рейтинге развития информационного общества занимают 26 и 22 место соответственно). Выборочная совокупность в количестве n = 1000 респондентов квотировалась по полу и возрасту (до 30 лет, от 30 до 60 лет, старше 60 лет). 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. Экспертный опрос проводился среди государственных служащих, представителей науки и образования, муниципальных служащих, членов общественных организаций и политических партий вышеуказанных медианных регионов. Всего было опрошено 90 экспертов.

Анализ границ приватности и публичности персональных данных в цифровом сетевом пространстве

В одной из публикаций приводят такой пример. По одной лишь фотографии человека, размешенной в Интернете, используя поисковые системы, страницы социальных сетей, блогов и форумов, можно найти всю необходимую информацию, которая позволяет идентифицировать человека и его близких родственников [Докучаев, Маклачкова, Статьев].

По мнению представителей экспертного сообщества, чаще всего граждане сталкиваются с неправомерным разглашением личного номера телефона, неправомерным использованием личных данных, онлайн-слежкой, а также кражей персональных данных. Подробное распределение представлено на Рисунке 1.

Оценка результатов массового опроса полностью подтвердила обозначенную экспертами тенденцию. Так, с неправомерным использованием в сети Интернет конфиденциальных сведений сталкивались практически 2/3 граждан (а именно 67%). Наиболее остро данная проблема стоит в столичных мегаполисах – 75%.

Среди наиболее актуальных проблем несанкционированного использования данных для каждого конкретного типа населённых пунктов стоит выделить:

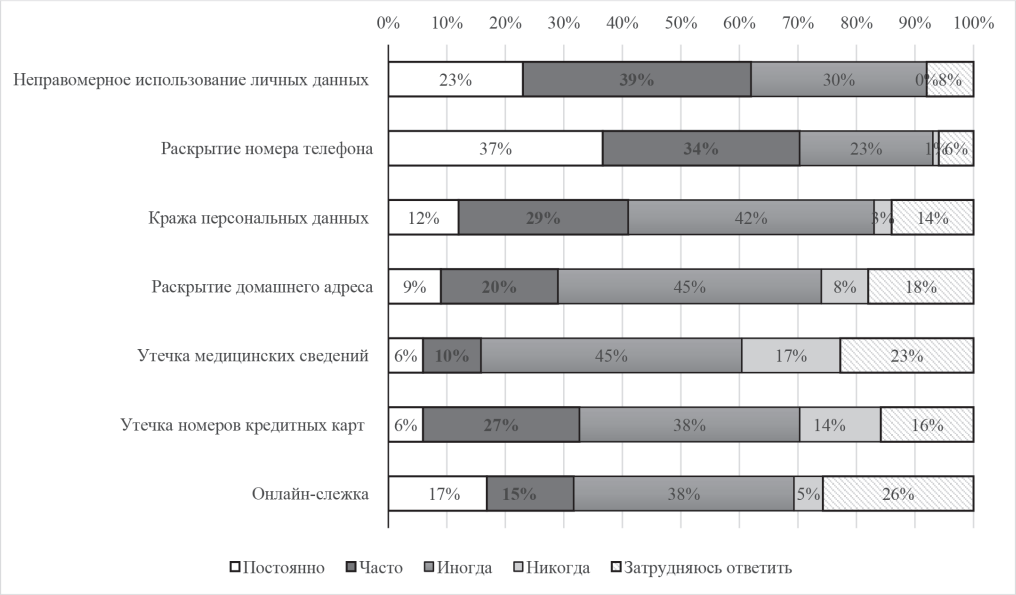

Рисунок 1. Распределение ответов экспертов на вопрос «На ваш взгляд, как часто население сталкивается со следующими ситуациями в сети Интернет?» / Distribution of experts' answers to the question «In your opinion, how often does the population encounter the following situations of identity fraud on Internet?»

Москва и Санкт-Петербург: кража персональных данных – 77%, раскрытие номера телефона – 73%, неправомерное использование личных данных – 60% и раскрытие домашнего адреса – 33%.

Областные центры: раскрытие номера телефона – 65%, неправомерное использование личных данных – 55%, кража персональных данных – 25% и онлайн-слежка – 24%.

Районные центры: раскрытие номера телефона – 59%, неправомерное использование личных данных – 55%, кража персональных данных – 42% и онлайн-слежка – 36%.

Сельские поселения: раскрытие номера телефона – 48%, неправомерное использование личных данных – 42%, кража персональных данных – 39% и онлайн-слежка – 35%.

Также стоит отметить, что чаще всего с проблемами хищения конфиденциальных данных сталкивались респонденты средней возрастной категории – 72%, в то время как среди молодёжи этот показатель составил 67%, пожилых респондентов – только 52%. Подробная информация о распределении представлена на Рисунке 2.

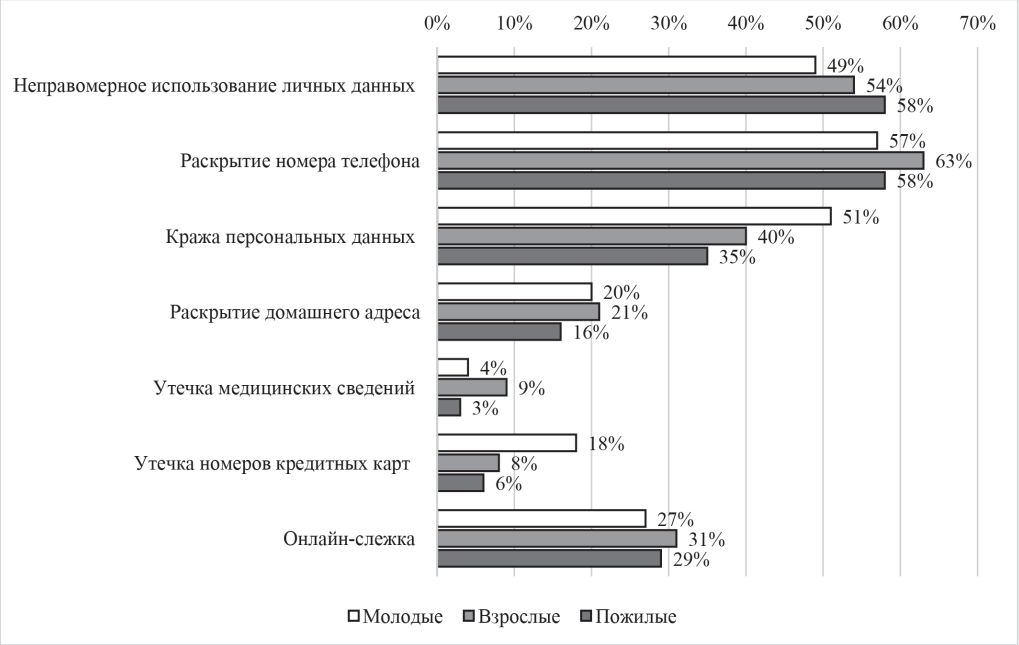

Рисунок 2. Возрастная структура респондентов массового опроса, которые сталкивались с проблемами хищения конфиденциальных данных в сети Интернет / Age structure of the respondents of the mass survey who faced the problems of theft of confidential data on the Internet

Таким образом, согласно полученным сведениям, наиболее остро для граждан стоят вопросы предотвращения разглашения номера телефона, неправомерного использования личных данных и кражи персональных данных. Решение проблем несанкционированное использования личных данных невозможно без активного нормативно-правого регулирования и административного участия органов власти. Особенно опасно, когда целью мошенников становятся пожилые граждане, средний уровень владения цифровой компетентности среди которых меньше, чем в остальных возрастных категориях. В частности, как минимум 6% процентов лиц пожилого возраста заявляли, что сталкивались с утечкой номеров кредитных карт.

Отметим, что уровень цифровой компетентности не высок даже в молодежной среде [Каргаполова, Каргаполов, Давыдова, Дулина], поэтому на практике эффективным решением проблемы также может стать более активное продвижение «уроков цифровой грамотности» для всех категорий и возрастов граждан. При этом вовсе не обязательно устраивать полноценные курсы, достаточно организовать общественное обсуждение вопроса и напомнить гражданам, что о вы-

сокой ценности персональных данных, необходимости их постоянной защиты, а также некоторых способах, для которых мошенники могут подобную информацию использовать. И здесь показателен опыт реализации программы повышения финансовой грамотности Центробанка, в рамках которой осуществляется формирование навыков распознавания мошеннических действий в отношении денежных средств граждан. Полезным может стать распространение коротких тематических видеороликов, рассказывающих о способах хищения личных данных граждан и простых механизмах защиты от этого. Выбор именно видео-формата обосновывается его высокой популярностью в настоящее время среди Интернет-пользователей, в том числе в социальных медиа.

К сожалению, чтобы столкнуться со сбором персональных данных в сетевом пространстве, вовсе не обязательно посещать «заражённые» шпионскими программами сайты или мошеннические ресурсы, достаточно просто выйти в Сеть и ввести запрос в любом популярном поисковом агрегаторе. Причём Интернет-пользователи далеко не всегда понимают, насколько опасным может быть подобное раскрытие конфиденциальности.

В настоящее время возникает проблема защиты пользовательских данных, (так называемых цифровых профилей), собираемой в сети устройствами и сервисами в течение продолжительного времени. Такие данные, хотя изначально и не являются персональными, в совокупности и при дополнительной обработке позволяют восстанавливать информацию о конечном пользователи. Наш опрос экспертов показывает, что большинство из них (46%) хорошо осведомлены о том, что Интернет-сайты, социальные сети и поисковые системы могут собирать данные для веб-аналитики; 37% заявили, что имеют об этом только общие представления и 9% ранее о данной возможности осведомлены не были. Еще 8% экспертов с ответом затруднились. Наиболее осведомлёнными о проблеме стали представители сферы науки и образования – 71%, муниципальные служащие – 55%, члены партий и общественных объединений – 54% и только четвертыми в этом списке оказались государственные служащие – 50%. Примечательно, что наибольший процент участников исследования, услышавших о проблеме впервые, был зарегистрирован среди муниципальных служащих – 10%. Подробное распределение представлено на Рисунке 3.

Большинство участников массового опроса – 46% – заявили, что хорошо осведомлены о возможности сбора сайтами систем веб-аналитики, еще 36% респондентов обладают только общей информацией. Ничего не слышали о подобном функционале только 8% граждан. Наибольший уровень осведомлённости был зафиксирован среди жителей столичных мегаполисов – 70%, значительно меньше в областных и районных центрах по 46%, в то время как в сельской местности указанный показатель не превысил 31%.

Несмотря на то, что основная часть Интернет-пользователей осведомлена о возможности сбора поисковыми системами и популярными сетевыми ресурсами персональных данных, все ещё остаются граждане, которые вовсе не имеют

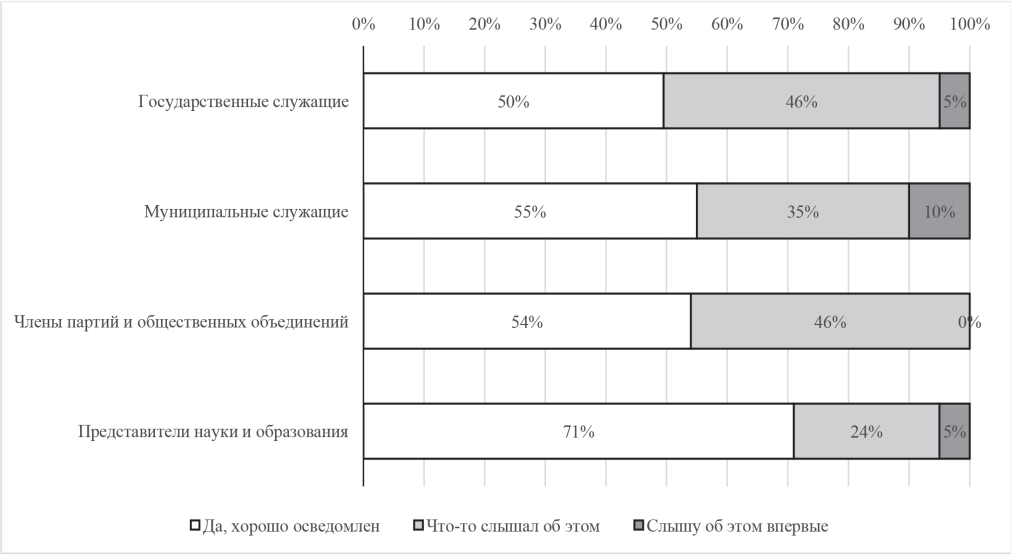

Рисунок 3. Распределение ответов экспертов на вопрос «Интернет-сайты, социальные сети, поисковые системы могут собирать данные для веб-аналитики. Скажите, пожалуйста, Вы знаете, что-то слышали об этом или слышите впервые?» / Distribution of experts' answers to the question «Internet sites, social networks, and search engines collect data for web analytics. Do you know, have heard anything about it, or do you hearing about it for the first time?»

никакой информации о данном вопросе. Но и знание проблемы не даёт никаких гарантий, что пользователю не придётся с ней столкнуться на практике. В связи с этим, на наш взгляд, актуальным представляется введение требования по обязательному и постоянному информированию граждан Интернет-сервисами о необходимости защиты личных данных и, при необходимости, выбора конкретного режима конфиденциальности.

Для чего поисковым системам и общедоступным Интернет-платформам персональные данные граждан? В качестве формальных целей как правило указывается оптимизация «умными алгоритмами» новостных и поисковых лент исходя из интересов сетевых пользователей. На практике подобная информация также используется для более эффективного показа контекстной и таргетированной рекламы. Чем больше пользователь «рассказывает» о себе системе, тем более точечная реклама ему может быть продемонстрирована. К сожалению, даже самые эффективные антивирусные системы и программы сетевой безопасности не могут гарантировать обеспечение 100% защиты конфиденциальных сведений граждан, в связи с этим, информация из поисковых сервисов также может попасть в руки мошенников.

Вопрос защиты персональных данных имеет двойственную природу, поскольку предполагает передачу сведений о гражданах как третьим лицам, так и органам власти. Мнение экспертов по данному вопросу не оказалось однозначным. Так, большинство участников исследования считают возможной переду государственным и муниципальным структурам сведения о: месте проживания – 51%, дате рождения – 56%, образовании – 57%, ФИО – 57% и гендере – 68%.

Запрет на сбор персональных данных для госструктур эксперты считают целесообразным по следующим категориям: должность – 56%, фотографии – 63%, музыкальные предпочтения – 63%, информация об имуществе – 75%, информация о зарплате и доходах – 76%, политических взглядах – 76%, информация о покупках и тратах – 77%, сведения о состоянии здоровья – 78%, данные геолокации – 79%, вероисповедание – 81%.

Не сложилось однозначного мнения у экспертов только в вопросе передачи государственным и муниципальным органам сведений о месте работе, e-mail и телефонах граждан: доля «за» и «против» в этих случаях приближается к 50%. Несмотря на однозначность ряда указанных выше позиций, стоит отметить, что распределение ответов экспертов оказалось неоднородным и находится в прямой зависимости от структур, которые они представляют. В частности, большинство респондентов из числа государственных и муниципальных служащих выразили полную готовность к передаче персональных данных по 7 позициям, члены политических партий и общественных объединений – только по 1 позиции, а представители науки и образования – по 4.

Среди причин подобного распределения, на наш взгляд, можно выделить большее доверие со стороны государственных и муниципальных служащих как к аппаратно-технической части и методам сбора и анализа персональных данных граждан, так и к самим операторам таких систем. В свою очередь общественники и представители научного сообщества не погружены в детали, которые позволили бы сформировать более доверительное отношение (см. таблица 1).

Исходя из этого, при осуществлении со стороны органов власти сбора и анализа персональных данных целесообразным выступает обеспечение максимальной прозрачности в применяемых методах, а также целесообразным выступает раскрытие целей аккумулирования подобной информации.

В вопросе передачи персональных данных органам власти в обобщенном виде для принятия управленческих решений граждане в ряде вопросов оказались более открытыми, чем эксперты, но основная часть сведений все еще остается достаточно закрытой. В частности, абсолютное большинство респондентов выразили готовность передать информацию о своём гендере – 71%, возрасте – 65%, образовании – 61% и семейном положении – 54%. Наиболее закрытыми для анализа стали сведения о покупках и тратах, геолокации и состоянии здоровья. Подробное распределение представлено в Таблице 2.

Таблица 1. Распределение ответов экспертов на вопрос «Согласны ли вы, что органы власти смогут собирать в сети Интернет следующие персональные данные граждан для анализа и принятия решений?» с распределением на представляемые сферы / Distribution of experts' answers to the question: «Do you agree that the authorities will be able to collect the following personal data of citizens on the Internet for analysis and decision-making?»

	Государственные служащие	**Муниципальные служащие**	**Члены политических партий и общ. объединений**	**Представители науки и образования**
1. Пол	86%	80%	54%	52%
2. Дата рождения	77%	55%	46%	43%
3. E-mail, телефон	59%	60%	27%	52%
4. Место проживания	55%	70%	31%	52%
5. Образование	64%	65%	46%	52%
6. Место работы	50%	60%	27%	43%
7. Должность	55%	50%	31%	33%
8. Фотографии	46%	35%	31%	29%
9. Данные геолокации	23%	25%	15%	10%
10. Информация о состоянии здоровья	27%	30%	15%	10%
11. Информация о зарплате, доходах	23%	35%	15%	14%
12. Информация об имуществе	23%	45%	15%	10%
13. Вероисповедание	23%	30%	8%	10%
14. Музыкальные предпочтения	41%	45%	27%	29%
15. Политические взгляды	27%	25%	19%	14%
16. Данные о покупках, тратах	23%	30%	12%	19%

Ежедневно социальные сети аккумулируют широкий комплекс персональных данных пользователей, от личных переписок до данных банковских карт. В связи с этим администрации большинства сетевых платформ предусмотрели возможность использования разных режимов приватности на выбор самого пользователя. Наибольшую открытость в этом вопросе продемонстрировали муниципальные служащие, члены политических партий и общественных объединений, 50% экспертов из числа которых сделали информацию из личных страниц доступной для всех участников сетевого сообщества, в то время, как госслужащие – 32%, а представители науки и образования – 29%.

Таблица 2. Распределение ответов участников массового исследования на вопрос «Согласны ли Вы предоставить органам власти следующие данные, размещённые в сети Интернет, для использования в обобщенном виде для принятия решений?» / Distribution the answers of the participants of the mass survey to the question: «Do you agree that the authorities will be able to collect the following personal data of citizens on the Internet for analysis and decision-making?»

	Да	**Нет**	**Затрудняюсь ответить**
1. Пол	71%	24%	5%
2. Возраст	65%	31%	4%
3. Семейное положение	53%	40%	7%
4. Место проживания	33%	60%	8%
5. Образование	61%	30%	8%
6. Место работы	33%	54%	13%
7. Должность	35%	51%	13%
8. Фотографии	18%	67%	15%
9. Данные геолокации	15%	72%	13%
10. Информация о состоянии здоровья	17%	71%	12%
11. Информация о зарплате, доходах	18%	73%	9%
12. Информация об имуществе	18%	73%	9%
13. Вероисповедание	40%	53%	8%
14. Музыкальные предпочтения	50%	42%	9%
15. Политические взгляды	31%	57%	12%
16. Данные о покупках, тратах	15%	74%	11%

Большинство государственных служащих выбрали режим приватности «доступна только друзьям» – 55%, среди муниципальных служащих данный показатель достиг 40%, членов партий и общественных объединений – 46%, представителей науки и образования – 57%. Доступной только избранным собственные аккаунты сделали 5% муниципальных служащих и 4% членов политических партий и общественных объединений.

Наивысший уровень приватности «не доступна никому» установили 9% государственных служащих и 5% представителей сферы науки и образования. Не пользуются социальными сетями: 5% экспертов из числа госслужащих, 5% муниципальных служащих и 10% сотрудников научных и образовательных организаций.

Непосредственно сами пользователи социальных медиа показали гораздо большую осторожность в обнародовании личных профилей в социальных медиа. Так, режим «доступна всем пользователям» установили только 34% молодёжи, 31% средней возрастной группы и 40% пожилых респондентов. При этом полностью недоступной информацию сделали 4% молодёжи, 3% средней группы и 2% пенсионеров. Подробное распределение результатов представлено на Рисунке 4.

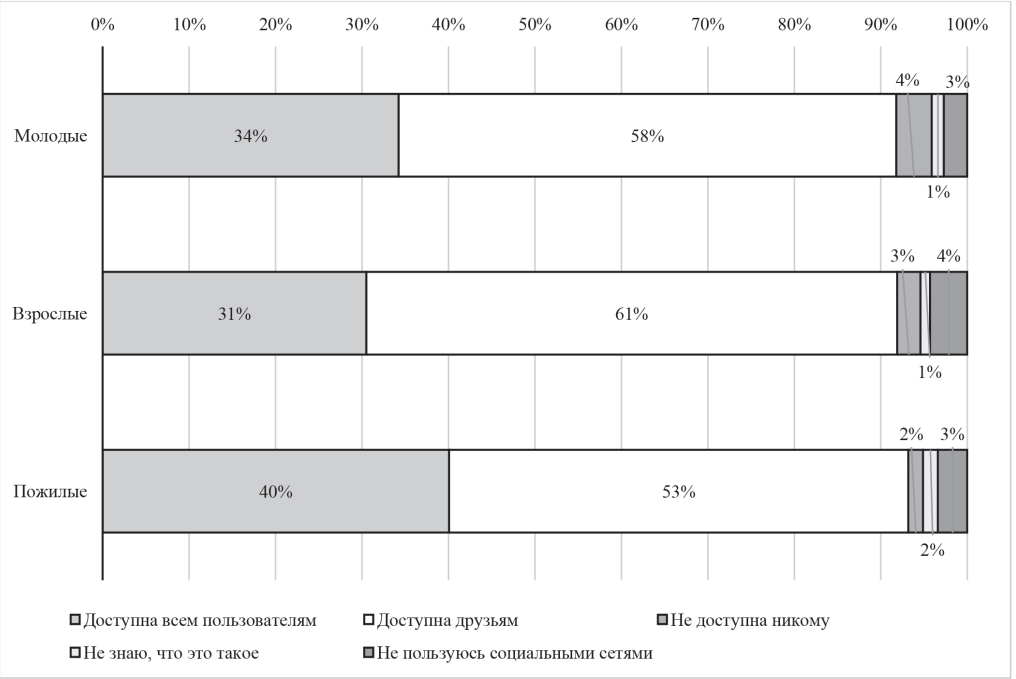

Рисунок 4. Возрастная структура распределения ответов респондентов на вопрос «Какую степень приватности Вы выбираете для своей страницы в социальных сетях?» /
Age structure of the distribution of respondents' answers to the question «What degree of privacy do you choose for your page on social networks?»

Вопрос приватности в социальных медиа напрямую связан со служебной и трудовой деятельностью, которую осуществляют граждане. Если блогеры, журналисты и депутаты, как правило, стремятся к максимальной публичности, то сотрудники правоохранительных органов личную информацию в открытом доступе размещают крайне редко. Большинство экспертов поддержали возможность введения запрета на раскрытие в сети Интернет и социальных сетях информацию о службе для военнослужащих (54%) и полицейских – 50%, при этом аналогичные меры считают недопустимыми для государственных служащих – 60%, муниципальных служащих – 55%, представителей бюджетной сферы – 49%, судей – 48% и депутатов – 58%.

Мнение участников массового опроса по ряду позиций оказалось сопоставимым. Так, большинство респондентов поддержали введение запрета на раскрытие служебной информации в социальных сетях для военнослужащих – 55%, сотрудников полиции – 53% и судей – 49%. Противоположное мнение большинство участников опроса высказали в отношении депутатов – 52%, работников

коммерческих организаций – 44%, сотрудников бюджетных организаций – 48% и муниципальных служащих – 45%.

Однозначное мнение не сформировалось только в отношении государственных служащих: 45% – против и 44% – «за».

Неоднозначным оказалось и распределение мнения экспертного сообщества по вопросу запрета на размещение в сети Интернет информации об имуществе высших должностных лиц государства. Подробное распределение представлено Таблице 3.

Таблица 3. Распределение ответов экспертов на вопрос «Как вы относитесь к инициативе запрета размещения информации об имуществе высших должностных лиц государства в сети Интернет?» / Distribution of experts' answers to the question «How do you feel about the initiative to ban the posting of information about the property of high-ranking government officials on the Internet?»

	Государственные служащие	**Муниципальные служащие**	**Члены политических партий и общ. объединений**	**Представители науки и образования**
Полностью одобряю	14%	20%	15%	19%
Скорее одобряю	23%	20%	15%	0%
Скорее не одобряю	41%	10%	23%	48%
Совершенно не одобряю	18%	45%	38%	24%
Мне все равно	5%	5%	8%	9%

Полностью одобряют данную меру только 17% экспертов; скорее одобряют, чем нет – 15%. Совершенно не одобряют – 31% экспертов, скорее не одобряют – 30%. Затруднились с ответом – 7%. Наибольшую лояльность к инициативе продемонстрировали муниципальные и государственные служащие – 40% и 37% соответственно, в то время, как 72% представителей сферы науки и образования и 61% членов политических партий и общественных объединений восприняли её отрицательно.

Ключевым инструментом разграничения личного и общественного в медиапространстве эксперты считают специальную нормативно-правовую базу. За её создание выступили 66% участников исследования, в то время, как против подобной меры высказались только 13%.

Поддержали необходимость дополнительного нормативно-правового регулирования и участники массового опроса, за эту меру высказались 48% респондентов, против – 19%. Стоит отметить, что наибольшую целесообразность в данной мере увидели граждане средней возрастной группы, а также жители населённых пунктов районного и сельского уровня. Подробное распределение.

Выводы. Таким образом, сегодня продолжает сохраняться актуальность проблемы обеспечения всесторонней защиты личных данных граждан, поскольку их разглашение может привести к нанесению значительного репутационного или финансового ущерба. В этом контексте в общественном сознании актуализирует вопрос границах публичного и приватного использования персональной информации. Проведённый массовый и экспертный опрос о границах приватности и публичности персональных данных в цифровом сетевом пространстве показал следующее:

– с неправомерным использованием в сети Интернет конфиденциальных сведений сталкивались практически 2/3 граждан, наиболее остро эта проблема стоит в столичных мегаполисах; экспертное мнение подтверждает правомерность данной проблемы;

– большинство экспертов и участников массового опроса осведомлены о том, что Интернет-сайты, социальные сети и поисковые системы могут собирать данные для веб-аналитики;

– одновременно с этим большинство участников исследования считают возможной переду персональных данных органам власти в обобщённом виде для принятия управленческих решений сведений о месте проживания, возрасте, семейном положении, образовании и половой принадлежности; наиболее закрытыми для анализа стали сведения о покупках и тратах, геолокации и состоянии здоровья;

– режим приватности в социальных сетях зависит от уровня публичности человека: для государственных служащих, членов партий и общественных объединений, представителей науки и образования он выше, чем для рядовых граждан; при этом в последнем случае много зависит от знания о возможности установления приватности информации для социальных сетей;

– большинство экспертов и рядовых граждан поддержали возможность введения запрета на раскрытие в сети Интернет и социальных сетях информацию о службе для военнослужащих и полицейских, при этом аналогичные меры считают недопустимыми для государственных служащих, муниципальных служащих, представителей бюджетной сферы и депутатов; только относительно судей мнение населения и экспертов не совпало: первые считают не допустимым, а вторые – возможным;

Ключевым инструментом разграничения личного и общественного в медиапространстве должна стать специальная нормативно-правовая база, за создание которой выступила 2/3 экспертов и почти половина граждан.

Источники

Воронина И.А. (2019). Обеспечение информационной безопасности в Российской Федерации: проблемы законодательного регулирования // Юридические науки, правовое государство и современное законодательство. Сборник статей VI Международной научно-практической конференции. Пенза: Наука и Просвещение. С. 123-129.

Горбунов А.С. (2018). Личность и цифровые технологии в информационном массовом обществе // Вестник Московского государственного областного университета. Серия: Философские науки. № 4. С. 8-16.

Дементьев С.А. (2017). Анализ информационной безопасности современного общества: от дисциплинарных методологических подходов к трансдисциплинарному // Общество и право. № 4 (62). С. 249-253.

Диев В.С. (2007). Некоторые концептуальные подходы к определению понятия «безопасность» // Вестник НГУ. Серия: Философия. Т. 5. № 1. С. 65-68.

Докучаев В.А., Маклачкова В.В., Статьев В.Ю. (2020). Цифровизация субъекта персональных данных // T-Comm: Телекоммуникации и транспорт. Том 14. №6. С. 27-32.

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. 2020. Т. 13. № 3. С. 193-210.

Кривоухов А.А., Зотов В.В. (2017). Информационная безопасность как антропосоциотехнический феномен // Коммуникология. Т.5. №4. С. 71-81.

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

Babintsev V.P., Sapryka, V.A. (2013). Opportunities of sociology in the time of troubles // World Applied Sciences Journal, Vol. 26. Issue 12. P. 1535-1537.

■ ■ ■ Balance of Private and Public in the Use of Personal Data in the Digital Network Space[1]

Zotov V.V.[1], Gubanov A.V.[2]

1. Moscow Institute of Physics and Technology (National Research University), Moscow, Russia.
2. Belgorod State National Research University, Belgorod, Russia.

Abstract. The relevance of the study is determined by the need to ensure the comprehensive protection of citizens' personal data, since their disclosure can lead to significant reputational or financial damage. In this context, the analysis of the boundaries of public and private in public consciousness takes on a special meaning. In a mass and expert survey conducted on this issue, it was found that almost 2/3 of citizens were faced with the misuse of confidential information on the Internet. But most experts and participants in the mass survey are aware that Internet sites, social networks and search engines can collect data for web analytics. At the same time, most participants in the study consider it possible to transmit personal data to the authorities in a generalized form for making managerial decisions about the place of residence, age, marital situation, education and gender; the most closed for analysis were information on purchases and spending, geolocation and health. The privacy regime in social networks depends on the level of publicity of a person: for state employees, members of parties and public associations, representatives of science and education, it is higher than for ordinary citizens (for them it depends on knowledge of such a possibility of setting social networks). Most experts and ordinary citizens supported the possibility of introducing a ban

[1] The reported study was funded by the Russian Foundation for Basic Research (RFBR) and the Expert Institute for Social Research (EISR) according to the research project № 20-011-31535 «Public governance in a digital society: towards a new social contract».

on the disclosure on the Internet and social networks of information about service for military and police personnel, while similar measures are considered unacceptable for government officials, municipal employees, representatives of the public sector and deputies; only regarding judges, the opinion of the population and experts did not coincide: the former consider not acceptable, and the latter – possible. It can be assumed that the digitalization of society does not aggravate the problem of demarcation of private and public. However, a key tool for distinguishing between personal and public in the media space is the creation of a special regulatory framework.

Keywords: digital network space, public governance, public communications space, private sphere, public sphere, personal data

For citation: Zotov V.V., Gubanov A.V. (2021). Balance of private and public in the use of personal data in the digital network space. *Communicology (Russia).* Vol. 9. No. 2. P. 15-30. DOI: 10.21453/2311-3065-2021-9-2-15-30.

Inf. about the authors: Zotov Vitaliy Vladimirovich – D.Sc.(Soc.), Prof., Professor at the Department of Philosophy, Moscow Institute of Physics and Technology (National Research University); Gubanov Alexander Vladimirovich – Cand.Sc.(Soc.), Belgorod State National Research University. *Address*: 141701, Russia, Moscow region, Dolgoprudny, Institutskii per., 9. *E-mail:* zotov.vv@mipt.ru; aleksandrgubanov1@mail.ru.

Received: 01.03.2021. *Accepted:* 21.03.2021.

References

Voronina I.A. (2019). Ensuring information security in the Russian Federation: problems of legislative regulation. In: Legal sciences, the legal state and modern legislation. Collection of articles of the VI International Scientific and Practical Conference. Penza: Science and Enlightenment. P. 123-129 (In Rus.).

Gorbunov A.S. (2018). Personality and digital technologies in the mass information society. *Bulletin of Moscow State Regional University. Series: Philosophical Sciences.* No. 4. P.8-16 (In Rus.).

Dementyev S.A. (2017). Analysis of information security of modern society: from disciplinary methodological approaches to transdisciplinary. *Society and law.* Vol. 4 (62). P.249-253 (In Rus.).

Diev V.S. (2007). Some conceptual approaches to the definition of «security». *NSU Bulletin. Series: Philosophy.* Vol. 5. No 1. P. 65-68 (In Rus.).

Dokuchaev V.A., Maklachkova V.V., Statev V.Yu. (2020) Digitalization of the personal data subject. *T-Comm*. Vol. 14. No.6, P. 27-32 (in Rus.).

Kargapolova E.V., Kargapolov S.V., Davydova Ju.A., Dulina N.V. (2020). Information competences of young people within digitalization of society. *Economic and Social Changes: Facts, Trends, Forecast.* Vol. 13. No 3. P. 193-210 (In Rus.).

Krivoukhov A.A., Zotov V.V. (2017). Information security as an anthroposociotechnical phenomenon. *Communicology.* Vol.5. No.4. P. 71-81. (In Rus.).

Shkudunova Yu. V. (2007) Conceptual framework of «publicity» and «privacy». *Herald of Omsk University,* Vol. 4. No 46. P. 65-68 (In Rus.).

Babintsev, V.P., Sapryka, V.A. (2013) Opportunities of sociology in the time of troubles. *World Applied Sciences Journal.* Vol. 26. Issue 12. P. 1535-1537.