

# ГРАЖДАНСКАЯ АКТИВНОСТЬ И ПРАВА ЧЕЛОВЕКА В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

DOI: 10.19181/vis.2022.13.3.832  
EDN: WVMOVV



## Приватность в сети и цифровая покорность: исследование аудитории интернета

**Ссылка для цитирования:** Назаров М. М. Приватность в сети и цифровая покорность: исследование аудитории интернета // Вестник Института социологии. 2022. Т. 13. № 3. С. 87–107. DOI: 10.19181/vis.2022.13.3.832; EDN: WVMOVV

**For citation:** Nazarov M. M. Online Privacy and Digital Submissiveness: A Study of the Internet Audience. *Vestnik instituta sotziologii*. 2022. Vol. 13. No. 3. P. 87–107. DOI: 10.19181/vis.2022.13.3.832; EDN: WVMOVV



### Назаров Михаил Михайлович<sup>1</sup>

<sup>1</sup>Институт социально-политических исследований ФНИСЦ РАН,  
Москва, Россия

vy175867@yandex.ru

AuthorID ПИНЦ: 74313

**Аннотация.** Технологическая природа интернета предопределяет прозрачность многих практик поведения в сети и актуализирует проблематику приватности в онлайн-среде. В работе приводятся результаты анализа отношения к онлайн-приватности в российском обществе. Эмпирическую основу составляют данные исследования, проведенного в Москве в 2021 г. Показано, что в практику российской аудитории интернета широко вошли действия, связанные с оставлением персональных данных в сети. Большинство респондентов (84%) разделяют представления о том, что доступ к их персональным данным, их обработка и использование должны осуществляться на основе согласия пользователей. Подобные установки сочетаются с низкой информированностью о сути использования персональных данных, а также с опытом их нелегитимного использования со стороны третьих лиц. По всей видимости, эти обстоятельства стали основанием того, что более 60% опрошенных указали на свою озабоченность вопросами безопасности в сфере онлайн-приватности. Приватность в цифровой среде испытывает влияние технологической эволюции медиа, с одной стороны, и политико-экономических и социокультурных факторов их использования – с другой. В этой связи на российской эмпирической базе были верифицированы известные в мировой литературе теоретико-прикладные концепции парадокса цифровой приватности и цифровой покорности. Выявлено противоречие между широким распространением обеспокоенности конфиденциальностью персональных данных и невысокими усилиями по обеспечению их защиты. В группе обеспокоенных безопасностью персональных данных 30% пользователей в своем реальном поведении онлайн не предпринимало никаких шагов в этом направлении. В рамках

исследования зафиксированы проявления феномена цифровой покорности, сопряженного с установкой на «неизбежность» принятия новых координат приватности, которые несет с собой мир интернета. Отсутствие действий по защите персональных данных (при общей обеспокоенности этим вопросом) оказывается сопряженными с неверием в защиту онлайн-приватности. В целом по массиву 40% респондентов были согласны с тем, что «слишком поздно защищать персональные данные, вся информация обо мне уже есть в интернете». С помощью регрессионного анализа определены индикаторы, коррелирующие с такими оценками. Результаты работы могут быть использованы при выработке оптимальных решений по обеспечению безопасности персональных данных – области, где на сегодня сталкиваются интересы личности, общества, бизнеса, государства.

**Ключевые слова:** приватность онлайн, персональные данные, интернет, частное и публичное, медиа, конфиденциальность, парадокс приватности, цифровая покорность

Жизнь современного человека трудно представить вне разнообразных практик в цифровой среде. Одной из особенностей коммуникационных технологий в интернете является широкое использование данных о пользователях. Это создаёт основу для функционирования множества удобных пользовательских сервисов. Вместе с тем объективно повышается значимость вопросов конфиденциальности персональных данных, обеспечения приватности в сети. История показывает, что представления о приватности так или иначе соотносятся с прогрессом коммуникативных технологий. Не является исключением и нынешняя ситуация. Наряду с высоким уровнем обеспокоенности людей вопросами безопасности персональных данных, мы наблюдаем и другой феномен – т. н. «цифровой покорности». Суть его состоит в том, что существенная часть аудитории считает неизбежным потерю приватности в сети. Результаты исследования интернет-практик аудитории в этой области обсуждаются в статье.

## Теоретико-методологические основания исследования

В самом общем плане приватность является близка по смыслу таким понятиям как право на частную жизнь, конфиденциальность. Сфера приватности предполагает автономию индивида, но не его изолированность. Здесь формируются и развиваются способности, вкусы, стиль жизни – уникальность индивида, создающая основу коллективных взаимодействий в публичной сфере [3, с. 343]. Показательной в этой связи является оценка З. Баумана: «Если полная свобода – скорее мысленный эксперимент, нежели практический опыт, то свобода в менее концентрированной форме практикуется под именем “приватности”. Приватность – это право предотвращать вторжение других людей (как индивидов или как агентов какой-то надындивидуальной инстанции) в конкретные места, в конкретные моменты или в конкретные занятия» [1, с. 99]. Согласно К. Фуксу, приватность правомерно также рассматривать как аспект безопасности [8, р. 8].

Исследование трансформаций, происходящих в области частного (и сопряжённой с ним области публичного), позволяет лучше понять направления долгосрочных социальных изменений в обществе. Это особенно актуально в связи с бурным развитием коммуникационных технологий и формированием всеобъемлющей цифровой среды. Здесь информационное взаимодействие индивидов, групп, институтов приобретает новые «измерения» в части приватности. Применительно к информационной приватности далее будем опираться на одно из наиболее распространённых определений, принадлежащих А. Вестину: «Приватность – это требование отдельных лиц, групп или учреждений самостоятельно определять, когда, как и в какой степени информация о них передается другим» [15, р. 7].

Современные концепции частного / публичного являются результатом осмысления норм и практик национального государства, политико-экономических прав, присущих капитализму и демократии. Представления об этом изменяются во времени. По мнению Ю. Хабермаса, в условиях раннебуржуазной эпохи частная жизнь «проживалась» как в профессиональной, так и семейной сфере. По мере развития капитализма профессиональная сфера становится некоторой «квази-публичной» областью, тогда как сфера частного «сжимается» до размеров семьи. Причём частная автономия всё в большей степени относится к области потребления и досуга [5, с. 223–225, 344]. Однако здесь за счёт роста пропагандистского влияния медиа область частного оказывается всё менее защищённой, по крайней мере, в эмоциональном плане [5, с. 229].

Ключевой технологический фактор, который привнёс новые изменения в проблематику приватности, связан с развитием интернет-среды и новейших медиа – социальных сетей, видеохостингов, поисковых систем, мессенджеров. Благодаря интерактивности и другим инновациям поведение в интернете становится всё более прозрачным, причём фиксируется это посредством т. н. персональных данных<sup>1</sup>. С одной стороны, речь идёт о персональных данных, которые конечные пользователи оставляют при регистрации на тех или иных сервисах. С другой – технологическая организация деятельности интернет-платформ такова, что здесь по определению происходит мониторинг или отслеживание поведения пользователя в сети при «рыхлом» согласии или практически без согласия с его стороны<sup>2</sup>. Именно в этой связи возникает область актуальной напряжённости по вопросу приватности в сети.

<sup>1</sup> Наше понимание персональных данных опирается на трактовку, содержащуюся в ведущем европейском документе в этой области – Общем регламенте защиты данных (GDPR – General Data Protection Regulation). Здесь персональные данные определяются как любая информация, касающаяся идентифицируемого физического лица. Последний может быть идентифицирован прямо или косвенно, в частности, посредством ссылки на такие идентификаторы, как имя, идентификационный номер, данные о местоположении, онлайн-новый идентификатор или на один или несколько факторов, характеризующих физические, физиологические, генетические, психические, экономические, культурные или социальные особенности личности. General Data Protection Regulation. GDPR. 2018. URL: <https://gdpr-info.eu/> (дата обращения: 04.12.2021).

<sup>2</sup> Это обусловлено тем, что цифровое устройство пользователя имеет т. н. IP-адрес, позволяющий идентифицировать компьютер, смартфон, смарт ТВ, игровую приставку; для этого используются уникальные идентификаторы – файлы Куки, трекинг-пиксели и прочие технологические решения для фиксации контактов с контентом и рекламой или с другими целями.

Одной из важных посылок нашей работы является представление о социальном характере приватности. Это понятие предполагает наличие «другого» субъекта, которому информация предоставляется или не предоставляется и который может иметь или не иметь одинаковых ожиданий от её раскрытия и сокрытия [14]. Причём в качестве такого субъекта могут выступать индивид, группа, организация. Структурирование приватной информации может быть обусловлено принятыми социальными нормами и связано зачастую с властными отношениями и вопросами социального контроля. Немаловажно и то, что доминирующая ныне либеральная концепция приватности делает исключительный акцент на индивидуальных правах. По справедливому замечанию критиков, в стороне остаётся вопрос о том, что эти ценности нарушаются посредством корпоративного мониторинга и надзора за пользователями [12, р. 158]. Причём возможности эти существенно возрастают в условиях всеобъемлющего распространения интернет-медиасреды.

В последние два десятилетия в мировой науке вопросы прикладного изучения приватности в онлайн-среде получили достаточно серьёзную разработку. Эта тема является междисциплинарной областью, которая привлекает внимание специалистов, занятых в сфере социологии, социальной психологии, исследований медиа-коммуникаций и других смежных дисциплин. Остановимся далее на результатах исследования т. н. парадокса приватности, имеющего непосредственное отношение к предмету нашего анализа.

В чём состоит содержание данного явления? Согласно эмпирическим исследованиям, далеко не всегда наблюдается положительная связь между субъективной важностью приватности и поведением индивидов в сети. Фактически, несмотря на высокую озабоченность вопросом приватности, реальное поведение пользователей в сети оказывается существенно более «мягким» или вовсе говорит об обратном. Ситуация, при которой фиксируется разрыв между отношением к приватности и фактическим поведением, получила название парадокса приватности. В работе С. Кюколакиса предложена одна из наиболее полных систематизаций исследований, посвящённых анализу «разрывов» между заявленным и фактическим поведением в отношении их персональных данных в сети интернет [13]. Объяснения этого группируются вокруг нескольких содержательных подходов.

Если рассматривать действия индивидов как экономических агентов, то ожидаемые потери конфиденциальности следует соотносить с потенциальными выгодами раскрытия. Фактическое поведение индивидов определяется компромиссом, в основе этого лежит рациональный расчёт. В опоре на социально-психологический ракурс анализа акцент делается, среди прочего, на т. н. эвристиках аффекта, поскольку индивиды склонны недооценивать риски конфиденциальности, связанные с вещами, которые им нравятся, например удобными интернет-сервисами. Разрыв в установках и поведении может быть обусловлен и тем, что преимущества раскрытия персональной информации воспринимаются как немедленные, а риски – как отложенные на будущее. Приватность в соци-

альных сетях также правомерно рассматривать в контексте дифференциации двух ключевых типов социальности по Ф. Тённису – общности (Gemeinschaft) и общества (Gesellschaft). Причём в социальных сетях как общностях участники объединены внутренними эмоциональными связями и неявными правилами, усиливающими чувства принадлежности. Одним из элементов этого является практика обмена информацией о себе с другими, что органично для таких общностей. При этом раскрытию персональной информации отдаётся приоритет над тем, что исходит от социальной сети как общества, – абстрактным предписанием типа политики конфиденциальности [13].

Заметим, что в отдельных исследованиях парадокс приватности ставится под сомнение в силу отсутствия достаточных эмпирических доказательств. Тем не менее конвенциональная точка зрения, особенно в цифровом бизнес-дискурсе, сводится к тому, что фактическое размывание приватности и минимизация регулирования в этой области являются императивом цифровой среды.

В последние годы в литературе наметился новый поворот этой темы. Всё больше исследований фиксируют, что, несмотря на желание людей контролировать свои персональные данные, их фактические возможности оказываются минимальными. Причём это происходит на фоне регулярно становящихся достоянием гласности фактов нарушений в этой области [10]. В результате настроения пользователей меняются.

В этой связи известный американский специалист в области социологии медиа Й. Туров и его коллеги выдвинули идею «цифровой покорности» [11; 7]. Представление о «цифровой покорности» (смирении, сдачи – digital resignation) предлагается в качестве альтернативы рассмотренному выше парадоксу приватности. С точки зрения авторов, согласие пользователей на раскрытие их персональных данных обусловлено не рациональной оценкой выгод и потерь при получении цифровых сервисов; или невысокой информированностью о негативных последствиях раскрытия данных, которые проявятся в будущем, тогда как дополнительные преимущества сервисов оказываются доступными «здесь и сейчас». Проведенные Туровым и его коллегами эмпирические исследования позволили сделать следующие выводы. Использование индивидами сервисов, предполагающих раскрытие их персональных данных (при том, что люди рассматривают это как нарушение их конфиденциальности), имеет другие основания. Покорность означает принятие чего-то нежелательного, но неизбежного, фактически речь идет о повиновении воле другого. Соответственно, поведение части пользователей отражает «цифровую покорность», форму некоторого смиренного цифрового прагматизма. С одной стороны, индивиды разделяют представления о том, что их частная жизнь находится под угрозой в цифровой среде; с другой – им свойственно осознание того, что избежать нарушения своей конфиденциальности в цифровой среде крайне сложно. Другими словами, люди не удовлетворены фактом роста мониторинга персональных данных со стороны компаний, но при этом убеждены в неизбежности «цифрового надзора». Именно такое понимание «цифровой покорности» далее используется в нашей работе.

Решающая роль в формировании и поддержании такой ситуации принадлежит ведущим технологическим компаниям интернет-бизнеса – Alphabet (Google), Meta (Facebook), Microsoft, Apple и другим. Для защиты сложившегося на сегодня статус-кво используются различные корпоративные технологии. Практики саморегулирования цифровой индустрии предполагают такие стратегии и тактики, которые формируют у пользователя ощущение, что использование персональных данных – это «нормально», а контроль за этим процессом ничего не даёт. Распространёнными в этой связи риторическими практиками являются неверное наименование, отвлечение, использование расплывчатой терминологии. Тексты политики приватности, в которых говорится об условиях конфиденциальности платформенных сервисов, обладают высокой лингвистической сложностью и зачастую неподъёмны для рядового пользователя [11].

Российские эмпирические исследования приватности в интернете были немногочисленными. В частности, проведён вторичный анализ данных в связи с задачами оценки экономических и правовых следствий приватности в условиях цифровизации [4]. Больше число академических публикаций имело социально-философскую направленность [6; 2].

## Центральные вопросы и эмпирическая основа исследования

В данной работе рассмотрены следующие исследовательские вопросы. Каковы практики поведения в сети в отношении раскрытия персональной информации и каков уровень обеспокоенности безопасностью данных в сети? Как на эмпирическом уровне соотносятся обеспокоенность защитой персональных данных, с одной стороны, и практики обеспечения приватности – с другой? Существуют ли проявления цифровой покорности, и если да, то какие обстоятельства способствуют этому явлению в наибольшей степени?

В ходе анализа использовалась система показателей и индикаторов, отражающих представления о приватности в онлайн-среде. К ним относились: практики поведения в сети, сопряжённые с раскрытием персональной информации; общая озабоченность приватностью в интернете; знание об использовании персональных данных интернет-компаниями; общее отношение к возможности обеспечения приватности в сети; представление о дилемме приватности в обмен на повышение качества сервисов; доверие к интернет-компаниям и организациям, использующим персональные данные пользователей; правовые регуляции, направленные на обеспечение приватности в сети. Отдельным показателям соответствовал набор эмпирических индикаторов, которые использовались в ходе полевого этапа исследования. Подробнее система показателей и эмпирических индикаторов приведена в таблице 1.

Таблица 1 (Table 1)

**Конфиденциальность персональных данных в онлайн-среде:  
показатели и индикаторы**

*Privacy of personal data in the online environment: readings and indicators*

Показатели сознания	Эмпирические индикаторы
Озабоченность обеспечением приватности в сети	Степень обеспокоенности пользователя безопасностью персональных данных – отслеживанием онлайн-поведения, несанкционированным доступом к данным, к содержанию общения в сети
Информированность об использовании приватных данных	Уровень знания пользователей о практиках использования их персональных данных интернет-компаниями
Доверие к государственным, общественным, бизнес-организациям, работающим с персональными данными пользователей	Уровень доверия к онлайн-субъектам, использующим пользовательские данные (к рекламодателям, магазинам интернет-торговли, поисковым системам, сервисам гос. организаций и др. – всего 11 индикаторов)
Установки пользователей об обеспечении безопасности персональных данных в интернете	Согласие / несогласие с оценочными суждениями о различных сторонах безопасности персональных данных в интернете: «Защита персональных данных предполагает, что информация о личной жизни и имуществе доступна другим только с согласия человека». «Защита персональных данных – это миф, с его помощью власти скрывают угрозу правам частной жизни и имуществу граждан». «Защита персональных данных теперь относительно. Это нормально, что в интернете проводится отслеживание и наблюдение за поведением. Данными о себе можно делиться и даже продавать».
Воспринимаемая онлайн-приватность	«При использовании интернета моя персональная информация становится доступна тем, кому бы я не хотел ее передавать». «Мне нечего скрывать от других, поэтому меня мало волнует вопрос о защите персональных данных в интернете». «Слишком поздно защищать мои персональные данные, вся информация обо мне уже есть в интернете»
Дилемма «безопасность данных в онлайн vs бесплатность и более качественный контент»	Два варианта предпочтения пользователя: риск для безопасности данных, но получение большего числа бесплатных и качественных сервисов, и наоборот
Регуляции сферы онлайн-приватности	Отношение к необходимости большего / меньшего законодательного регулирования в данной области
Показатели поведения	Эмпирические индикаторы
Фиксация персональных данных в сети	Приходилось ли пользователям оставлять информацию о себе в интернете (фio, возраст, паспортные данные и т. п. – всего 9 индикаторов)
Действия в связи с принятием «Политики конфиденциальности» онлайн-сервисов	Набор вариантов реакции пользователей: от поверхностного («соглашаюсь, практически не читаю») до внимательного («подробное чтение с последующим согласием»)
Защитные действия по защите конфиденциальности данных	Действия, предполагающие стирание файлов-куки, использование специальных программ
Опыт нелегитимного использования со стороны третьих лиц	Действия мошенников, использовавших персональные данные пользователя

Эмпирическая база работы – данные сравнительного исследования проблем приватности в интернете, проведённого в Москве в 2021 г.<sup>1</sup> Использовалась репрезентативная квотная выборка со связанными параметрами. Метод сбора информации – интернет-опрос. Общее число опрошенных  $N = 793$ . Полевой этап проходил в июне-июле 2021 г. Приведённые ниже результаты касаются респондентов, которые с различной периодичностью используют интернет, их доля составила 89% от общего массива. Исследование является продолжением проекта, начатого в Москве в мае-июне 2020 г. ( $N = 872$ ).

## Результаты исследования

### *Практики поведения в сети в отношении раскрытия персональной информации и отношение к безопасности персональных данных*

Широкое внедрение интернета и цифровых сервисов оказалось сопряжённым с тем, что действия пользователей прямо или косвенно предполагали оставление своих персональных данных в сети. Согласно результатам, подобные практики получили достаточно высокую распространённость (см. табл. 2).

Таблица 2 (Table 2)

**Распределение ответов на вопрос:**  
«Приходилось ли вам оставлять в интернете следующую информацию о себе?», %  
*Distribution of answers to the question:*  
“Have you ever left the following information about yourself on the Internet?”, in %

	Приходилось часто	Приходилось иногда	Не приходилось	Затруд. ответить
Фамилия, имя	61,2	34,3	3,2	1,3
Адрес проживания	26,4	58,5	12,9	2,2
Возраст	44,0	45,7	7,8	2,5
Семейное положение	15,5	43,3	38,2	3,0
Паспортные данные	13,6	56,7	25,5	4,2
Номер телефона	53,0	39,9	5,4	1,7
Место текущего расположения	25,3	41,9	28,6	4,2
Наличие детей	6,0	33,3	57,6	3,1
Уровень благосостояния	3,5	26,1	64,6	5,8

<sup>1</sup> Исследование проводилось Центром социологии религии и социокультурных процессов ИСПИ ФНИСЦ РАН.

Такие действия, как фиксация данных о своих фамилии и имени, домашнем адресе, возрасте, номере телефона, осуществляли часто или иногда более 85% опрошенных. Оставляли данные о своём семейном положении, а также данные геолокации – своего текущего положения порядка 60–70% респондентов. Наименее распространёнными были действия, связанные с оставлением в сети данных о наличии детей и своём благосостоянии, – об этом заявили 29% и 39% участников исследования соответственно. Характерно, что приведённые в таблице данные 2021 г. мало отличаются от аналогичных, зафиксированных нами в 2020 г.

Очевидно, тот факт, что пользователи часто фиксируют в интернет-среде разнообразную информацию о себе, соотносится с вопросами об информированности людей о последующем использовании этих данных, а также об их безопасности. В целом уровень информированности респондентов о том, как используются их персональные данные интернет-компаниями и организациями, является невысоким. Около половины опрошенных (47,6%) указали, что они знают об этом очень мало или ничего не знают. Другая значительная часть респондентов (48,6%) заявила о том, что они знают только о некоторых сторонах использования их персональных данных. Существенная меньшая часть участников исследования (13,5%) сообщила о том, что они хорошо знают, как используются их персональные данные. Затруднились ответить 3,8% респондентов.

В рамках исследования респондентам было предложено высказать своё отношение к различным по содержанию и оценочной направленности суждениям о безопасности персональных данных и практиках их защиты. Эти суждения в целом отражают основные «полюса» оценок предмета, присутствовавших в общественном дискурсе.

Выделим ряд важных моментов. Первый касается вопроса о приватности и персонального согласия. Подавляющее большинство опрошенных (84%) разделяли идею о том, что защита и, соответственно, доступ к персональным данным третьих лиц предполагает получение личного согласия пользователей. Второй момент относится к фактическому положению дел с вопросом о защите персональных данных на сегодня. Более половины респондентов (59%) считали, что при использовании интернета их персональные данные так или иначе оказываются доступны тем, кому они не предназначались. Причём 40% пользователей считали, что сейчас уже поздно защищать их персональные данные, поскольку они «уже есть» в сети.

Кроме того, существенная часть пользователей разделяет мнения, ставившие так или иначе под сомнение важность приватности в цифровой среде и необходимость защиты персональных данных. Так, около трети респондентов (28%) согласилось с тем, что в современных условиях защита персональных данных становится относительной. Они разделяют подходы, согласно которым отслеживание коммуникативного поведения в сети является нормальной технологической и бизнес-практикой. С этим корреспондирует мнение о том, что защита персональных данных

не является чем-то практически важным. По мнению 27% опрошенных, идея защиты персональных данных служит прикрытием желания властей минимизировать права граждан на неприкосновенность частной жизни. Наконец, 19% респондентов указали на их установку на полную открытость – отсутствие чего-либо, что стоит скрывать от других. Исходя из этого, вопрос защиты персональных данных в интернете является для них не слишком актуальным.

Технологически в интернет-среде реальной является ситуация отслеживания коммуникативного поведения – посещения тех или иных сайтов пользователями для обеспечения в последующем, например, таргетированной рекламы или иных бизнес-задач. Широкое распространение практики, когда люди оставляют в сети различные данные о себе, объективно уменьшает порог несанкционированного доступа к персональным данным. В ряде случаев эксперты также говорят о том, что более открытой оказывается и переписка пользователей в сети.

Можно предположить, что текущий пользовательский опыт соотносится с представлением респондентов о проблеме безопасности информации личного характера в интернете. Для выявления этого использовался индикатор уровня обеспокоенности безопасностью персональных данных в интернете. Большая часть опрошенных была обеспокоена проблемой безопасности персональных данных – в целом таковых оказалось 62,4%. Не были обеспокоены – 16,4%; заняли нейтральную позицию по этому вопросу или не дали ответа – 18,7% участников исследования. Результаты анализа показывают, что уровень обеспокоенности защитой персональных данных оказывается примерно равным в различных социально-демографических группах (пол, возраст, образование, доход). Значимых отличий здесь не выявлено.

Широкое распространение обеспокоенности защитой персональных данных может быть вызвано разными причинами. В частности, в ходе исследования 47% респондентов указали на то, что им приходилось сталкиваться с действиями мошенников, которые использовали их персональные данные. Показательно, что большая часть респондентов считала, что законы, регулирующие безопасность использования персональных данных, должны быть более жёсткими (66,2%). Предлагали оставить уровень регулирования без изменений – 14,0%, сделать более мягким – 2,8%, затруднились ответить – 17,0%. Ожидаемо, что большее предпочтение регуляциям отдавали респонденты, более обеспокоенные вопросом безопасности персональных данных, а также встречавшиеся с негативными практиками в этой области.

### *Обеспокоенность защитой персональных данных и практики обеспечения приватности*

Проявляют ли пользователи активность по обеспечению своей приватности в сети? Зафиксировано, что «старались использовать имеющиеся возможности для защиты информации о себе в интернете» 53,5% респондентов; не практиковали подобные действия – 32,7%; затрудни-

лись ответить – 13,7%. Учитывая это обстоятельство, подробнее был рассмотрен вопрос о том, как обеспокоенность приватностью в сети соотносится с практическими действиями по её защите.

Напомним, что в целом по массиву более половины аудитории (62,4%) беспокоил вопрос о безопасности персональных данных в сети. Причём отношение представителей этой группы к действиям по обеспечению приватности было различным. Большая часть респондентов в этой группе (69,9 %) старалась осуществить защитные действия. Вместе с тем около трети респондентов (30,1%) никаких действий в этом направлении на практике не предпринимали. Это свидетельствует об устойчивом и достаточно широком распространении феномена сознания и поведения людей – озабоченности безопасностью личных данных, с одной стороны, и отсутствии каких-либо действий в направлении её защиты – с другой. Наличие указанного сочетания признаков было также выявлено с помощью применения других методов анализа, в частности двухступенчатого кластерного анализа<sup>1</sup>.

Существуют ли содержательные особенности среди лиц, обеспокоенных безопасностью персональных данных и по-разному включённых в защиту этих данных? Для ответа на этот вопрос была создана специальная категориальная переменная, шкальные признаки которой отражают различные ориентации на защиту своей приватности в сети: обеспокоены приватностью и стараются защитить свои персональные данные; обеспокоены приватностью и имеют нейтральные установки по защите данных; обеспокоены приватностью и не стремящиеся к её защите? Затем для понимания содержательных особенностей различных ориентаций на защиту персональных данных в анализе были использованы переменные – оценочные суждения, отношение к которым отражает установки респондентов к различным сторонам онлайн-приватности и к её защите.

Поскольку шкалы изучаемых переменных были категориальными, то для анализа был применен однофакторный дисперсионный анализ Краскэла-Уоллиса. Была проведена проверка модели влияния группирующих переменных (отношения к оценочным суждениям о персональных данных в сети) на ориентации респондентов на защиту своей онлайн-приватности. Результаты анализа показаны в таблице 3. Здесь приведены данные о количестве респондентов, принадлежащих каждой из градаций группирующей переменной и средний ранг анализируемой переменной в каждой из групп. Также в таблице 3 содержатся результаты проверки статистической гипотезы о том, что средние ранги в каждой из сравниваемых групп равны между собой. Фактически эта гипотеза эквивалентна предположению об отсутствии влияния группирующей переменной на анализируемую переменную.

<sup>1</sup> В рамках последовательного построения классификаций – от 3-х до 6 кластерных решений.

Таблица 3 (Table 3)

**Проверка модели связи представлений о приватности в сети  
с активностью защиты персональных данных**

*(в группе обеспокоенных безопасностью персональных данных)*

*Checking the model of linking privacy perceptions in the network with the activity of  
protecting personal data (in the group concerned about the security of personal data)*

Группирующие переменные – отношение к оценочным суждениям		N	Средний ранг	Статистики теста	
«Защита персональных данных предполагает, что информация о личной жизни и имуществе доступна другим только с согласия человека»	Согласны	318	172,38	Хи-квадрат	0,335
	Нейтральны	9	186,67	Значимость	0,846
	Не согласны	18	177,08		
«Защита персональных данных – это миф, с его помощью власти скрывают угрозу правам частной жизни и имуществу граждан»	Согласны	135	164,94	Хи-квадрат	2,720
	Нейтральны	121	175,10	Значимость	0,257
	Не согласны	89	182,36		
«Защита персональных данных теперь относительна. Это нормально, что в интернете проводится отслеживание и наблюдение за поведением. Данными о себе можно делиться и даже продавать»	Согласны	100	165,19	Хи-квадрат	1,802
	Нейтральны	61	167,27	Значимость	0,406
	Не согласны	182	177,33		
«Мне приходилось сталкиваться с действиями мошенников, которые использовали мои персональные данные»	Согласны	183	173,16	Хи-квадрат	0,619
	Нейтральны	18	186,67	Значимость	0,734
	Не согласны	144	171,09		
«Слишком поздно защищать мои персональные данные, вся информация обо мне уже есть в интернете»	Согласны	132	150,23	Хи-квадрат	23,460
	Нейтральны	80	168,60	Значимость	0,000
	Не согласны	132	197,14		

Обращаясь к таблице 3, можно проследить характер этой зависимости. Здесь надо учитывать, что анализируемая переменная – ориентация на защиту персональных данных – имеет определённый порядок. Соответственно, средний ранг этой переменной был наиболее низким в группе тех, кто был согласен с оценочным суждением. Т.е. мнение о том, что «поздно защищать персональные данные», соотносится с низким уровнем практической активности по защите данных. И наоборот, для тех, кто не разделяет такое мнение, уровень ориентаций на защиту своих персональных данных является максимальным. Другими словами, неиспользование возможностей защиты своих персональных данных (при одновременной обеспокоенности обеспечением приватности в интернете) соотносится с представлением об особенностях организации интернет-пространства как такового. По всей видимости, прошлый опыт использования сети привёл респондентов к представлению о том, «вся информация обо мне уже есть в интернете».

С этим вопросом корреспондирует отношение пользователей к политике конфиденциальности интернет-ресурсов, которое также было изучено в ходе исследования. Как известно, при загрузке сайта или другого сервиса пользователю предлагается ознакомиться с т. н. «политикой конфиденциальности». Это происходит в полуавтоматическом режиме. Причём без «нажатия» – клика на соответствующий индикатор, свидетельствующий об ознакомлении с политикой, пользователь не может продолжить работать с сервисом. Считается, что таким образом интернет-компании информируют пользователей об особенностях использования персональных данных и сопряжённых вопросах.

Какими на практике являются действия пользователей, когда им предлагается познакомиться с политикой конфиденциальности? Согласно исследованию, половина (50,4%) респондентов не читает раздел о политике конфиденциальности; 8,2% не знают о существовании этого раздела. Около четверти респондентов (24%) заявили, что хотя и имеют желание быть информированными о политике конфиденциальности, но на практике это сделать сложно. Показательно, что среди пользователей, обеспокоенных приватностью в сети, доля подробно читающих политику конфиденциальности оказывается сопоставимой с долей тех, кто этого не делает (66,7% против 60,5%).

### *Цифровая покорность и её детерминанты*

На предыдущих этапах анализа было зафиксировано, что порядка 40% респондентов разделяют пессимистические представления о возможностях обеспечения эффективной безопасности приватности в интернете. Респонденты считали, что слишком поздно защищать их персональные данные, поскольку вся информация о них уже имеется в сети. Более того, эти настроения корреспондировали с отсутствием практических действий пользователей по защите своих персональных данных. Т. е. люди были вынуждены мириться со сложившимся положением дел, «покорно» принимая новые координаты приватности в цифровой среде. Следующий шаг анализа состоял в определении того, какие переменные способствуют максимальной выраженности этого явления?

В этой связи данные были проанализированы с помощью бинарной логистической регрессии. Цель использования этого статистического метода состояла в определении тех независимых переменных, которые повышают вероятность того, что респонденты разделяли скептические настроения относительно защиты их персональных данных в сети (зависимая переменная). В качестве независимых переменных или предикторов использовались все индикаторы, отражающие особенности сознания и поведения пользователей в предметной области.

Таблица 4 (Table 4)

**Регрессионная модель – предикторы пессимистических представлений о возможности защиты персональных данных в сети («Слишком поздно защищать мои персональные данные, вся информация обо мне уже есть в интернете»)**  
*Regression model – predictors of pessimistic ideas about the possibility of protecting personal data on the network (“It’s too late to protect my personal data, all the information about me is already on the network”)*

	B	Exp (B)	Значимость
<i>Оставляют персональные данные в сети:</i>			
О своей фамилии, имени	1,557	4,744	0,001
О своем местоположении (геолокация)	0,740	2,096	0,000
Не знают о том, как их персональные данные используются интернет-компаниями и организациями	0,421	1,523	0,082
Обеспокоены безопасностью персональных данных в сети	-0,392	0,675	0,054
<i>Установки о безопасности персональных данных в интернете:</i>			
«Защита персональных данных – это миф, с его помощью власти скрывают угрозу правам частной жизни и имуществу граждан»	0,413	1,511	0,038
«Защита персональных данных теперь относительна. Это нормально, что в интернете проводится отслеживание и наблюдение за поведением»	0,566	1,762	0,007
Предпочитают риск безопасности в пользу качественного сервиса и бесплатного контента	0,448	1,566	0,100
Недоверие онлайн-субъектам, использующим персональные данные: социальные сети	0,600	1,822	0,002
Действия в отношении «Политики конфиденциальности» онлайн-порталов и сервисов: не читают	0,407	1,502	0,029
Осуществляют действия по защите своей приватности в сети	-0,503	0,605	0,008
Опыт нелегитимного использования данных со стороны третьих лиц	0,650	1,915	0,001
<i>Воспринимаемая приватность в сети:</i>			
«При использовании интернета моя персональная информация становится доступна тем, кому бы я не хотел ее передавать»	1,129	3,092	0,000
«Мне нечего скрывать от других, поэтому меня мало волнует вопрос о защите персональных данных в интернете»	1,075	2,930	0,000
<i>Обеспечение государством норм демократического общества:</i>			
Не согласны с тем, что обеспечивается безопасность граждан	0,651	1,918	0,007
Не согласны с тем, что соблюдаются права человека	-0,514	0,598	0,048
Социально-демографические характеристики: 14–29 лет	-0,719	0,487	0,009
Константа	-4,075	0,017	0,000
R-квадрат Нэйджелкерка	0,394		

Результаты логистической регрессии показаны в таблице 4. Из всего перечня анализируемых переменных приводятся только те предикторы, которые оказываются статистически значимыми. Статистическая значимость – это вероятность наступления или не наступления исследуемого события. Уровень  $p \leq 0,5$  фиксирует наличие связи между независимой переменной и предиктором (с вероятностью 95%). Для каждого предиктора приведён коэффициент В. Чем большим является значение В, тем больше вероятность влияния предиктора на зависимую переменную. Применялся пошаговый метод анализа влияния независимых переменных на зависимую переменную. Все переменные, включенные в анализ, были предварительно дихотомизированы.

Опираясь на полученные результаты, можно говорить о том, что существует несколько групп предикторов – переменных, влияющих на зависимую переменную, – принятие скептических представлений о возможности защиты персональных данных в интернете.

Остановимся сначала на двух группах переменных, оказывающих максимальное влияние на зависимую переменную. Первая относится к практикам оставления в сети информации о себе. Из всего перечня таких действий только два оказались статистически значимыми и имели высокую предсказательную силу – фиксация фамилии и имени, а также местоположения (сервисы геолокации). Особенно ярко это относится к индикатору фамилии и имени, поскольку у тех, кто оставляет такие данные в сети, пессимизм в части защиты персональных данных проявляется в 1,5 раза чаще, чем в среднем по массиву ( $B = 1,55$ ). Близкие к максимально высокому уровню влияния на зависимую переменную имеют отдельные характеристики воспринимаемой приватности в сети. Это относится к представлениям о том, что при использовании интернета персональная информация о пользователе попадает к тем, кому она не предназначена (предсказательная сила этого предиктора  $B = 1,12$ ). Также это относится к предпочитающим быть «прозрачными», поскольку им «нечего скрывать от других в сети» ( $B = 1,07$ ).

Вероятность принадлежности к группе скептически оценивающих возможности защиты приватности в сети возрастает среди респондентов, обладающих рядом других характеристик (рост в пределах 40–70%). Это относится как к характеристикам сознания, так и поведения, о которых говорится ниже.

Среди характеристик сознания можно выделить отсутствие у респондентов знаний о том, как используются персональные данные интернет-компаниями и организациями. Кроме того, важным предиктором является согласие с тезисами: о том, что под прикрытием защиты персональных данных происходит вмешательство в частную жизнь; о том, что приватность в сети является относительной. Вероятность принадлежности к группе скептически оценивающих возможности защиты цифровой приватности возрастает, если респонденты соглашались рисковать безопасностью персональных данных, но получать более качественный сервис и онлайн-контент. Здесь же выделяются такие

предикторы, как недоверие к социальным сетям в части приватности; отсутствие общей обеспокоенности безопасностью своих персональных данных в интернете.

Характеристики поведения, повышающие вероятность скептических представлений о возможностях защиты приватности, отражают следующие индикаторы. С одной стороны, это априорное согласие (без какого-либо знакомства с содержанием) с «политикой конфиденциальности» сайтов и сервисов; с другой – опыт незаконного использования своих персональных данных со стороны третьих лиц. Вероятность проявления скептических представлений также оказывается большей в группе респондентов, не предпринимающих каких-либо практических действий по защите своей приватности в сети.

Можно предположить, что вопрос о защите приватности является связанным с оценками респондентами того, как государство выполняет ключевые нормы демократического общества. Результаты показывают, что пессимизм в отношении защиты персональных данных на 65% более вероятным является среди тех, кто не считает, что государство обеспечивает безопасность своих граждан.

Также был изучен вопрос о влиянии социально-демографических показателей на зависимую переменную. Практически все составляющие индикаторов пола, возраста, образования, дохода имеют уровень значимости больше 0,5 и не влияют на зависимую переменную. Исключением является принадлежность к возрастной группе «14–29 лет». Среди респондентов, не принадлежащих к этой группе, скептицизм относительно возможности защиты персональных данных оказывается распространён с вероятностью на 70% большей, чем в среднем по массиву.

## Заключение

Результаты исследования показывают, что в практику российских интернет-пользователей широко вошли действия, связанные с оставлением своих персональных данных в сети. При этом большая часть пользователей имеют низкую информированность или вообще не знают о том, как их персональные данные используются интернет-компаниями. Анализ отношения пользователей к конфиденциальности в цифровой среде показал, что подавляющее большинство респондентов (84%) разделяет представления о том, что доступ к данным со стороны третьих лиц предполагает персональное согласие пользователей. Вместе с тем подобные установки в отношении онлайн-приватности далеко не всегда воплощаются на практике.

Значительная часть пользователей (59%) согласилась с суждением о том, что их персональные данные в сети попадают к тем, кому они не предназначались; 47% респондентов указали на то, что они сталкивались с действиями мошенников, которые использовали их персональные данные. По всей видимости, эти обстоятельства стали основанием того,

что более 60% опрошенных указали на свою озабоченность вопросами безопасности в сфере онлайн-приватности. Судя по имеющимся данным, проблемы безопасности персональных данных в равной мере касаются представителей различных социально-демографических групп аудитории – значимых отличий в этом вопросе не обнаружено.

Полученные результаты фиксируют имеющийся разрыв между обеспокоенностью приватностью в онлайн-среде, с одной стороны, и практическими усилиями пользователей, направленными на обеспечение безопасности в этой области, – с другой. В группе обеспокоенных безопасностью персональных данных 30% пользователей в своём реальном поведении онлайн не предпринимало никаких шагов в этом направлении. Это касается как использования специальных программных решений, так и отношения к «политике конфиденциальности» онлайн-площадок и сервисов. Судя по всему, здесь проявляется известный «парадокс приватности», зафиксированный ранее в зарубежных исследованиях.

Отсутствие действий по защите персональных данных (при общей обеспокоенности этим вопросом) оказывается сопряжённым с особым типом отношения к защите онлайн-приватности, условно говоря, пессимистического плана. Было зафиксировано влияние на указанный тип поведения представлений о том, что «слишком поздно защищать мои персональные данные, вся информация обо мне уже есть в интернете». Как представляется, здесь просматривается установка на то, что нет иного варианта, кроме как принять новые координаты приватности, которые несёт с собой мир интернета. Другими словами, в этом находит своё выражение одна из сторон феномена цифровой покорности, о котором говорилось при обсуждении теоретико-прикладных оснований нашего исследования.

Немаловажно, что скептическое отношение к возможностям защиты персональных данных в целом по массиву разделяет существенная доля пользователей – 40%. В этой связи с помощью бинарной логистической регрессии были определены переменные, повышающие вероятность согласия с данной установкой. К переменным с наибольшей предсказательной силой относятся: активное оставление данных о себе в сети; представление о том, что в интернете персональные данные попадают к тем, кому они не предназначались; ориентации на то, что в сети «мне нечего скрывать от других». Ряд других переменных – с меньшей предсказательной силой – также позволяет лучше охарактеризовать содержательные особенности группы, скептически настроенной в отношении безопасности персональных данных. К ним относятся: представления об относительности защиты данных в современных условиях; предпочтение более качественных и бесплатных сервисов за счёт риска безопасности данных; низкая информированность об использовании персональных данных третьими сторонами; отсутствие практических действий по защите онлайн приватности.

Зафиксированный в нашем исследовании высокий уровень обеспокоенности граждан вопросами безопасности персональных данных в интернете оказывается сопоставимым с аналогичными показа-

телями в других странах и регионах мира. В этой связи сошлёмся на данные международного сравнительного исследования пользователей по теме интернет-безопасности и доверия в сети, проведённого CIGI-Ipsos в 2019 г.<sup>1</sup> Согласно данным этого проекта, в целом были обеспокоены вопросами онлайн-приватности 62% пользователей в Италии, 68% в Германии, 73% в Великобритании, 78% в США. При этом наблюдается рост этого показателя во времени.

Очевидно, что вокруг темы приватности в интернете сталкиваются интересы общества, бизнеса, государства. И это тем более так, поскольку приватность является центральной гражданской ценностью. Наше исследование показало, что в обществе существует запрос на обеспечение безопасности данных и конфиденциальности в сети. Причём 66% пользователей считают, что законы в этой области должны быть более жёсткими.

Следует отметить, что во многих странах мира в последнее десятилетие наблюдается усиление активности государства и общества в части юридической защиты приватности граждан в интернете. основополагающий документ в этой области в ЕС был принят в 2018 г. Общий регламент защиты данных (GDPR – General Data Protection Regulation) является центральным звеном защиты конфиденциальности<sup>2</sup>. Среди основных моментов: согласие со стороны пользователей, наличие у них возможностей контроля; наличие «права быть забытым» в отношении их данных; ответственность компаний за несанкционированный доступ или потерю данных.

В нашей стране правовые основы регулирования в этой области заложены в Федеральном законе «О персональных данных», принятом в 2006 г. С ним соотносится Федеральный закон о едином регистре сведений о гражданах России, принятый в 2020 г. и вызвавший неоднозначные оценки. С одной стороны, закон создаёт рамки для использования цифровых платформ и больших данных для прогнозирования и администрирования процессов в том числе в сфере государственного управления; автоматизации услуг и сервисов для граждан<sup>3</sup>. Критики отмечают противоречия закона с конституционными нормами, обеспечивающими права и свободы граждан; закон несёт риски правового, технологического, управленческого и прочего плана, включая риски безопасности, как для граждан, так и для государства и общества в целом<sup>4,5</sup>. По всей видимости, необходимо дальнейшее совершенствование законодательной базы в этой области.

<sup>1</sup> The State of User Privacy and Trust Online. CIGI-Ipsos Global Survey on Internet Security and Trust. 2019. URL: <https://www.internetsociety.org/resources/doc/2019/the-state-of-user-privacy-and-trust-online/> (дата обращения: 18.01.2022).

<sup>2</sup> General Data Protection Regulation. GDPR. URL: <https://gdpr-info.eu/> (дата обращения: 14.01.2021).

<sup>3</sup> Что такое единый регистр сведений о населении и зачем он необходим. URL: <http://duma.gov.ru/news/48646/> (дата обращения: 18.01.2021).

<sup>4</sup> ЕФИР: легализация вмешательства в частную жизнь — самоликвидация демократии. URL: <https://rossaprimavera.ru/article/3d6b8204> (дата обращения: 12.01.2021).

<sup>5</sup> Нас разбудят в другой стране: завтра налоговая получит все сведения о вас и вашей семье. URL: <http://worldcrisis.ru/crisis/3614161> (дата обращения: 12.01.2021).

В целом, как представляется, задачи обеспечения приватности в онлайн-среде являются значимыми в широком социальном плане. Справедливой можно считать точку зрения, что погружение индивидов в среду автоматического отслеживания и сбора персональных данных несёт угрозу нарушения минимальной целостности личности. В этой среде у индивидов теряется возможность автономного выбора – т. е. пространство реализации их «самости». Быть «самим собой» означает быть рефлексивно вовлечённым в процесс своего развития. Это предполагает наличие у субъекта минимальной отграниченности – сферы приватного. Кроме того, социальная среда перестаёт формироваться на основе взаимных ожиданий людей, а становится предметом технологических манипуляций с данными. Это, в свою очередь, трансформирует индивидуальную свободу выбора, которая является основой представлений о конфиденциальности в целом [9, р. 182]. Таким образом, социальное управление инновациями в цифровой среде должно учитывать необходимость обеспечения приватности как одной из ключевых ценностей, связанных с правами и свободами граждан.

## Библиографический список

1. Бауман З. Свобода / Пер. с англ. Г. Дашевского. М.: Новое изд-во, 2021. 204 с.
2. Заякин А. М., Комаров С. В. Эффект медиации: бытие между публичностью и приватностью // Вестник Челябинского государственного университета. 2019. № 8 (430). Философские науки. Вып. 53. С. 35–43. DOI: 10.24411/1994-2796-2019-10806
3. Новая философская энциклопедия. М.: Мысль, 2010. Т. III. 692 с.
4. Орлов М. О., Шаткин М. А. Приватность в условиях цифровизации // Социологические исследования. 2019. № 4. С. 15–25. DOI: 10.31857/S013216250004583-4
5. Хабермас Ю. Структурное изменение публичной сферы: Исследования относительно категории буржуазного общества / Пер. с нем. В. В. Иванова. М.: Весь Мир, 2016. 344 с.
6. Чеснокова Л. В. Индивидуализированное общество как социокультурный фундамент приватности // Идеи и идеалы. 2019. Т. 11. № 3. Ч. 2. С. 375–379. DOI: 10.17212/2075-0862-2019-11.3.2-375-389
7. Bagger C. An organisational cultivation of digital resignation? Enterprise social media, privacy, and autonomy // Nordicom Review. 2021. Vol. 42. No. 4. P. 185–198. DOI: 10.2478/nor-2021-0049
8. Bauman Z. Privacy, Secrecy, Intimacy, Human Bonds, Utopia – and Other Collateral Casualties of Liquid Modernity // Modern Privacy. Shifting Boundaries, New Forms / Ed. by H. Blatterer, P. Johnson, M. R. Markus. London: Palgrave, 2010. P. 7–22.

9. Couldry N., Mejias U. *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating it for Capitalism*. Stanford, California: Stanford University Press, 2019. 323 p.
10. Draper N. From privacy pragmatist to privacy resigned: challenging narratives of rational choice in digital privacy debates // *Policy & Internet*. 2017. Vol. 9. No. 2. P. 232–251. DOI: 10.1002/POI3.1423333
11. Draper N., Turow J. The corporate cultivation of digital resignation // *New media & society*. 2019. Vol. 21. No. 8. P. 1824–1839. DOI: 10.1177/1461444819833331
12. Fuchs C. *Social Media. A Critical Introduction*. London: Sage, 2014. 293 p.
13. Kokolakis S. Privacy attitudes and privacy behaviour: a review of current research on the privacy paradox phenomenon // *Computers & Security*. 2017. Vol. 64. P. 122–134. DOI: 10.1016/j.cose.2015.07.002
14. Marx G. T. Privacy. *The Blackwell Encyclopedia of Sociology*. 2007. URL: <https://onlinelibrary.wiley.com/doi/book/10.1002/9781405165518> (дата обращения: 25.11.2021).
15. Westin A. F. *Privacy and Freedom*. New York: Atheneum, 1967. 487 p.

Получено редакцией: 24.03.22

---

#### СВЕДЕНИЯ ОБ АВТОРЕ

**НАЗАРОВ Михаил Михайлович**, доктор политических наук, главный научный сотрудник, Институт социально-политических исследований ФНИСЦ РАН

DOI: 10.19181/vis.2022.13.3.832

EDN: WVMOVV

## Online Privacy and Digital Submissiveness: A Study of the Internet Audience

*Mikhail M. Nazarov*

Institute of Socio-Political Research of FCTAS RAS, Moscow, Russia

E-mail: vy175867@yandex.ru

ORCID ID: 0000-0002-9099-981X

**For citation:** Nazarov M. M. Online Privacy and Digital Submissiveness: A Study of the Internet Audience. *Vestnik instituta sotziologii*. 2022. Vol. 13. No. 3. P. 87–107. DOI: 10.19181/vis.2022.13.3.832; EDN: WVMOVV

**Abstract.** The technological nature of the Internet predetermines the transparency of many practices of online behaviour and actualises the issue of privacy in the online environment. The article presents the results of an analysis of attitudes towards online privacy in Russian society. The empirical basis is provided by the data of the study conducted in Moscow in 2021. It is shown that the practice of the Russian Internet audience widely includes actions related to leaving personal data online. The majority of respondents (84%) share the view that access to their personal data, their processing and use should be based on the consent of users. Such attitudes are combined with low awareness of the essence of the personal data use, and of the experience of their illegitimate use by third parties. Apparently, these circumstances were the reason that more than 60% of respondents indicated their concerns about security issues in the field of online privacy. Privacy in the digital environment is influenced by the technological evolution of media, on the one hand, and political, economic and sociocultural factors of their use, on the other hand.

In this regard, on the Russian empirical basis, the theoretical and applied concepts of the paradox of digital privacy and digital obedience, known in the world literature, were verified. A contradiction is revealed between the widespread concern about the confidentiality of personal data and low efforts to ensure their protection. In the group concerned about the security of personal data, 30% of users did not take any steps in this direction in their real online behaviour. As part of the study, manifestations of the phenomenon of digital obedience, associated with the installation of the “inevitability” of accepting the new coordinates of privacy that the Internet world brings with it, were recorded. The lack of action to protect personal data (with a general concern about this issue) is associated with a lack of confidence in the protection of online privacy. Overall, 40% of respondents across the array agreed that “it’s too late to protect personal data, all information about me is already on the Internet”. With the help of regression analysis, indicators were identified that correlate with such assessments. The results of the work can be used in the development of optimal solutions to ensure the security of personal data – an area where the interests of the individual, society, business, and the state collide today.

**Keywords:** online privacy, personal data, internet, private and public, media, privacy, privacy paradox, digital obedience

## References

1. Bauman Z. Freedom. Transl. from Eng. by G. Dashevsky. Moscow, Novoye izdatel'stvo, 2021: 204 (in Russ.).
2. Zayakin A. M., Komarov S. V. Mediation effect: being between publicity and privacy. *Vestnik Chelyabinskogo gosudarstvennogo universiteta*, 2019: 8 (430). *Filosofskiye nauki*: 53: 35–43 (in Russ.). DOI: 10.24411/1994-2796-2019-10806
3. Novaya filosofskaya entsiklopediya [The New Philosophical Encyclopedia]. Vol. III. Moscow, Mysl, 2010: 692 (in Russ.).
4. Orlov M. O., Shatkin M. A. Privacy in the conditions of digitalization. *Sotsiologicheskie issledovaniya*, 2019: 4: 15–25 (in Russ.). DOI: 10.31857/S013216250004583-4
5. Habermas J. The Structural Transformations of the Public Sphere. Research on the category of bourgeois society. Transl. from Germ. by V. V. Ivanov. Moscow, Ves Mir, 2016: 344 (in Russ.).
6. Chesnokova L. V. Individualized society as a socio-cultural foundation of privacy. *Idey i idealy*, 2019: 11: 3: 2: 375–379 (in Russ.). DOI: 10.17212/2075-0862-2019-11.3.2-375-389
7. Bagger C. An organisational cultivation of digital resignation? Enterprise social media, privacy, and autonomy. *Nordicom Review*, 2021: 42: 4: 185–198. DOI: 10.2478/nor-2021-0049
8. Bauman Z. Privacy, Secrecy, Intimacy, Human Bonds, Utopia – and Other Collateral Casualties of Liquid Modernity. In *Modern Privacy. Shifting Boundaries, New Forms*. Ed. by H. Blatterer, P. Johnson, M. R. Markus. London, Palgrave, 2010: 7–22.
9. Couldry N., Mejias U. *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating it for Capitalism*. Stanford, California, Stanford University Press, 2019: 323.
10. Draper N. From privacy pragmatist to privacy resigned: challenging narratives of rational choice in digital privacy debates. *Policy & Internet*, 2017: 9: 2: 232–251. DOI: 10.1002/POI3.1423333
11. Draper N., Turow J. The corporate cultivation of digital resignation. *New media & society*, 2019: 21: 8: 1824–1839. DOI: 10.1177/1461444819833331
12. Fuchs C. *Social Media. A Critical Introduction*. London, Sage, 2014: 293.
13. Kokolakis S. Privacy attitudes and privacy behaviour: a review of current research on the privacy paradox phenomenon. *Computers & Security*, 2017: 64: 122–134. DOI: 10.1016/j.cose.2015.07.002
14. Marx G. T. Privacy. *The Blackwell Encyclopedia of Sociology*, 2007. Accessed 25.11.2021. URL: <https://onlinelibrary.wiley.com/doi/book/10.1002/9781405165518>
15. Westin A. F. *Privacy and Freedom*. New York, Atheneum, 1967: 487.

The article was submitted on: March 24, 2022

---

### INFORMATIONS ABOUT THE AUTHOR

**Mikhail M. Nazarov**, Doctor of Political Sciences, Chief Researcher,  
Institute of Socio-Political Research of FCTAS RAS