ВЕСТНИК РОССИЙСКОЙ АКАДЕМИИ НАУК, 2021, том 91, № 3, с. 257–264

ИЗ РАБОЧЕЙ ТЕТРАДИ ИССЛЕДОВАТЕЛЯ

КОНФИДЕНЦИАЛЬНОСТЬ В ЦИФРОВОЙ СРЕДЕ: УСТАНОВКИ НАСЕЛЕНИЯ

© 2021 г. М. М. Назаров[a],*, Е. А. Кублицкая[a],**

[a] Институт социально-политических исследований Федерального научно-исследовательского социологического центра Российской академии наук, Москва, Россия

**E-mail: vy175867@yandex.ru*

***E-mail: eakubl@yandex.ru*

Поступила в редакцию 18.09.2020 г.
После доработки 28.09.2020 г.
Принята к публикации 05.10.2020 г.

В работе приводятся результаты изучения отношения населения к конфиденциальности персональных данных в Интернете. Эмпирическим основанием статьи стал репрезентативный опрос населения Москвы, проведённый в мае–июне 2020 г. Зафиксировано, что практика представления личной информации при пользовании различными интернет-сервисами получила широкое распространение. В то же время две трети респондентов заявили об обеспокоенности безопасностью информации личного характера в сети Интернет. Согласно модели бинарной регрессии, наиболее сильные предикторы такого беспокойства соотносятся с наличием у респондентов доминирующих установок о конфиденциальности; практиками оставления информации о себе в сети (прежде всего о своих детях); негативными оценками обеспечения безопасности как нормы жизни демократического общества и общей неудовлетворённостью функционированием политической системы.

Ключевые слова: конфиденциальность, Интернет, социальные медиа, частное и публичное, защита персональных данных.

DOI: 10.31857/S0869587321020055

Тот факт, что использование цифровых технологий, массовое распространение интернет-сервисов кардинально влияет на многие стороны жизни общества, уже стал общим местом. При использовании Интернета людям приходится оставлять в сети разнообразные данные о себе, в том числе личного характера. Неслучайно поэтому в фокусе общественного внимания оказался вопрос конфиденциальности в цифровой среде. Очевидно, что эта проблема имеет актуальные социально-политические и культурные составляющие, значима с точки зрения социального управления.

Какова же распространённость практик, предполагающих фиксацию персональных данных при использовании различных интернет-сервисов? Каковы особенности отношения людей к конфиденциальности в сети? Какие факторы детерминируют уровень обеспокоенности людей проблемой безопасности личной информации? Эти вопросы станут предметом обсуждения в настоящей статье.

О ключевых понятиях и методологии исследования. Проблематика конфиденциальности носит междисциплинарный характер и имеет важное значение в таких сферах, как медицина, компьютерные науки, финансы и банковское дело, пра-

НАЗАРОВ Михаил Михайлович – главный научный сотрудник ИСПИ ФНИСЦ РАН. КУБЛИЦКАЯ Елена Александровна – руководитель Центра социологии религии и социокультурных процессов ИСПИ ФНИСЦ РАН.

вопримененение. Имея в виду широкий социальный контекст, термин “конфиденциальность” в мировом исследовательском дискурсе трактуется в качестве рядоположенного понятиям “защита приватности”, “право на частную жизнь”, “секретность”.

В рамках классических либеральных представлений идея конфиденциальности связана с концепциями индивидуализма, личных прав, права собственности и ограниченного регулирования социально-экономических процессов и жизни общества со стороны правительства. Немаловажное значение имеет различение общественной (публичной) и частной сфер. Первая охватывает область политики, общественных отношений и публичных дебатов, вторая соотносится с приватной, предполагающей неприкосновенность, отсутствие вмешательства, стороной жизни, которая касается семьи, религиозных и иных убеждений, личного пространства [1, p. 17–32].

Актуальность изучения проблематики конфиденциальности оказалась сопряжённой с широким развитием информационных процессов, повышением роли средств массовой информации в жизни общества. Одно из наиболее часто используемых определений конфиденциальности применительно к сфере социальной жизни было предложено в 1960-х годах А.Ф. Вестином: “Конфиденциальность – это требование отдельных лиц, групп или учреждений самостоятельно определять, когда, как и в какой степени информация о них передаётся другим” [2, p. 7]. Исследователи справедливо обращают внимание на тот факт, что конфиденциальность – социально обусловленное явление, в котором важное значение имеют психологические аспекты, связанные с частной жизнью людей. Кроме того, понимание конфиденциальности зависит от контекста той или иной культуры [3].

В связи с развитием Интернета изучение конфиденциальности получило новый импульс. В частности, была предложена концепция *управления коммуникационной конфиденциальностью* (communication privacy management) [4, p. 796–798]. Индивиды постоянно адаптируют уровень конфиденциальности и раскрытия информации в соответствии с условиями внешней и внутренней среды своего существования. Это объясняется необходимостью обеспечения открытости социума, с одной стороны, и сохранения права на частную жизнь и автономию субъекта – с другой. Считается, что управление конфиденциальностью строится на ряде базовых посылок. Так, люди обоснованно считают, что информация о них принадлежит им, равно как и право распоряжаться ею. Выстраивание границ вокруг частной информации обусловлено культурой, а также социальным и личностным контекстом. Когда индивид делится с другим информацией о себе, то другой становится владельцем этой информации с вытекающей из этого ответственностью по её защите. Раскрытие частной информации предполагает механизм координации, чтобы обе стороны одинаково относились к доступности её третьим сторонам. Если стороны по-разному относятся к доступности этой информации для других, то возникает неопределённость границ, чреватая вмешательством, нарушением неприкосновенности.

В последние два десятилетия в мировой науке проведено много прикладных исследований в этой области. Например, изучены факторы, влияющие на обеспокоенность вопросами конфиденциальности при использовании Интернета в целом и социальных сетей в частности [5, 6]. Проведён эмпирический анализ того, как социальные сети изменяют межличностные отношения вследствие общего сжатия частного пространства [7], а также связи между коммуникационной грамотностью и отношением к рекламному отслеживанию пользователей смартфонов [8].

Эмпирическое основание нашего исследования – данные репрезентативного опроса населения Москвы в возрасте 15 лет и старше (опрошено 872 человека), проведённого в мае–июне 2020 г. Применялась квотная выборка со связанными параметрами. Метод сбора информации – онлайн-опросник.

Для решения поставленных задач использовалось несколько групп эмпирических индикаторов. Первая группа – индикаторы коммуникативного поведения. Фиксировалась самооценка средней длительности использования двух ведущих на сегодня медиа – Интернета и телевидения, определялось, в каких случаях и как часто участникам исследования в своей повседневной практике приходилось оставлять в Интернете информацию личного характера. Измерения производились с помощью частотной шкалы (“приходилось часто”, “приходилось иногда”, “не приходилось”). Вторая группа эмпирических индикаторов касалась сферы сознания – представлений респондентов о конфиденциальности в современной цифровой среде. Использовались восемь оценочных суждений, интерпретирующих феномен конфиденциальности. Отношение к каждому суждению фиксировалось с помощью номинально-упорядоченной пятичленной шкалы с крайними позициями “1 – совсем не согласен”, “5 – полностью согласен”. Наряду с этим, применялись индикаторы, отражающие отношение людей к различным сторонам социально-политической действительности.

Предполагалось, что текущий пользовательский опыт в сети, социальные представления, а также понимание сути конфиденциальности так

Таблица 1. Распределение ответов на вопрос “Приходилось ли вам оставлять в интернете следующую информацию о себе?”, % от числа опрошенных

Индикаторы	Приходилось часто	Приходилось иногда	Не приходилось	Затрудняюсь ответить
Фамилия, имя	53	39	6	2
Номер телефона	42	43	14	1
Ваш возраст	33	51	13	2
Адрес проживания	23	54	21	2
Место вашего текущего расположения	17	44	36	3
Место работы/учёбы	16	51	30	3
Паспортные данные	14	54	30	2
Семейное положение	11	46	41	2
Социальные контакты	9	34	50	7
Интересы в области культуры и развлечений	8	34	57	1
Наличие детей (если есть)	7	35	56	2
Политические предпочтения	4	17	76	3
Данные о состоянии здоровья	4	30	64	2
Уровень благосостояния	3	24	70	3
Религиозные предпочтения	3	20	75	2

или иначе влияют на отношение людей к проблеме безопасности информации личного характера, выкладываемой в Интернете. С этой целью измерялся уровень обеспокоенности данной проблемой с помощью пятичленной шкалы с крайними позициями “1 – совсем не беспокоит”, “5 – сильно беспокоит”.

Эмпирические результаты. Согласно полученным данным, 93% населения Московского региона являются пользователями Интернета. При этом 67% опрошенных на период исследования пребывали в сети более двух часов в день. Активное использование Интернета сопряжено с оставлением в сети той или иной личной информации (табл. 1). Прежде всего это касается таких параметров личной идентификации, как: фамилия, имя; номер телефона; возраст; адрес проживания; паспортные данные; место работы/учёбы; информация о текущем местоположении. Более 60% респондентов указали, что они оставляли в сети данные о себе часто или иногда. Реже в Интернете фиксируются индивидуальные интересы, включая политические или религиозные взгляды, сведения о благосостоянии, состоянии здоровья. Это делали с различной степенью периодичности от 20 до 30% участников исследования.

Если люди оставляют информацию частного порядка в сети, возникает правомерный вопрос о её конфиденциальности. Как же интерпретируется это понятие в массовом сознании? Чтобы определить это, использовались восемь оценочных суждений, имеющих разный смысл. К полученным данным была применена процедура факторного анализа.

С помощью факторного анализа проводится группировка близких между собой (в статистическом плане) оценочных индикаторов в некоторые укрупнённые категории. Это позволяет сократить размерность описания анализируемого явления. Важный содержательный момент процедуры факторного анализа состоит в том, что она позволяет очертить смысловое пространство изучаемого феномена в массовом сознании. При этом каждый из выявляемых факторов характеризуется набором наиболее значимых в статистическом смысле оценочных суждений. Таким образом, факторы выявленной модели отражают в своей совокупности ключевые знаки некоторого условного языка, с помощью которого респонденты в пространстве оценочных переменных фиксируют своё отношение к конфиденциальности. Резуль-

Таблица 2. Факторная структура оценочных суждений о конфиденциальности

	Суждение/факторы	1	2	3
1	Конфиденциальность – это когда личная информация доступна только с ведома или согласия человека	0.746		
2	Конфиденциальность – это контроль над информацией о себе, своём имуществе, возможность самому решать, что доступно другим, а что нет	0.740		
3	Конфиденциальность – это когда другие люди и организации не могут получить доступ к информации о чужом имуществе или личной жизни	0.712		
4	Конфиденциальность – это возможность распространения и продажи информации о себе, участие в этом третьих лиц		0.696	
5	Конфиденциальность – это общие ссылки на безопасность, что всё защищено и под контролем		0.659	
6	Конфиденциальность – это нормально, когда в Интернете обеспечивается отслеживание, наблюдение, мониторинг		0.572	
7	Конфиденциальность – это угроза со стороны властей в отношении прав людей, их имущества и личной жизни			0.787
8	Конфиденциальность – это миф, конфиденциальности не существует			0.548

Примечание: В таблице приведены факторные нагрузки больше 0.5.

таты представлены в виде матрицы факторных нагрузок (табл. 2).

Использовался метод главных компонент с последующим варимакс-вращением. В результате было выделено три фактора, объясняющих 53.7% вариации исходных переменных. Результат теста KMO (0.761) говорит об общей пригодности структуры полученных данных для факторного анализа. Тест Бартлетта, проверяющий гипотезу о некоррелированности переменных, имеет показатель значимости менее 0.001. Это говорит о том, что применение факторного анализа к исследуемой выборочной совокупности правомерно. Ниже приведены содержательные характеристики каждого из факторов.

Фактор 1 – “конфиденциальность предполагает полный контроль личной информации со стороны индивида”. Здесь наибольшие факторные нагрузки получили переменные, которые отражают традиционные представления о конфиденциальности. Речь идёт об индивидуальном согласии на доступ к приватной информации, отсутствии возможности у третьих сторон – других индивидов или организаций – доступа к информации о личной жизни или имуществе граждан. Степень доступа к персональным данным есть сфера индивидуального решения каждого.

Фактор 2 – “конфиденциальность в цифровой среде становится относительной”. Высокие нагрузки по второму фактору (см. табл. 2) соотносятся с представлениями о конфиденциальности, которые были привнесены в общественный дискурс в связи с массовым распространением интернет-практик. Теперь конфиденциальность приобретает новые измерения. Это обусловлено прежде всего мониторингом действий пользователей со стороны разнообразных сервисов, а также возможностями получения доступа к сервисам более высокого уровня за счёт некоторого снижения уровня конфиденциальности.

Фактор 3 – “конфиденциальности не существует, зачастую, это прикрытие для вмешательства в личную жизнь”. Здесь высокие факторные нагрузки отмечены относительно двух переменных, которые отражают сомнение в наличии в современном мире конфиденциальности как таковой, с одной стороны, и опасения, что за обсуждением этой проблематики скрывается угроза нарушения властями прав личности – с другой.

Данные факторного анализа были преобразованы путём регрессии в три новые переменные. Важно, что эти комплексные переменные позволяют охарактеризовать обобщённые установки респондентов относительно конфиденциальности в цифровой среде. Первая переменная отражает оценки, согласно которым “конфиденциальность – это контроль людей за своими данными”. Вторая переменная связана с представлениями, что сейчас “конфиденциальность – относительна”. Третья переменная соотносится с трактовкой: “конфиденциальность – это прикрытие вмешательства в личную жизнь”. Оговоримся, что описанная ста-

тистическая модель имеет ограничения, так как часть дисперсии признаков осталась нераспознанной. В рамках исследования также изучался вопрос о том, в какой мере респонденты озабочены проблемой безопасности личной информации, передаваемой в сеть. Большинство опрошенных проявили обеспокоенность (65%); указали на то, что этот вопрос их не беспокоит 16%; заняли нейтральную позицию – "отчасти беспокоит, отчасти нет" 19%.

Что же побуждает людей волноваться по поводу наличия сведений о них в Интернете? Для ответа на этот вопрос применялась бинарная логистическая регрессия. Цель анализа данных состояла в выявлении связи между независимыми переменными и зависимой переменной. Поскольку данный метод анализа имеет вероятностную природу, то независимые переменные также называются предикторами. Зависимая переменная характеризовала обеспокоенность респондентов проблемой безопасности личного характера в интернете. В качестве независимых использовались несколько групп переменных: социально-демографические характеристики; переменные, отражающие поведение в сети – в каких случаях люди оставляют (или нет) информацию о себе в интернете; комплексные переменные, фиксирующие то, как люди относятся к феномену конфиденциальности; переменные, характеризующие отношение к общему социально-политическому контексту (удовлетворённость обеспечением норм демократического общества), которые могут соотноситься с отношением к проблеме безопасности персональных данных.

В результате применения логистической регрессии было выявлено несколько значимых в статистическом плане независимых переменных, которые в наибольшей степени связаны с зависимой переменной – обеспокоенностью людей проблемой конфиденциальности личных данных. Расчёты показывают, что с вероятностью 95% можно утверждать, что приведённые ниже независимые переменные (предикторы) имеют связь с зависимой переменной.

Наибольшую предсказательную силу в модели имеют предикторы, связанные с комплексными переменными, характеризующими отношение к конфиденциальности. Те респонденты, для которых свойственны установки о том, что "конфиденциальность – это контроль людей за своими данными", в 5 раз чаще обеспокоены безопасностью информации личного характера, представленной в Интернете, чем другие опрошенные, а разделяющие утверждение, что "конфиденциальность – это прикрытие вмешательства в личную жизнь", – в 2 раза. Повышает обеспокоенность и факт передачи в сеть сведений о детях – в 1.46 раза. Существенной оказывается роль оценок текущего социально-политического контекста. Так, респонденты утверждающие, что государство не обеспечивает безопасность граждан как важную норму демократического общества, в 1.58 раза чаще озабочены сохранностью персональных данных, а считающие необходимым радикально изменить существующую политическую систему общества – в 1.42 раза.

Рассчитанная в ходе процедуры логистического анализа точность предсказания статистической модели – 69.8%. При этом обеспокоенность безопасностью информации личного характера в Интернете достоверно предсказывается в 78.2% случаев, отсутствие обеспокоенности – в 54.5%.

Конфиденциальность в цифровом мире: регулирование, социальные следствия. Проблемы конфиденциальности данных в современной цифровой среде носят глобальный характер. Показательно, что приведённые здесь результаты сопоставимы с оценками населения, зафиксированными за последние пять лет в других странах. Так, по данным репрезентативного опроса, проведённого в 2016 г. среди жителей ЕС, озабоченность сбором персональных данных в Интернете высказали 55% опрошенных [9]. Исследование 2015 г. среди населения Великобритании в возрасте 18 лет и старше показало, что вопрос конфиденциальности в онлайн-пространстве беспокоил 58% респондентов [10]. Согласно исследованию пользователей мобильных устройств в возрасте 18–65 лет в США в 2019 г. 60% из них озабочены этой проблемой [11].

Реагирует ли общество и если да, то как на проблему сохранности личных данных в Интернете? Обратим внимание на регулирующие практики, принятые в ЕС и США. Отметим, что принятие соответствующих законов было вызвано тем, что способы, с помощью которых доминирующие субъекты рынка собирали, накапливали и генерировали данные, были далеки от прозрачных. Зачастую пользователи оказывались в зависимом положении, причём порой отмечалось недобросовестное использование данных.

Основополагающий документ в этой области в ЕС был принят в 2018 г. Общий регламент защиты данных (GDPR – General Data Protection Regulation) стал центральным звеном сохранения конфиденциальности[1] [12]. Применительно к наше-

[1] В рамках GDPR 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, онлайновый идентификатор, или на один или несколько факторов, характеризующих физические, физиологические, генетические, психические, экономические, культурные или социальные особенности личности.

му обсуждению важно, каким статусом наделяет закон пользователя с точки зрения контроля персональных данных. Работа с личной информацией должна быть организованы таким образом, чтобы потребителям в подробной и доступной форме разъяснялось, как используются сведения о них. Должны быть предоставлены инструменты контроля за использованием персональных данных, получено согласие на предоставление и обработку данных. Признаётся "право быть забытым", то есть прекратить доступ к личным данным. Организациям рекомендуется использовать методы "псевдоанонимизации", позволяющие продолжить сбор и анализ персональных данных, с одной стороны, и обеспечивающих конфиденциальность клиентов – с другой. Организации несут ответственность за несанкционированный доступ к личным данным или их потерю.

Похожей логике следует Калифорнийский закон о защите прав потребителей от 2018 г. (The California Consumer Privacy Act of 2018), на который активно ссылаются при обсуждении регулирования использования персональных данных в США. Потребители наделяются правом знать, какую информацию о них собирала компания, её источники, цели использования, кому эта информация раскрывается или продаётся. Пользователь может отказать компании в разрешении продавать свою личную информацию третьим сторонам. Также у него есть право на удаление личной информации (за некоторыми исключениями) из баз данных бизнес-структур и право на получение равных услуг и цен даже при условии реализации права на неприкосновенность частной жизни [13].

В нашей стране правовые основы регулирования в рассматриваемой области закреплены Федеральным законом "О персональных данных", принятым в 2006 г. Позднее, в 2011 г., в закон были внесены поправки, расширяющие толкование понятия персональных данных. Здесь, как и в упомянутых выше зарубежных аналогах, присутствует норма о предоставлении индивиду подробных сведений о целях, механизмах и способах использования таких сведений. Вместе с тем в литературе высказывается точка зрения, согласно которой в условиях усложнения цифрового коммуникационного ландшафта и развития технологий добиться эффективного воплощение прав в отношении согласия на обработку персональных данных становится всё сложнее. Ставится вопрос о необходимости привести в соответствие реалиям цифровой эпохи сложившееся правовое понимание персональных данных [14]. Ещё более актуальной эта проблема стала в связи с принятием в июне 2020 г. ФЗ "О едином федеральном информационном регистре, содержащем сведения о населении Российской Федерации". Как известно, этот закон вызвал неоднозначные оценки представителей общественности, специалистов, законодателей. В пользу закона говорит то, что он позволяет властям более чётко прогнозировать развитие страны, оперативно администрировать самые разнообразные процессы. Несомненный плюс для граждан – автоматизация большого числа бюрократических процедур (например, получения и замены паспорта и др.), что экономит время [15].

В то же время, по мнению его критиков, закон вызывает ряд вопросов. Его положения находятся в противоречии с конституционными нормами, обеспечивающими права и свободы граждан, с нормами закона "О персональных данных", запрещающими сбор, хранение, использование и распространение информации о частной жизни лица без его согласия. В соответствии с законом о едином федеральном регистре предполагается, что хранение и передача персональных данных из регистра может происходить с привлечением широкого круга ведомств/организаций. Фактически к ним относятся представители так называемой третьей стороны (включая бизнес-структуры), находящиеся вне контроля граждан. В нынешнем его виде закон несёт риски правого, технологического, управленческого и прочего плана, включая риски безопасности как для граждан, так и для государства и общества в целом [16, 17]. По всей видимости, предстоит дальнейшее совершенствование законодательной базы в этой области посредством внесения необходимых дополнений и поправок.

Обсуждая результаты проведённого исследования, отметим, что интерпретация конфиденциальности трансформируется с течением времени. Очевидно, что ключевыми субъектами в разграничении публичной и частной сфер являются государство, бизнес и гражданское общество. По замечанию, известного британского социолога З. Баумана, «в течение большей части современной эры "нападение" на частно-государственную границу ожидалось именно со стороны различных учреждений... стремившихся взять под административный контроль или ограничить сферу индивидуальной или групповой свободы и, как следствие, лишив людей "убежища" в форме личной безопасности» [18, p. 9].

Вместе с тем по мере развития электронных СМИ и социальных сетей наблюдается другая тенденция. Предметом освещения в медиа становятся те стороны жизни, которые ранее носили частный характер. Неслучайно стали говорить о современном обществе как *обществе самораскрытия*, когда среда формирует ситуацию опосредованного присутствия. В этих условиях индивидам, как известным персонам, так и простым людям, легко создать некоторую интимную форму

самопрезентации, сделать видимым тот или иной аспект своей личной жизни [19].

Важное обстоятельство, влияющее на размывание границ частного и публичного, связано с экономическим императивом деятельности глобальных компаний – производителей товаров и услуг, равно как и обслуживающих их рекламно-коммуникационных групп. На основе интерактивной природы интернета генерируются огромные потоки данных о потребителях – об их поведении и интересах. Фактически сами пользователи являются поставщиками этих данных. Будучи соответствующим образом обработанными, данные приобретают высокую коммерческую ценность, поскольку без них невозможны целенаправленное продвижение и персонализация маркетинга. В контексте нашего обсуждения важно, что в значительной своей части сбор и обработка персональной информации происходят по умолчанию – согласие фиксируется самим фактом начала работы с тем или иным сервисом.

Однако, дело не только в собственно сборе данных. Ключевую роль в разработке персональных сервисов играют технологии *предиктивной аналитики*: на основе данных и профилей пользователей действуют разнообразные поисковые и рекомендательные сервисы. Причём максимальный учёт особенностей поведения и предпочтений индивидов невозможно отделить от параллельного формирования их потребностей. Фактически выбор и принятие решений прямо или косвенно оказываются под воздействием внешних технологий.

Таким образом, проблема конфиденциальности в интернет-пространстве более глубокая, чем это может показаться на первый взгляд. Персональные данные не являются исключительно технологическим или экономическим феноменом. Конфиденциальность и защита персональных данных относятся к базовым правам человека. Отдельные исследователи справедливо, на наш взгляд, утверждают, что погружение индивидов в среду автоматического отслеживания и сбора данных несёт угрозу нарушения минимальной целостности личности [20, p. 182]. Имеется в виду, что в этой ситуации индивиды утрачивают открытое пространство автономного выбора – пространство реализации их “самости”. Быть самим собой означает в том числе вовлечённость в процесс своего развития, что предполагает хотя бы минимальную обособленность субъекта, которая лежит в основе индивидуальности. В цифровую эпоху социальная среда перестаёт формироваться на основе взаимных ожиданий людей, становясь предметом технологических манипуляций с данными. Это в свою очередь трансформирует индивидуальную свободу выбора, которая составляет основу представлений о конфиденциальности.

ИСТОЧНИКИ ФИНАНСИРОВАНИЯ

Исследование выполнено в ИСПИ ФНИСЦ РАН в рамках Программы фундаментальных научных исследований государственных академий наук на 2013–2020 годы № 185 “Цивилизационные перемены в современной России: духовные процессы, ценности, идеалы” по государственному заданию НИР “Социокультурные и религиозные процессы в современной России”.

ЛИТЕРАТУРА

1. *Berg C.* The Classical Liberal Case for Privacy in a World of Surveillance and Technological Change. London: Palgrave Macmillan, 2018.
2. *Westin A.F.* Privacy and Freedom. New York: Atheneum, 1967.
3. *Altman I.* Privacy Regulation: Culturally Universal or Culturally Specific? // Journal of Social Issues. 1977. V. 33(3). P. 66–84.
4. *Petronio S.* Privacy Management Theory. Encyclopedia of Communication Theory / Littlejohn S., *Foss K.* (eds). London: Sage, 2009. P. 796–798.
5. *Dinev T., Hart P.* Internet privacy concerns and their antecedents – measurement validity and a regression model // Behaviour & Information Technology. 2004. V. 23 (6). P. 413–422.
6. *Tsay-Vogel M., Shanahan J., Signorielli N.* Social media cultivating perceptions of privacy: a 5-year analysis of privacy attitudes and self-disclosure behaviors among Facebook users // New media & society. 2018. V. 20(1). P. 141–161.
7. *Chambers D.* Networked intimacy: Algorithmic friendship and scalable sociality // European Journal of Communication . 2017. V. 32(1). P. 26–36.
8. *Ketelaar P.E., van Balen M.* The smartphone as your follower: The role of smartphone literacy in the relation between privacy concerns, attitude and behavior towards phone-embedded tracking // Computers in Human Behavior. 2018. V. 78. P. 174–182.
9. Online privacy and data protection in the European Union (EU). Statista. https://www.statista.com/study/38093/online-privacy-and-data-protection-in-the-european-union-eu-statista-dossier/
10. Online privacy in the United Kingdom (UK). Statista. https://www.statista.com/study/32598/online-privacy-in-the-united-kingdom-uk/
11. Online privacy in the United States. Statista. https://www.statista.com/study/17352/online-privacy-statista-dossier/
12. General Data Protection Regulation. GDPR. https://gdpr-info.eu/
13. The California Consumer Privacy Act of 2018. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375
14. *Шайдуллина В.К.* Большие данные и защита персональных данных: основные проблемы теории и практики правового регулирования // Общество:

политика, экономика, право. 2019. № 1 (66). С. 51–55.

15. Что такое единый регистр сведений о населении и зачем он необходим. http://duma.gov.ru/news/48646/
16. ЕФИР: легализация вмешательства в частную жизнь – самоликвидация демократии. https://ross-aprimavera.ru/article/3d6b8204
17. Нас разбудят в другой стране: завтра налоговая получит все сведения о вас и вашей семье. http://worldcrisis.ru/crisis/3614161
18. *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 Macmillan, 2010.
19. *Thompson J.B.* The New Visibility // Theory, Culture & Society. 2005. V. 22(6). P. 31–51.
20. *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.