РОССИЙСКАЯ АКАДЕМИЯ НАУК

ИНСТИТУТ НАУЧНОЙ ИНФОРМАЦИИ
ПО ОБЩЕСТВЕННЫМ НАУКАМ

НАУКОВЕДЧЕСКИЕ ИССЛЕДОВАНИЯ
2020

ЕЖЕГОДНИК

МОСКВА
2020

И.А. Асеева

ПРОБЛЕМА ПРИВАТНОСТИ В ЦИФРОВУЮ ЭПОХУ[1]

DOI: 10.31249/scis/2020.00.03

Аннотация. Будучи неотъемлемым правом гражданина демократического государства, право на неприкосновенность частной жизни в цифровую эпоху подвержено постоянным вторжениям и посягательствам. Частная жизнь становится объектом интереса общественности, государственных спецслужб, коммерческих организаций, криминала, получивших с помощью инфокоммуникационных технологий возможность не только присматривать за личностью через переписку и анализ персональных данных, но и манипулировать потребительским выбором, формировать спрос, отслеживать перемещения и контакты. Вместе с тем, как показывают результаты социологических исследований, само современное общество становится всё более открытым, а пользователи интернет-ресурсов, при отмечаемой значимости личной информации, часто добровольно выкладывают терабайты фотографий и видео, теряя границу между приватностью и публичностью, морально приемлемым и юридически запрещенным.

Abstract. Being an inalienable right of a citizen of a democratic state, the right to privacy of life in the digital age is exposed to constant intrusions and encroachments. Private life is becoming an object of interest for the public, state intelligence agencies, commercial organizations, and crime, who have received the opportunity through information and communication technologies not only to look after a person through correspondence and analysis of personal data, but also to ma-

[1] Статья подготовлена при поддержке гранта РНФ (проект № 19-18-00504).

nipulate consumer choice, generate demand, track movements and contacts. At the same time, as the results of sociological studies show, modern society itself is becoming more open, and users of Internet resources give the important personal information, often voluntarily post terabytes of photos and videos, losing the border between privacy and publicity, morally acceptable and legally prohibited.

Ключевые слова: приватность; конфиденциальность; цифровая эпоха; информационно-коммуникационные технологии.

Keywords: privacy; confidentiality; the digital age; information and communication technologies.

Социальный институт неприкосновенности частной жизни, зачатки которого можно наблюдать еще при общинно-родовом строе, в современном обществе приобретает важнейшее значение не только в смысле необходимости прояснения и уточнения его этических, юридических, экономических, психологических и иных границ, но и в смысле осознанности проницаемости и прозрачности этих рамок, вызванных фантастическими возможностями новых информационных технологий по сбору, анализу, корреляции, прогнозированию разнородной информации о человеке, его личности, образе жизни, личных связях и поступках. Актуальность и острота этой проблемы – проблемы приватности (от англ. private – частный) – связаны со многими аспектами: стремительным развитием инфо-коммуникативных цифровых технологий, дискуссионным правовым регулированием этой сферы, социальной напряженностью, возникающей в процессе трансформации традиционных способов жизнедеятельности и коммуникации между людьми.

С древнейших времен признание личностных прав является важнейшим признаком общества, регулируемого некими общепринятыми нормами. Уже во второй половине IX в. в славянском письменном законодательном памятнике «Закон судный людем» подробно расписываются санкции за «обиду», нанесенную чести и достоинству личности пострадавшего [7].

Формирование в юридической науке понятия права на приватность связывают с известной публикацией в 1890 г. статьи «Право быть оставленным в покое» американскими юристами Сэмюэлом Уорреном и Луи Брендайсом [37], в которой впервые был прописан принцип равной и полной защиты не только права собственности, но и личных прав. Вместе с тем авторы указывали

на границы реализации права, на сохранение тайны о личных делах. Так, сведения о человеке, открытые и переданные им добровольно, а также информация, отвечающая государственным или общественным интересам, не противоречат праву на неприкосновенность частной жизни.

В советский период российской истории трактовка личного и частного сильно зависела от идеологической конъюнктуры и ассоциировалась с неприемлемыми буржуазными ценностями. Поэтому в Конституции РСФСР 1918 г. приоритетным оказалось коллективное право в ущерб личному. Например, Н.А. Семашко, будучи народным комиссаром здравоохранения РСФСР, призывал отменить в советской медицине принцип сохранения врачебной тайны, мотивируя тем, что болезнь – это не позор, и у советского человека не должно быть секретов от товарищей, особенно в трудной жизненной ситуации. Впрочем, тема уважения приватности в медицине требует более подробного изучения и будет рассмотрена ниже.

Норма уважения личной жизни вернулась в Конституцию 1936 г., закрепив неприкосновенность личности, жилища и тайну переписки, отвергнув право частной собственности, не соответствующее идеологии социалистического государства [9].

После Второй мировой войны стала очевидной необходимость укрепления этой нормы в международном праве. Так, в 1948 г. во Всеобщей декларации прав человека, принятой резолюцией 217 А (III) Генеральной Ассамблеи ООН (статья 12), а в 1966 г. в Международном пакте о гражданских и политических правах (статья 17) было сформулировано: «Никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произвольным посягательствам на неприкосновенность его жилища, тайну его корреспонденции или на его честь и репутацию. Каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств» [4]. Под влиянием этих документов и в российских законах укрепляется тенденция в сторону признания и защиты прав и свобод человека и гражданина. В ныне действующей Конституции РФ 1993 г. государство выступает гарантом признания и защиты этих прав, в частности статья 23 гарантирует «право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени; тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения» [8]. Таким образом, и в тради-

ционных нормах общества, и в официальных государственных документах закреплено понятие «частная жизнь».

Содержание понятия «частная жизнь» всесторонне и подробно разработано в философии, юриспруденции, психологии и социологии. Так, М.В. Баглай отмечает, что частную жизнь «составляют те стороны личной жизни человека, которые он в силу своей свободы не желает делать достоянием других. Это своеобразный суверенитет личности, означающий неприкосновенность ее "среды обитания", исключая ситуации нарушения закона» [2, с. 219]. Частная жизнь человека выражается в его праве на автономию и свободу, праве на защиту от вторжения других людей и государственных институтов. При этом лишь сам человек или суд, действующий по законам правового, демократически организованного государства, могут разрешить такое вторжение [22, с. 119]. Приватность не раз отстаивалась в Европейском суде по правам человека, в частности в решении от 16 декабря 1992 г. по делу «Нимитц против Германии», в решении от 22 февраля 1994 г. по делу «Бургхарц против Швейцарии», в решении от 9 июня 2005 г. по делу «Фадеева против Российской Федерации» и др. Таким образом, было однозначно подтверждено право человека на установление и поддержание отношений с другими людьми, право на уважение неприкосновенности жилища, право на сохранение в тайне содержания личной корреспонденции и устных разговоров, в том числе и осуществленных с помощью электронных средств связи.

Современные технологические, информационные и социальные процессы, особенно бурно протекающие в актуальной ситуации растущей сложности и неопределенности, приводят к необходимости корректировки устоявшихся моделей поведения, форм коммуникации, юридического регулирования в различных социокультурных средах. Многие из этих процессов уже немыслимы без цифровых технологий [20]. Поэтому и проблема приватности приобретает новый ракурс – возможность и границы неприкосновенности частной жизни в цифровой реальности – интернет-приватность. Интернет-приватность С.А. Назаров определяет как «атрибут права на неприкосновенность частной жизни, общественные отношения, возникающие при реализации человеком его права на конфиденциальную переписку и общение через средства интернет-коммуникации и (или) его стремлении сохранить свое пребывание в сети Интернет тайным от посторонних глаз» [11, с. 132].

Информационно-сетевые технологии, модернизация коммуникационных гаджетов и программ, ситуация вынужденной дистанционной работы фактически переформатировали общество под цифровой порядок и добавили ранее неизвестные проблемы. Эти проблемы связаны не только с новыми качественными возможностями и сложностью отбора и систематизации информации, обучением в удаленном режиме, но и с появлением неоднозначных и еще не изученных психоментальных феноменов новой виртуальной и киберфизической реальности и необходимостью этического и правового отклика.

Уважение интернет-приватности (e-Privacy) предполагает, во-первых, реализацию прав личности на секретность частной коммуникации и анонимность пребывания в Сети, а во-вторых, моральный и юридический запрет нарушения конфиденциальности личной информации и использования ее в корыстных целях. Однако в реальности это совершенно не так. Крупные цифровые компании могут, например, отслеживать интересы граждан, использовать эту информацию в рекламных целях и в определенной мере манипулировать ею [28]. Amazon, например, анализирует данные о покупках 152 млн клиентов объемом около 1 эксабайта для построения прогнозов торговых потребностей [16]. М. Энзеринк и Дж. Чин в статье «Конец частной жизни» пишут о том, что с момента рождения и на протяжении всей жизни люди оставляют огромное количество электронных следов, обмениваются данными, делятся проблемами [30]. Поэтому все труднее сохранить в секрете личные данные человека, информацию о его здоровье, предпочтениях, финансовых возможностях и политических пристрастиях. Появляются технологии, способные распознать и установить личность человека по случайной фотографии, мелькнувшей в социальных сетях. Ян Ле Кун, руководитель исследований в сфере искусственного интеллекта, проводимых лабораторией Facebook (Нью-Йоркский университет), утверждает, что цель состоит не в том, чтобы вторгаться в частную жизнь более чем 1,3 млрд активных пользователей Facebook, а в том, чтобы защищать ее. Как только система Дипфейс (DeepFace) идентифицирует лицо на одной из 400 млн новых фотографий, ежедневно загружаемых пользователями, «вы получите сигнал тревоги от Face-book, сообщающий вам, что вы появились на снимке», – объясняет Ле Кун. После этого человек может стереть свое лицо со снимка, чтобы защитить свою частную жизнь [30].

Между тем проблема информационной безопасности связана не только с охраной личного архива человека, но и с выполнением государственных задач по защите граждан от терроризма и преступности. Разумеется, государственный подход в разных странах может существенно различаться в зависимости от идеологии и расстановки приоритетов. Так, в 2010 г. компания Google была вынуждена покинуть рынок КНР в связи с отказом заниматься дальнейшей цензурой поисковых запросов [26], а в 2015 г. Apple отказалась предоставить ФБР технические средства для взлома айфона террориста, совершившего теракт в Сан-Бернардино. Однако еще памятны прецеденты с выступлениями агента национальной безопасности США Эдварда Сноудена и Джулиана Ассанжа, основателя WikiLeaks.

Дисбаланс, возникающий при противопоставлении приватного и публичного, приводит к дополнительной социальной напряженности, росту киберпреступлений, нарушению права неприкосновенности частной жизни даже законопослушных граждан и ощущению постоянной слежки. Как заявил в своем выступлении на ежегодном форуме Всемирной встречи на высшем уровне под эгидой ООН по вопросам информационного общества зам-министра связи и массовых коммуникаций РФ Рашид Исмаилов, и государство, и все участники рынка информационных услуг должны выработать единую конвенцию в сфере регулирования Интернета [18]. В частности, одним из пунктов может быть сохранение тайны личной переписки добропорядочных граждан, но в то же время – контроль и запрет публичных страниц и аккаунтов групп, пропагандирующих терроризм и иную преступную деятельность. Один из примеров подобного компромиссного сотрудничества, согласно отчету главы сервиса Telegram Павла Дурова, – блокировка более 8500 каналов, связанных с терроризмом в октябре 2017 г. [27]. В связи с этим дискуссионным и деликатным остается вопрос о законности и моральной допустимости мониторинга общего потока пользовательских сообщений, их сбора и хранения. Доверительные отношения между обществом и государством могут быть нарушены. Например, показательны результаты референдума, прошедшего в Нидерландах в марте 2018 г. [17]. Большинство жителей страны выразили протест против инициативы силовых структур (48,9% голосов против 47,2%). Однако новый закон был одобрен обеими палатами парламента и позволил спецслужбам отслеживать интернет-трафик, прослушивать телефонные переговоры граждан, взламывать электронные устройства подозре-

ваемых, собирать базу ДНК и даже предоставлять собранные сведения зарубежным спецслужбам. Обратим внимание, что этот закон противоречит ранее принятым документам ЕС, вводящим более жесткие правила конфиденциальности телекоммуникаций [31].

В России приватность в сети Интернет регулируется с 1996 г. на основе Системы оперативно-разыскных мероприятий (СОРМ). Новое поколение СОРМ, по словам О.Ю. Стороженко, должно аккумулировать структурированную информацию о любом человеке (его номерах телефонов, звонках, контактах, перемещениях, темах разговоров дома, посещаемых сайтах и иных данных) [21, с. 69]. Вместе с тем опрос россиян об их отношении к доступу ФСБ к их личной переписке показал, что лишь 3% считают это допустимым, «31% отметили, что считают это недопустимым ни в каких случаях, большинство, 61%, отметили, что это допустимо в некоторых случаях и 5% затруднились с ответом на данный вопрос. Тем, кто ответил, что считают чтение личной переписки сотрудниками ФСБ допустимым, задавался вопрос о том, в каких случаях это допустимо. Ответы включали в себя в основном террористическую деятельность, антигосударственные преступления, борьбу с преступностью и наркотрафиком, военные действия. В таких случаях респонденты, участвовавшие в данном исследовании, готовы пожертвовать конфиденциальностью собственной переписки, чтобы содействовать мероприятиям ФСБ» [19].

Еще один аспект проблемы, связанной с санкционированием проникновения в персональные данные, возникает при обсуждении приоритета личных или общественных интересов в ситуациях крупных эпидемий, например, вызванных вирусами Эбола, H1N1 или коронавирусом SARS-CoV-2. Большинство государствен-ных регламентов направлены на защиту общественного здоровья в ущерб сохранению тайны частной жизни. Но использование личной информации может быть продиктовано не только благими намерениями в интересах государства и социальной значимостью, а еще незаконными или корыстными интересами третьих лиц. В 2007 г. кардиолог вице-президента США Дика Чейни не одобрил использование его пациентом беспроводного стимулятора сердца из-за риска постороннего вмешательства в его работу. Современные миниатюрные медицинские приборы, такие как инсулиновые насосы, непрерывные мониторы глюкозы, стимуляторы сердца или дефибрилляторы, могут с помощью Интернета пересылать сообщения лечащему врачу. Но если для компьютеров и смартфонов созданы и применяются обновления

безопасности, то для медицинских приборов на первом месте стоит надежность и легкость в использовании пациентами. Эксперты по безопасности демонстрируют, что с помощью легкодоступного оборудования, руководства для пользователя и знания кода прибора они могут взять под контроль прибор или осуществлять мониторинг посылаемых им данных [29].

С цифровизацией банковской и торговой сфер и их сращиванием на основе скоринговых и скрининговых интересов связана угроза манипулирования данными. Сегодня банки собирают информацию о клиентской базе потенциальных заемщиков не только в социальных сетях [32], но и изучая потребительскую корзину клиентов с целью определения наиболее полного личностного профиля возможного заемщика. Речь идет о наиболее полной информации, восстановленной по оплатам банковской картой в кинотеатрах, аптеках, медицинских учреждениях, на вокзалах. Фактически это не только социально-психологический профиль, но и проблемы здоровья, культурных и политических предпочтений и другие факты личной жизни, которые легко восстанавливаются в таком расширенном скрининге, но нарушают этические нормы вторжения в приватные пространства личности [33].

Фактически частные данные, собранные полулегально через банковско-маркетинговый скрининг и соцсети, всё чаще становятся товаром, и это не может не вызывать чувства протеста. Так, в марте 2018 г. популярный сервис Facebook, британская аналитическая компания Cambridge Analytica и сотрудник Кембриджского университета были обвинены в утечке персональных данных около 50 млн человек [14]. Распространенное по Сети исследовательское приложение, способное якобы делать предсказания на основе анализа личностных черт пользователя, было удалено. Однако оказалось, что невозможно удалить полностью все загруженные данные одного пользователя, и выяснилось, что был несанкционированный доступ этой программы к информации друзей пользователя, загрузившего себе это приложение. Компания Facebook оправдывалась тем, что список контактов, содержание телефонных разговоров и SMS собирались только с согласия пользователей [24] и исключительно в их интересах, чтобы защитить от оскорбительного контента [25]. Однако, по данным службы интернет-безопасности компании InfoWatch, лишь только за первую половину 2017 г. вследствие 925 крупных инцидентов была зафиксирована утечка 7,78 млрд записей с персональными и платежными данными по всему миру, что составило восьмикрат-

ный рост по сравнению с 2016 г. [13]. Более того, в 2011 г. было обнаружено, что крупнейшие интернет-провайдеры США продавали смартфоны с предустановленным программным обеспечением, которое могло контролировать всё – от посещаемых сайтов до поисковых запросов. По словам провайдеров, целями данной слежки был якобы поиск неисправностей, а не коммерческая заинтересованность. Причем правительство США, президент Барак Обама в частности, настоятельно рекомендовало производить смартфоны с возможностью контроля за уплатой налогов и предупреждения терроризма [12]. Собранная таким образом информация позволяет не только нарушать неприкосновенность личных данных, но еще и использовать ее в интересах третьих лиц. Между тем результаты проведенного нами в 2019 г. социологического опроса среди жителей г. Курска (Россия) показали: 69,4% опрошенных не согласны предоставлять подробную личную информацию, которую они не выкладывали в социальные сети; 8,2 – безразличны; 3,7% – абсолютно согласны; больше половины респондентов (61,1%) считают себя объектом манипуляций с использованием социальных технологий (рекламы, в частности); 38,9% – не считают [1, с. 149].

Нарушение приватности, конфиденциальности как со стороны государства, бизнес-корпораций, так и со стороны криминальных киберструктур подрывает базовые права человека на личное пространство и личную информацию, защита которых гарантируется государством и правовой системой лишь формально. Возникает проблема принятия новых кодексов, направленных на защиту прав личности в цифровую эпоху. Причем скорость принятия соответствующих законов резко отстает от скорости появления новых угроз для личности в киберфизической реальности.

Однако корни нарастающей проблемы кроются еще глубже. Необходимо, на мой взгляд, отдельно отметить значимые экзистенциально-антропологические аспекты. Современное общество переживает период значительных психоментальных трансформаций. Современную эпоху называют «гиперинформационной». Например, по данным Facebook, пользователи ежедневно обмениваются 500 терабайтами информации, 300 млн фотографий, 2,7 млрд «лайков», а Google фиксирует 5,3 млрд запросов в день [16]. Причем, по расчетам аналитиков Международной исследовательской и консалтинговой компании IDC, занимающейся изучением мирового рынка информационных технологий и телекоммуникаций, объем данных растет в геометрической прогрессии. Авторы этого

доклада также утверждают, что «по сравнению с сегодняшним днем каждый человек будет в 20 раз чаще взаимодействовать с Интернетом или с устройствами с выходом в Интернет. Если сейчас среднее количество взаимодействий – чуть больше 600, то к 2025 г. мы будем сталкиваться с сетью 4800 раз в день». Эксперты IDC прогнозировали, что «с 2009 по 2020 г. объем мировых данных увеличится в 44 раза, потом – в 50 раз, теперь уже значится цифра 55 раз. Каждый год IDC с учетом анализа новых данных перестраивает кривую роста вверх, как правило, на несколько зеттабайт, по последнему отчету с 2009 г. объем данных за год с 0,8 зеттабайт вырастет до 44 зеттабайт в 2020 г. К 2025 г., согласно исследованию IDC по заказу Seagate, количество информации вырастет до 163 зеттабайт» [16].

Однако количество данных совсем не коррелирует с качеством и значимостью сохранения этой информации, с одной стороны, и фактической возможностью защитить личностно или государственно важную информацию – с другой. Кроме того, беспрецедентные объемы информации, которую приходится искать, осмысливать, отбирать и использовать, неминуемо приведут к изменению форм взаимодействия с этой информацией. Ученые отмечают, что обработка информации современным человеком переориентируется с понятийной на образную, с текста на картинку. В частности, одна из причин популярности ресурса Instagram заключается в том, что огромному количеству людей (ежедневно там выставляется около 700 млн фото и видео) дается возможность представить себя и свой мир не через привычные тексты, цифры, звуки, а через визуальные образы, причем не всегда однозначно одобряемые обществом, часто провокационные и выходящие за рамки традиционных моральных норм [3]. Кроме того, данные социологических исследований демонстрируют противоречия между тем, как респонденты отвечают на вопросы исследователей, и тем, как они реагируют эмоционально и мимически. Так, 60% опрошенных выразили нейтральное отношение к выложенным личным фотографиям незнакомцев, которые оцениваются скорее эстетически, чем этически. Вместе с тем на фотографии знакомых людей они реагировали очень эмоционально. Причем при показе опрошенным таких фото вне Instagram больше половины отреагировали удивлением, смущением или же вовсе отвращением. Это может говорить о том, что сеть Instagram уже стала привычной «сценой» для демонстрации данных фотографий, где это считается «нормальным» [10, с. 36–37]. В этом же исследовании показано,

что 27% респондентов на прямой вопрос «Почему люди перестали стесняться выставлять напоказ подобные фото?» заявили, что «все идет от общества: оно такое одобряет, становится более открытым» [10, с. 36].

Противоречивость процессов в цифровой реальности можно проследить на примере такой социокультурной характеристики, как доверие. С одной стороны, ученые констатируют постепенную либерализацию социальных норм и рост доверия в виртуальной реальности, с другой – пользователи Интернета озабочены проблемой защиты своей приватной сферы и воспринимают тотальный контроль как покушение на свои гражданские права.

Американский футуролог, социолог и политолог Ф. Фукуяма утверждает, что организация социальных интеракций в долгосрочном периоде, благополучие и даже конкурентоспособность государства зависят от уровня доверия в обществе. Именно доверие способно оживить и легитимировать такие формальные социальные институты, как габитус, традиции и мораль [23, с. 14–34]. Доверие выступает тем самым основанием, опираясь на которое выстраиваются предсказуемые отношения и между личностями, и между человеком, социальными системами и государством в целом [5]. Т. Парсонс рассматривал доверие как взаимный обмен ресурсами между подсистемами общества, которые предназначены для сохранения устойчивости общественной структуры. Слаженное действие всех систем обеспечивается генерализированными посредниками, с помощью которых осуществляется обмен информацией. Доверие является одним из таких генерализированных посредников в системе, обеспечивающих бесперебойный обмен информацией между подсистемами общества [15]. То есть можно проследить корреляцию между чувством безопасности человека, уровнем доверия и степенью защиты приватности. Причем информационно-коммуникативные технологии, Интернет в частности, создают особое пространство доверия, где взаимодействие возможно только при условии определенных доверительных отношений.

По данным Фонда «Общественное мнение», 33% населения России в целом доверяют информации, размещенной в Интернете, и 33% – не доверяют. Среди месячной аудитории Интернета более высокий процент – 48% респондентов – доверяют размещенной информации, но и доля не доверяющих среди пользователей оказалась выше – 38%. Самой доверяющей группой оказались пользователи социальных сетей: 51% представителей этой группы положительно ответили на вопрос о доверии [6]. Показателен тот факт,

что потребители читают информацию об интересующем их товаре или продукте, оставленную совершенно незнакомыми людьми, и используют ее для принятия собственного решения [35, с. 97–98]. Доверие, возникающее между акторами, строится на репутации, внешнем виде, манерах, действиях, целях взаимодействующих сторон [36], соответственно большое значение для человека имеет содержание, корректность и степень добровольной открытости доступной информации, а отсюда ощущение ценности и неприкосновенности частной жизни и желание ее защитить.

Социологические исследования отмечают актуальность проблемы приватности для пользователей Сети и демонстрируют разницу в ответах респондентов разного возраста, образования, пола и уровня доходов. Дара О'Нейл обнаружила, что, как ни странно, менее беспокоятся о личных секретах люди, имеющие высокий доход, высшее образование, а также мужчины [34]. Результаты нашего исследования в целом коррелируют с данными О'Нейл[1]. На вопрос «Как вы относитесь к утечке и продаже ваших персональных данных из баз банков, магазинов, медицинских учреждений?» респонденты со средним образованием и обладатели ученой степени реже отвечали отрицательно, чем опрошенные со средним профессиональным и высшим образованием. Из всех возрастных групп были больше озабочены сохранностью своих личных данных респонденты 18–25 лет – и мужчины чаще, чем женщины.

Таким образом, Интернет, став привычной уже деловой и личной коммуникационной площадкой, существенно корректирует принятые границы приватности. В зависимости от идеологии и культурных традиций разных народов границы приватности могут быть различными: от требования неукоснительного соблюдения неприкосновенности частной жизни в Европе до фактического

[1] Опрос проводился методом анкетирования в рамках авторского социологического исследования «Современные социальные технологии как инструмент управления установками личности», проведенного в июне – ноябре 2019 г. среди жителей г. Курска (Россия). Генеральная совокупность – жители города в возрасте от 18 лет и старше – 321 тыс. человек, метод выборки – квотный, выборочная совокупность – 384 респондента.

Материалы социологического исследования находятся в открытом доступе на сайте «Курский социологический клуб», вкладка «Выполненные исследования». Проект «Современные социальные технологии как инструмент управления установками личности». – Режим доступа: http://sociokursk.ru/?page_id=3979 (дата обращения: 01.06.2020).

приоритета общественного и публичного в Китае. Да и само современное общество становится всё более открытым и толерантным к постепенному расширению рамок моральной приемлемости и юридической дозволенности.

Во всем мире наблюдается постоянный рост объемов информации, которую пользователи выкладывают в Интернет добровольно и часто безответственно, доверяя ценные сведения о себе и своем образе жизни многочисленным интернет-ресурсам. Вместе с тем государство в лице спецслужб, коммерческие структуры, банки и другие заинтересованные стороны готовы пожертвовать ценностью неприкосновенности частной жизни, которая была законным правом человека демократического общества.

Конфиденциальность личной информации об образе жизни, здоровье, финансах и контактах по-прежнему воспринимается пользователями Интернета как ценность, и посягательство на нее остро переживается.

Список литературы

1. Асеева И.А. Готовы ли россияне к новой антропотехнореальности? // Вестник Института социологии. – 2020. – Т. 11, № 2. – С. 141–156.
2. Баглай М.В. Конституционное право Российской Федерации [Текст]: учеб. для вузов. – 6-е изд., изм. и доп. – М.: Норма, 2007. – 784 с.
3. Волина М. Социальные сети глазами психолога: зачем мы ведем Instagram? // Woman. – Режим доступа: https://woman.ua/99932-sotsialnie-seti-glazami-psihologa-zachem-mi-vedem-instagram/
4. Всеобщая декларация прав человека. – Режим доступа: https://www.un.org/ru/documents/decl_conv/declarations/declhr.shtml
5. Гидденс Э. Судьба, риск и безопасность // THESIS. – 1994. – № 5. – С. 107–134.
6. Гражданская активность в Интернете // ФОМ [on-line]. – Режим доступа: http://fom.ru/SMI-i-internet/10622
7. Закон Судный людем. Пространной и сводной редакции / под ред. М.Н. Тихомирова. – М.: Академия наук СССР, 1961. – 287 с.
8. Конституция Российской Федерации. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_28399/2573feee1caecac37c442734e00215bbf1c85248/
9. Майоров А.В., Поперина Е.Н. Формирование и развитие права на неприкосновенность частной жизни // Юридическая наука и правоохранительная практика. – 2012. – № 3 (21). – С. 34–38.

10. Мельников М.В., Моисеева З.Ф. Граница между личным и публичным пространством и ее особенности на примере социальной сети Instagram // Теория и практика общественного развития. – 2016. – № 10. – С. 32–37.
11. Назаров С.А. Концепция интернет-приватности // Сборник статей Международной научно-практической конференции «Актуальные вопросы современного права. Пути теоретического и практического решения проблем» (Уфа, 01.03.2018 г.). – Уфа: Аэтерна, 2018. – С. 130–133.
12. Обама выступил против смартфонов, к которым нельзя получить доступ // ТАСС. – 2016. – Режим доступа: http://www.tass.ru/mezhdunarodnaya-panorama/2733318/
13. Объем утечек конфиденциальной информации в мире в 2017 году вырос в 8 раз // РБК. – 2017. – Режим доступа: www.rbc.ru/technology_and_media/10/10/2017/59db57549a7947f8d8839ac3/
14. Очередной скандал с утечкой персональных данных сильно ударил по Facebook // Роскомсвобода. – 2018. – Режим доступа: https://roskomsvoboda.org/37210/
15. Парсонс Т. О структуре социального действия. – М.: Академический проект, 2000. – 880 с.
16. Попытки расчета количества информации на планете Земля. – Режим доступа: https://nag.ru/articles/article/101906/popyitki-rascheta-kolichestva-informatsii-na-planete-zemlya.html
17. Референдум о расширении полномочий спецслужб поделил Нидерланды на два почти равных лагеря // Роскомсвобода. – 2018. – Режим доступа: https://roskomsvoboda.org/37292/
18. Россия выступила за создание конвенции в сфере регулирования Интернета под эгидой ООН // Роскомсвобода. – 2018. – Режим доступа: https://roskomsvoboda.org/37273/
19. Савинкова Ю.К. Доверие информационным источникам и представления о конфиденциальности личной переписки в сети Интернет. – Режим доступа: https://www.hse.ru/data/2014/06/05/1323468899/Савинкова%20Ю.К.%20Доверие%20информационным%20ис..чной%20переписки%20в%20сети%20Интернет.docx
20. Социотехнический ландшафт цифровой реальности: философско-методологический концепт, онтологические матрицы, экспертно-эмпирическая верификация: коллективная монография / Аршинов В.И., Артеменко М.В., Асеева И.А., Буданов В.Г., Гримов О.А., Каменский Е.Г., Кореневский Н.А., Маякова А.В., Чеклецов В.В. / отв. ред. В.Г. Буданов, И.А. Асеева. – Курск: ЗАО «Университетская книга», 2019. – 212 с.
21. Стороженко О.Ю. Система технических средств для обеспечения функций оперативно-розыскных мероприятий: вчера, сегодня, завтра // Вестник Краснодарского университета МВД России. – 2014. – № 3 (25). – С. 69–72.

22. Фролова О.С. Частная жизнь в свете Конвенции о защите прав человека и основных свобод // Журнал российского права. – 2008. – № 10 (142). – С. 118–123.
23. Фукуяма Ф. Доверие: социальные добродетели и путь к процветанию: пер. с англ. – М.: АСТ, 2008. – 730 с.
24. Facebook годами собирал информацию о звонках и СМС пользователей так, что они об этом не догадывались. В соцсети говорят, что все законно // Meduza. – 2018. – Режим доступа: https://meduza.io/feature/2018/03/27/facebook-godami-sobiral-informatsiyu-o-zvonkah-i-sms-polzovateley-tak-chto-oni-ob-etom-ne-dogadyvalis-v-sotsseti-govoryat-chto-vse-zakonno
25. Facebook рассказал о сканировании личных сообщений пользователей // РБК. – 2018. – Режим доступа: https://www.rbc.ru/technology_and_media/04/04/2018/5ac4fd779a7947420af1b3bb
26. Google ушел из Китая // Forbes. – 2010. – Режим доступа: http://www.forbes.ru/tehno/internet-i-telekommunikatsii/46869-google-ushel-iz-kitaya/
27. Telegram в октябре заблокировал более 8500 каналов за связь с терроризмом // Ведомости. – 2017. – Режим доступа: https://www.vedomosti.ru/technology/news/2017/10/29/739749-telegram-v-oktyabre-zablokiroval/
28. Budanov V., Aseeva I. Manipulative marketing technologies in new digital reality // Economic Annals-XXI. – 2019. – Vol. 180 (11–12). – P. 58–68.
29. Clery D. Could your pacemaker be hackable? // Science. – 2015. – 30 January. – Vol. 347, Issue 6221. – P. 499.
30. Enserink M., Chin G. The end of privacy // Science. – 2015. – 30 January. – Vol. 347, Issue 6221. – P. 490–491.
31. EU lawmakers agree to strengthen privacy rules for WhatsApp, Skype. – Mode of access: https://in.reuters.com/article/us-eu-privacy/eu-lawmakers-agree-to-strengthen-privacy-rules-for-whatsapp-skype-idINKBN1CO2OO
32. Hagel J., Armstrong A. Net Gain: Expanding Markets Through Virtual Communities. – Cambridge: Harvard Business Press, 1997. – 235 p.
33. Lengare K.B. Data ethics and its role in digital era // Review of Research. – 2018. – August. – Vol. 7, Issue 11. – P. 1–7.
34. O'Neil D. Analysis of Internet Users' Level of Online Privacy Concerns // Social Science Computer Review. – 2001. – Vol. 19, N 1. – P. 17–31.
35. Punj G.N. Do consumers who conduct online research also post online reviews? A model of the relationship between online research and review posting behavior // Springer Science. – 2012. – P. 97–108.
36. Sztompka P. Trust. – Cambridge: Cambridge University Press, 1999. – 214 p.
37. Warren S., Brandeis L. The Right to Privacy // Harvard Law Review. – 1890. – P. 193–220. – Mode of access: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf