Мочалов А.Н. Цифровые следы человека и неприкосновенность частной жизни. // Антиномии. 2024. Т. 24, вып. 4. С. 164-189. https://doi.org/10.17506/26867206_2024_24_3_164

УДК 342.7
DOI 10.17506/26867206_2024_24_4_164

Цифровые следы человека и неприкосновенность частной жизни

Артур Николаевич Мочалов
Уральский государственный юридический университет им. В.Ф. Яковлева
г. Екатеринбург, Россия
E-mail: artur.mochalov@usla.ru

Поступила в редакцию 13.06.2024, поступила после рецензирования 27.09.2024, принята к публикации 11.11.2024

В статье рассматриваются конституционно-правовые проблемы обеспечения права человека на неприкосновенность частной жизни при сборе, хранении и использовании информации о нем, полученной из цифровых следов. Анализируется юридическая природа цифровых следов человека, приводится их авторская классификация. Отмечается, что в силу многообразия цифровых следов на них распространяются различные правовые режимы. Объединяет их то, что они всегда возникают в результате взаимодействия индивида с цифровым устройством, компьютерной системой или информационно-телекоммуникационной сетью и несут на себе отпечаток такого взаимодействия. В связи с этим автор отстаивает позицию, что цифровой след практически во всех случаях содержит в себе информацию о частной жизни индивида. Данную презумпцию следует закрепить в законе и исходить из нее при осуществлении правового регулирования использования цифровых следов. Автор приходит к выводу, что законодательство Российской Федерации не учитывает этой специфики цифровых следов, в результате чего информация, оставленная человеком в сети Интернет, практически без ограничений может использоваться как органами безопасности, так и частными компаниями – владельцами интернет-сайтов и поставщиками электронных услуг. При этом индивид практически во всех случаях утрачивает контроль за дальнейшей судьбой оставленного им цифрового следа. Такое положение дел рассматривается автором как непропорциональное ограничение права на неприкосновенность частной жизни. Автор соглашается с тем, что в цифровом мире приватность является относительной. Вместе с тем неприкосновенность частной жизни продолжает сохранять значение. Она ограждает индивида от чрезмерного контроля со стороны окружения, в том числе со стороны государства. По этой причине автор видит необходимость закрепления в законе гарантий недопустимости массового цифрового слежения за гражданами со стороны правоохранительных органов и органов безопасности, а также ограничений использования

цифровых следов администрациями интернет-сервисов. В частности, предлагается законодательно закрепить право интернет-пользователей запрещать автоматизированное предоставление тех или иных сведений владельцам сайтов, а также право отказаться от применения рекомендательных технологий.

Ключевые слова: цифровой след, информационные технологии, частная жизнь, неприкосновенность частной жизни, Интернет, большие данные, персональные данные, цифровой профиль

Благодарности: Исследование выполнено при финансовой поддержке Российского научного фонда, проект № 24-28-01378 «Разработка концепции правового регулирования цифрового профилирования, социального скоринга и использования цифровых следов», https://rscf.ru/project/24-28-01378/

Human Digital Footprints and Privacy

Artur N. Mochalov

Ural State Law University named after V.F. Yakovlev
Ekaterinburg, Russia
E-mail: artur.mochalov@usla.ru

Received 13.06.2024, revised 27.09.2024, accepted 11.11.2024

Abstract. The article explores the constitutional and legal challenges associated with ensuring the human right to privacy in the context of collecting, storing and utilizing information derived from digital traces. It analyzes the legal nature of human digital footprints and provides classification of their types. The article highlights that the diverse nature of digital footprints subjects them to various legal regimes, all of which emerge from an individual's interaction with digital devices, computer systems, or information and telecommunications network, thereby reflecting the imprint of such interaction. The author argues that digital footprints, in most instances, contain information pertaining to an individual's private life, a presumption that should be codified in law. Legal regulations governing the use of digital footprints should be grounded in this presumption. The author concludes that current legislation in the Russian Federation fails to account for the unique characteristics of digital traces, resulting in the unrestricted use of information left by individuals online by both security agencies and private companies. Consequently, individuals often lose control over the future of their digital footprints, which the author views as a disproportionate restriction of the right to privacy. While acknowledging that *privacy* is a relative concept in the digital realm, the author emphasizes it continued significance in protecting individuals from excessive control from external entities, including government authorities. For this reason, the author advocates for legal provisions that prohibit mass digital surveillance of citizens by law enforcement and security agencies, as well as restrictions on the use of digital traces by online services providers. In particular, the article proposes legislating the right of Internet users to prevent the automated sharing of certain information with website owners, as well as the right to refuse the use of recommendation technologies.

Keywords: digital footprint; information technology; privacy; Internet; big data; personal data; digital profile

Acknowledgements: The reported study was funded by the Russian Science Foundation (RSF), under project number 24-28-01378, titled "Development of the Concept of Legal Regulation of Digital Profiling, Social Scoring and the use of Digital Traces." For more information, please visit https://rscf.ru/project/24-28-01378/.

For citation: Mochalov A.N. Human Digital Footprints and Privacy, *Antinomies*, 2024, vol. 24, iss. 4, pp. 164-189. (In Russ.). https://doi.org/10.17506/26867206_2024_24_4_164

Введение

По данным *Mediascope*, аудитория Интернета в России в 2023 г. превысила 101 млн человек, а суточный охват составил 81 % населения[1]. Каждый пользователь оставляет на различных интернет-ресурсах множество данных, связанных с ним: начиная с поисковых запросов и геолокации и заканчивая персональной информацией (такой как имя, адрес или номер телефона) при регистрации на сайтах, заполнении интерактивных форм или оформлении заказов в интернет-магазинах.

Информация, оставляемая человеком в электронной форме в процессе взаимодействия с компьютерными устройствами и информационно-телекоммуникационными сетями, получила название «цифровых следов». Не имея материально-вещественной формы, цифровой след вместе с тем сохраняется в памяти устройств, обеспечивающих функционирование информационно-телекоммуникационной системы, в виде кодированного набора числовых данных. В этом качестве он может существовать сколь угодно долго, не утрачивая своих первоначальных свойств. Неудивительно, что на цифровые следы обратили внимание криминалисты (Буйнов 2023; Черданцев 2019). Доктринальное осмысление стали получать проблемы использования цифровых следов в качестве доказательств в судах (Лазарева 2023).

Однако правовое измерение цифровых следов простирается намного дальше вопросов раскрытия преступлений и судебного доказывания. Цифровые следы могут многократно копироваться и практически мгновенно передаваться по сетям связи; над ними могут производиться компьютерные вычисления, в том числе путем сопоставления с другими цифровыми данными, принадлежащими этому же лицу или другим лицам. Технологии «больших данных», ставшие возможными благодаря росту скорости обработки и передачи колоссальных информационных массивов, позволяют на основе анализа цифровых следов человека составлять его цифровой профиль, включающий производную (т.е. полученную посредством компьютерных вычислений) информацию о вероятных предпочтениях и интересах человека, его политических взглядах и религиозных убеждениях, о состоянии здоровья и т. д. (Виноградова и др. 2021; Савельев 2015: 51-52). Интеллектуальный анализ данных, основанный на технологиях машинного обучения, дает возможность по полученным сведениям прогнозировать

[1] Интернет в России в 2022–2023 годах. Состояние, тенденции и перспективы развития : отраслевой доклад. URL: https://digital.gov.ru/uploaded/files/internet-v-rossii-v-2022-2023-godah.pdf (дата обращения: 20.05.2024).

и направлять поведение индивида и целых групп, ранжировать субъектов и оценивать их действия (Виловатых 2020; Рувинский 2023). Эти ценные свойства цифровых следов обусловливают повышенный интерес к ним со стороны государственных и коммерческих структур, а также злоумышленников.

При этом процессы, связанные с использованием и обработкой цифровых следов, в большинстве случаев не находятся под контролем оставившего их индивида. Более того, сам факт оставления цифрового следа не всегда осознается человеком. Эти обстоятельства обусловили широкую академическую дискуссию о проблемах обеспечения прав человека в «цифровом мире» – начиная с прикладных вопросов получения согласия субъекта на обработку его персональных данных (Дупан (Гутникова) 2016; Талапина 2018) и заканчивая глобальной угрозой массовой «цифровой слежки» со стороны правительств разных стран (Савельев 2015; Watt 2017; Westerlund et al. 2021).

Предлагаемое исследование акцентирует внимание на некоторых фундаментальных юридических проблемах, связанных с формированием, передачей, хранением и последующим использованием цифровых следов человека. Поставленная задача осложняется по крайней мере двумя обстоятельствами. Во-первых, цифровые следы, как будет показано далее, обладают многообразием с точки зрения их правовых режимов и механизмов правовой охраны. Во-вторых, многие государства – включая Россию – в последнее десятилетие ввели законодательное регулирование, регламентирующее особенности оборота тех или иных разновидностей цифровых следов. По этой причине глобальная проблема, преломляясь через законодательство той или иной страны, неизбежно приобретает национальное измерение. Подходы, складывающиеся в отдельных государствах, отличаются своеобразием, в связи с чем их сравнительное исследование заслуживает отдельного обсуждения. В данной же статье мы ограничимся анализом ответов на глобальные вызовы цифровизации, которые предлагают в рассматриваемой части российское законодательство и правоприменительная практика.

Понятие цифровых следов и их классификация. В отечественной юриспруденции до настоящего времени не сложилось единообразного подхода к определению цифровых следов. В криминалистической науке под цифровыми (виртуальными) следами предлагается понимать любые сведения, оставленные и (или) сохраненные в информационном пространстве (Черданцев 2019: 179); компьютерную информацию о событиях, действиях, процессах и фактах, отраженную в компьютерных системах и сетях либо на отдельных носителях в процессе ее возникновения, обработки, хранения, передачи или удаления (Буйнов 2023: 21). В более широком контексте цифровой след есть результат фиксации тех или иных явлений в электронной форме (в виде числовых данных) на компьютерных устройствах, в компьютерных системах или информационно-телекоммуникационных сетях. Любой цифровой след несет в себе информацию об отражаемом им явлении,

представляет собой его числовой отпечаток, или – как его часто называют – «цифровую тень». Такая информация не всегда связана с человеком. Например, это может быть «отпечаток» какого-либо технологического процесса или производственного объекта. Но часто цифровой след содержит сведения о действиях людей, о характеристиках определенного человека или о связанных с ним событиях. В последнем случае можно говорить о *цифровом следе человека*.

Цифровые следы человека могут быть классифицированы по разным основаниям. Рассмотрим классификации, представляющие интерес с позиций юриспруденции и обозначенной проблематики.

1. *По способу закрепления* цифровые следы человека можно разделить на два вида. Первые сохраняются только на пользовательском устройстве, с которым взаимодействует индивид, тогда как вторые передаются по информационно-телекоммуникационным сетям и записываются в память носителей информации, не принадлежащих пользователю. Например, при осуществлении фотосъемки на простой цифровой фотоаппарат полученный цифровой след (фотоизображение и его метаданные – такие как дата и время съемки, геолокация) сохраняется лишь в памяти фотокамеры и, следовательно, остается недоступным другим лицам, помимо ее владельца. По-иному обстоит дело, если фотография сделана на смартфон, подключенный к Интернету, и сохраняется пользователем в «облачном» хранилище. Файл изображения вместе с метаданными в этом случае передается по сетям связи и записывается на внешнем оборудовании. Дальнейшая судьба переданного файла зависит уже не только от самого пользователя, но и от иных субъектов, которые получают техническую возможность обрабатывать сохраненную информацию, копировать и передавать ее третьим лицам, блокировать доступ к ней, удалять из памяти своего оборудования. Аналогичной является ситуация, когда пользователь делится записью, изображением или любым другим файлом в социальной сети, передает информацию по электронной почте или через мессенджер, размещает на сервисе фото- или видеохостинга. Во всех этих случаях доступ к цифровому следу и возможность его использования в собственных интересах появляется не только у оставившего его пользователя, но и у третьих лиц, в том числе у владельцев социальных сетей и иных интернет-сервисов, провайдеров услуг хостинга (хранения информации).

2. *По режиму доступа* цифровые следы, передаваемые посредством сети Интернет, можно подразделить на следы ограниченного доступа (остаются доступны пользователю или определенному им кругу лиц) и общедоступные следы. Например, данные, которые покупатель вводит при оформлении заказа в интернет-магазине, предназначены конкретному лицу (продавцу) и, следовательно, должны оставаться только в его распоряжении. То же касается, например, переписки в мессенджерах и в сервисах электронной почты. В публичный доступ такие цифровые следы попадают в основном в результате утечек и других неправомерных действий. Цифровые следы свободного доступа раскрываются неограниченному кругу лиц на законных основаниях. В основном это т. н. «пользовательский контент», который

делается общедоступным по решению самого пользователя – данные открытого профиля в социальной сети, посты, комментарии и т.д. На цифровые следы, представляющие собой общедоступную информацию, в полной мере распространяется правовое регулирование распространения информации. Так, если цифровой след содержит запрещенную к распространению информацию, то доступ к ней может быть ограничен по требованию Роскомнадзора в соответствии со ст. 15.1 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – Закон об информации). Требование об удалении материала (страницы сайта) направляется владельцу сайта через провайдера хостинга (т. е. лица, предоставляющего вычислительную мощность для размещения сайта в Интернете), а в случае ее неудаления провайдер хостинга, а затем и оператор связи обязаны заблокировать доступ пользователей к соответствующей странице интернет-сайта. Ограничивать доступ к запрещенному пользовательскому контенту должны и владельцы социальных сетей (ст. 10.6 Закона об информации). Данное регулирование хорошо иллюстрирует тезис о том, что оставленные человеком цифровые следы могут подвергаться обработке (удалению, блокировке) поставщиками интернет-услуг без участия их первоначального обладателя.

3. В основе следующей классификации цифровых следов лежит *наличие волевого момента*, т. е. стремления лица совершить действие, формирующее цифровой след. Воля индивида, выражающаяся в свободном принятии решения о совершении того или иного действия для реализации собственного интереса, означает сознательное регулирование человеком своего поведения (Фатьянов 2008: 5-6). Однако с учетом того, что цифровой след оставляет не сам человек, а компьютерное устройство, формирование цифрового следа не всегда есть результат сознательно-волевого действия индивида. По этой причине цифровые следы можно подразделить на, во-первых, оставляемые в результате осознанного волеизъявления индивида и, во-вторых, формируемые в автоматизированном режиме, без непосредственного участия человека. К первым можно отнести поисковые запросы в Интернете; данные, оставляемые при оформлении интернет-заказов или заполнении интерактивных форм на сайтах; пользовательский контент. В каждом из этих примеров человек, совершая осознанные волевые действия, преследует цель зафиксировать, передать конкретному получателю или открыто распространить определенную связанную с ним информацию, т.е. оставить цифровой след.

Вторую группу составляют цифровые следы, которые также образуются вследствие взаимодействия индивида с устройством, компьютерной системой или информационно-телекоммуникационной сетью, однако процесс образования и фиксации цифрового следа минует сознание индивида; его воля в этот момент направлена на достижение иной цели, а фиксация той или иной информации не охватывается его непосредственным интересом. Сюда относится, например, история просмотров и действий пользователей на сайтах – т. н. метаданные, которые собираются и сохраняются на оборудовании поставщиков интернет-услуг в автоматизированном режиме,

а также записываются на пользовательских устройствах в виде «куки»-файлов. В качестве метаданных может собираться масса сведений технического характера, на первый взгляд не имеющих отношения к личности пользователя – тип устройства, с которого осуществлен выход в Интернет (стационарный компьютер, ноутбук или смартфон), его модель, IP-адрес, страна и регион подключения, используемый на устройстве браузер и т. д.

Несмотря на то что формально метаданные содержат информацию скорее о технических устройствах, а не о пользователях, во многих случаях они могут прямо или косвенно указывать на личность владельца и содержать характеризующие его сведения – особенно при соотнесении с другими цифровыми следами, оставленными соответствующим пользователем и содержащими сведения персонального характера. Так, тип и модель устройства могут говорить об уровне материального благосостояния владельца, геолокация – о месте его нахождения в момент посещения сайта, а по IP-адресу можно определить оператора услуг доступа в Интернет и через него идентифицировать абонента. Поэтому метаданные также требуют особых мер защиты от произвольного использования. По поводу IP-адреса А. К. Жарова обращает внимание на то, что он указывает на «территориальную принадлежность, провайдера, технологию человека, вышедшего в Интернет, географическое место выхода в Интернет и [содержит] другую информацию», при этом подчеркивает, что в федеральном законе вопрос об отнесении IP-адресов (как и других цифровых идентификаторов) к персональным данным однозначно не решен, в связи с чем сохраняется неопределенность в правовом режиме таких цифровых следов, в том числе в вопросах установления пределов их использования и мер защиты (Жарова 2016). IP-адреса активно используются судами в качестве доказательств причастности лица к совершению правонарушения (например, отправка налоговой отчетности или платежных распоряжений разных налогоплательщиков с использованием одного и того же IP-адреса может свидетельствовать об их взаимозависимости или о согласованности действий[2]). При этом на сведения об IP-адресе не распространяется правовой режим тайны связи: таковой является содержание сообщения, но не идентификатор устройства, с которого оно отправлено[3]. В то же время в деле № А40-14902/2016 суд посчитал IP-адрес устройства физического лица персональными данными, отметив, что к таковым относятся «не только данные, позволяющие идентифицировать абонента, но также и сведения баз данных систем расчета за оказан-

[2] См., напр.: Постановление Арбитражного суда Уральского округа от 24 мая 2017 г. № Ф09-2083/17 по делу № А60-36692/2016; Постановление Арбитражного суда Западно-Сибирского округа от 28 октября 2020 г. № Ф04-3694/20 по делу № А27-16351/2019. При этом суды признают, что само по себе совпадение динамического IP-адреса, с учетом механизма присвоения IP-адресов и в отсутствие иных доказательств взаимозависимости, не свидетельствует о недобросовестности налогоплательщиков (см., напр.: Постановление Арбитражного суда Центрального округа от 4 мая 2017 г. № Ф10-1268/17 по делу № А54-6206/2015).

[3] Постановление Федерального арбитражного суда Московского округа от 12 марта 2013 г. № Ф05-1348/13 по делу № А40-112131/2012.

ные услуги связи, в том числе о соединениях, трафике и платежах абонента, также относятся к сведениям об абонентах», а IP-адрес и другие идентификаторы, собираемые при помощи «куки»-файлов, позволяют определить географическое положение пользователя и отличить его интернет-трафик от трафика других пользователей[4]. Указанный подход гармонирует с регулированием, содержащимся в параграфе 18 преамбулы Общего регламента Европейского Союза о защите данных (*GDPR*): согласно ему сетевые идентификаторы «могут оставлять следы, которые, в частности, в сочетании с уникальными идентификаторами и другой полученной серверами информацией могут использоваться для создания профилей физических лиц и для их идентификации».

4. *По характеру отражаемых сведений* одни цифровые следы человека отражают действия индивида исключительно в информационной среде, в том числе на различных сайтах в сети Интернет, в то время как другие могут выступать цифровыми отпечатками событий из мира физической реальности. Цифровой след – хотя и появляется в результате взаимодействия индивида с компьютерными устройствами и сетями – далеко не всегда связан только с его действиями в виртуальном пространстве. Например, геолокация, представляющая собой сведения о местоположении устройства, позволяет получить информацию о нахождении и перемещении его владельца в физическом пространстве (Иванова 2020). Примером цифровых следов, свидетельствующих об офлайн-активности индивида, могут служить следы, оставляемые в информационных системах электронными средствами идентификации – такими как FanID при посещении спортивных мероприятий. Цифровизация в определенном смысле стирает грань между физической и виртуальной реальностью: если в физическом мире происходит взаимодействие человека с компьютерными системами, они сохранят отпечаток такого взаимодействия.

Цифровые отпечатки физической реальности создаются и различными «умными устройствами», работающими на основе технологии «интернета вещей» – от «умных часов» и «виртуальных помощников» до систем «умного дома» и беспилотных автомобилей. Датчики «умных часов» и других подобных аксессуаров собирают информацию о физическом состоянии владельца (например, частота пульса или температура тела) и о его активности (например, количество шагов). На основе этой информации можно судить о состоянии здоровья человека, его образе жизни, режиме дня и т.д. Собранные сведения не только обрабатываются на устройстве, но и передаются по сети Интернет на серверы «облачных» вычислений, работа которых контролируется производителем устройства или лицензиатом установленного на нем программного обеспечения. Следы человеческой активности в физической реальности формируются и передаются «умными устройствами», как правило, в автоматизированном режиме, получившем название «трекинг» (что означает «отслеживание»), без специального волеизъявления владельца. Информация с датчиков «умного дома» (например, о температуре воздуха в помещении, о времени включения освещения или об использовании коммунальных ресурсов) на первый взгляд не носит

персонального характера. Однако в своей совокупности такие цифровые следы создают цифрового двойника объекта «умного дома» – виртуальную модель, содержащую актуальную информацию о параметрах, свойствах и характерных процессах оригинального объекта, позволяющую идентифицировать и прогнозировать изменения оригинального объекта[5]. Такая модель, в свою очередь, может нести в себе информацию о режиме дня и образе жизни проживающих лиц. То же можно сказать об «умном городе» с его системами видеофиксации и распознавания лиц: цифровой двойник города может содержать сведения обо всех активностях граждан в публичном пространстве.

Многообразие цифровых следов обусловливает различие в их правовом регулировании. Цифровые следы могут содержать персональные данные пользователя и попадать под действие Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (например, анкетная информация в профиле социальной сети, номер телефона в форме обратной связи, изображение лица). Некоторые следы могут не содержать персональных данных (например, запросы в поисковых сервисах или на сайтах маркетплейсов), однако представлять собой информацию об интересах и потребностях конкретного пользователя (личность которого часто может быть определена при соотнесении с другими цифровыми следами). На некоторые цифровые следы может распространяться тайна переписки или тайна связи (например, сообщения в мессенджерах или в сервисах электронной почты), другие же цифровые следы представляют собой общедоступную информацию. Ряд цифровых следов может содержать в себе иную охраняемую законом тайну – врачебную, банковскую или налоговую. Цифровые следы могут быть результатом творческой деятельности человека (например, фотография) и попадать под действие законодательства об интеллектуальной собственности, а могут иметь характер технической информации об устройстве. Но все они объединены общим признаком: представляя собой цифровое отражение той или иной деятельности конкретного человека, они несут информацию о его частной жизни.

Цифровые следы как отпечатки частной жизни человека. Независимо от того, к какому виду мы отнесем цифровой след человека, он потенциально может содержать информацию, касающуюся конкретного индивида – его действий, состояния здоровья, взглядов и убеждений, политических предпочтений, отношений с другими людьми и т. д. Иными словами, цифровой след отражает ту или иную сторону частной жизни лица.

Под частной жизнью человека понимается область его жизнедеятельности, «которая относится к отдельному лицу, касается только него и не подлежит контролю со стороны общества и государства, если носит

[5] Национальный стандарт РФ ГОСТ Р 71199-2023 «Системы киберфизические. Умный дом. Термины и определения» (утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 29 декабря 2023 г. № 1766-ст). Пункт 16.

непротивоправный характер» (Определение Конституционного Суда РФ от 28.06.2012 г. № 1253-О). Статья 17 Международного пакта о гражданских и политических правах запрещает произвольное или незаконное вмешательство в личную и семейную жизнь человека и гарантирует защиту закона от любого такого вмешательства. В основе права на неприкосновенность частной жизни лежит презумпция того, что «в жизни частных лиц должна существовать область, связанная с их независимым развитием, взаимодействием и свободой… которая является свободной от вмешательства государства, а также свободной от чрезмерного нежелательного вмешательства со стороны других лиц, не имеющих на это разрешения»[6]. Понятие частной жизни, как отмечается в научной литературе и в практике международных судебных органов, не предполагает исчерпывающего определения: оно охватывает бесконечное множество различных аспектов жизнедеятельности человека (Ромашов 2019: 110) – не только приватных, которые человек желает сохранить в тайне, но и тех, которые реализуются им в публичном пространстве[7].

Неприкосновенность частной жизни гарантируется и ст. 23 Конституции РФ. Она обеспечивается, в частности, запретом сбора, хранения, использования и распространения информации о частной жизни человека без его согласия (ч. 1 ст. 24 Конституции РФ), а также тайной переписки, телефонных переговоров, почтовых и иных сообщений (ч. 2 ст. 23 Конституции РФ). Конституционное закрепление права каждого человека на неприкосновенность частной жизни выступает, по справедливому замечанию Г.Б. Романовского, «признанием со стороны государства приоритета (первичности) индивидуума как субъекта права» (Романовский 2001: 23).

В связи с этим было бы справедливым закрепить в законе презумпцию отражения в любом цифровом следе человека информации о его частной жизни и поместить все цифровые следы человека под защиту ч. 1 ст. 23 и ч. 1 ст. 24 Конституции РФ. На этой презумпции должно основываться законодательное регулирование, связанное с оборотом и использованием данной информации независимо от ее правового режима.

Здесь можно возразить, что с технической точки зрения цифровой след – это результат функционирования компьютерных устройств или систем. Он генерируется не человеком, а машиной. Установить по одному лишь цифровому следу, кто конкретно взаимодействовал с устройством в момент его оставления, не всегда возможно. Однако если говорить о цифровых следах в Интернете, то следует иметь в виду, что современное

[6] Доклад Специального докладчика ООН по вопросу о поощрении и защите прав человека и основных свобод в условиях борьбы с терроризмом г-на Мартина Шейнина от 28.12.2009 № A/HRC/13/37. URL: https://documents.un.org/doc/undoc/gen/g09/178/06/pdf/g0917806.pdf?token=xd3bYoTgnODpTA4IVG&fe=true (дата обращения: 20.05.2024).

[7] См.: Постановление Конституционного Суда РФ от 25 мая 2021 г. № 22-П «По делу о проверке конституционности пункта 8 части 1 статьи 6 Федерального закона “О персональных данных” в связи с жалобой общества с ограниченной ответственностью “МедРейтинг”».

российское законодательство практически не оставляет возможности для анонимного пользования глобальной Сетью. В связи с этим оставленный устройством след почти всегда может быть соотнесен с конкретным лицом. Согласно п. 21 Правил оказания услуг связи по передаче данных (утверждены Постановлением Правительства РФ от 31 декабря 2021 г. № 2606) абонент при заключении договора должен предъявить документ, удостоверяющий личность. Аналогичные правила предусмотрены для предоставления услуг телефонной связи. В свою очередь, у организаторов сервисов мгновенных сообщений в сети Интернет существует обязанность идентифицировать каждого пользователя по абонентскому номеру оператора подвижной радиотелефонной связи (подп. 1 п. 4.2 ст. 10.1 Закона об информации). Обязанность идентификации клиентов предусмотрена и для провайдеров хостинга (п. 5 ст. 10.2-1 Закона об информации). С 1 января 2025 г. вступят в силу требования обязательной идентификации пользователей (по абонентскому номеру телефона либо с использованием предназначенных для идентификации информационных систем) в отношении всех сайтов, где предусмотрена регистрация пользователей в целях доступа к определенной информации или функционалу (п. 10 ст. 8 Закона об информации). Уже сегодня обязательная интеграция с Единой системой идентификации и аутентификации (ЕСИА) предусматривается для сервисов размещения объявлений в сети Интернет (подп. 7 п. 1 ст. 10.7 Закона об информации). Данное регулирование позволяет правоприменителю оперировать презумпцией, согласно которой субъектом, оставившим цифровой след, является лицо, идентифицированное в компьютерной сети в процессе взаимодействия с соответствующим сервисом (под личными данными которого выполнена авторизация в системе либо на которое зарегистрирован соответствующий абонентский номер или иной идентификатор услуг связи). Вероятно, единственным предусмотренным законом случаем принудительной анонимизации цифрового следа прошедшего процедуру идентификации интернет-пользователя является шифрование информации об избирателе, заполнившем избирательный бюллетень в ходе дистанционного электронного голосования (п. 16 ст. 64.1 Федерального закона от 12 июня 2002 г. № 67-ФЗ «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации»).

Конечно, не исключаются случаи, когда абонентским устройством пользуется другой человек – не тот, который заключил договор на предоставление услуг связи. Возможно и совершение действий на интернет-сайте под чужим аккаунтом, в том числе в результате неправомерной авторизации (взлома аккаунта, кражи или утечки пароля), а также создания вымышленных аккаунтов с использованием телефонных номеров, зарегистрированных на посторонних лиц («хищение личности»). Сокрытие данных о пользователе может достигаться с использованием различных программных средств – «анонимайзеров», виртуальных частных сетей (VPN) или интернет-браузеров, работающих по специальным протоколам. Однако подобные ситуации не являются массовыми и не опровергают выдвинутый выше тезис о соотносимости цифрового следа и индивида, которому

этот след принадлежит. Тем более что в спорных случаях реальный пользователь, как правило, может быть установлен на основе дополнительной информации (в том числе путем сопоставления с другими цифровыми следами), а при раскрытии преступлений – в результате оперативно-разыскных мероприятий.

Законодательное регулирование использования цифровых следов в контексте права на неприкосновенность частной жизни. Исходя из предположения о том, что цифровой след человека отражает тот или иной аспект его частной жизни, рассмотрим подробнее вопрос о том, насколько правовое регулирование использования цифровых следов в законодательстве Российской Федерации отвечает требованиям ст. 17 Международного пакта о гражданских и политических правах и ст. 23 и 24 Конституции РФ.

Как уже отмечалось, по своей природе и содержанию цифровые следы человека не одинаковы. Различно и их правовое регулирование. Однако, презюмируя наличие в каждом из них сведений о частной жизни конкретного индивида, такое регулирование должно содержать достаточный уровень гарантий уважения частной жизни и ее неприкосновенности. Комитет ООН по правам человека в Замечаниях общего порядка № 16 подчеркнул, что право на неприкосновенность частной жизни должно быть подкреплено в национальном законодательстве «гарантиями от любого такого вмешательства и таких посягательств, независимо от того, совершаются ли они государственными органами, физическими или юридическими лицами»[8]. Данное право не относится к числу абсолютных (не подлежащих ограничениям), однако при этом всякое вмешательство, разрешаемое государством, должно осуществляться не иначе как на основании закона. Такое вмешательство должно быть обоснованным и отвечать целям и задачам Пакта. По мнению Комитета, в законодательстве страны должны подробно определяться конкретные обстоятельства, в которых такое вмешательство может допускаться. Решение о санкционировании вмешательства должно приниматься только компетентным органом, определенным законом, и строго индивидуально.

Хранению личной информации в компьютерных системах посвящен п. 10 Замечаний. Каждое лицо, по мнению Комитета, «должно иметь право удостовериться в ясной форме, содержится ли в автоматизированных файлах данных информация личного характера, и если содержится, то какая и с какой целью». Каждое лицо также должно иметь возможность удостовериться, какие государственные органы или частные лица контролируют или могут контролировать их файлы.

Цифровой след остается в сфере полного контроля оставившего его человека, строго говоря, только в одной ситуации: если он был сформирован в результате волевых действий лица и сохранен только на принадлежащем ему устройстве. Впрочем, даже в этом случае гарантия неприкосновенности

[8] Замечания общего порядка № 16 «Статья 17. Право на личную жизнь». Принято Комитетом по правам человека на его 32-й сессии (1988).

частной жизни не является абсолютной: в практике работы правоохранительных органов нередки случаи изъятия содержимого цифровых устройств, в том числе без судебного решения (Даниленко, Васильев 2020).

В остальных случаях судьба цифрового следа, включая его дальнейшее хранение, использование, копирование, передачу или удаление, оказывается во власти других лиц. Сам же индивид – даже если цифровой след был сформирован в результате его волевых действий – утрачивает возможность контролировать последующие операции с ним. Оставление цифрового следа в Интернете имеет необратимый характер. Так, удаление ранее оставленного поста или комментария со своей страницы в социальной сети не влечет уничтожения истории публикаций на оборудовании владельца интернет-платформы. Администрация социальной сети сохраняет возможность использования этих данных и передавать другим лицам, в том числе правоохранительным органам. В результате «люди оказываются бессильны, поскольку практически невозможно отследить, кто и какой информацией о них обладает, не говоря уже о том, чтобы контролировать множество ситуаций, в которых такая информация может использоваться», – констатируется в п. 13 Доклада Верховного комиссара ООН по правам человека «Право на неприкосновенность частной жизни в цифровой век»[9].

Сохранность цифровых следов, недопущение их попадания к злоумышленникам также зависит от владельцев интернет-сайтов и других поставщиков услуг в Интернете и от принимаемых ими мер защиты информации. Даже у крупных поставщиков интернет-услуг, направляющих значительные средства на обеспечение информационной безопасности, периодически происходят утечки. Результатом утечек может быть раскрытие «чувствительной» информации о пользователях. Например, в 2022 г. известный федеральный сервис доставки готовой еды объявил об утечке пользовательских данных. Раскрытыми оказались сведения о заказах, сделанных пользователями, об их стоимости, об адресах и о времени доставки. По этому факту было возбуждено уголовное дело, а администрация сервиса оштрафована на 60 тыс. рублей за нарушение требований по защите персональных данных (ч. 1 ст. 13.11 КоАП РФ). Размер штрафа, конечно же, несоизмеримо мал в сравнении с вероятными негативными последствиями, которые могли наступить для пользователей. Отдельные пользователи обратились с иском к владельцу сервиса[10], требуя компенсации морального вреда и возложения на ответчика обязанности опубликовать информацию о принятых мерах по защите пользовательских данных. Вместе с тем суды

[9] Право на неприкосновенность частной жизни в цифровой век: Доклад Верховного комиссара Организации Объединенных Наций по правам человека от 3 августа 2018 г. № A/HRC/39/29. URL: https://documents.un.org/doc/undoc/gen/g18/239/60/pdf/g1823960.pdf?token=nfiuD3B5ocl7hq1Vln&fe=true (дата обращения: 20.05.2024).

[10] См.: Клиенты «Яндекс.Еды» подали коллективный иск из-за утечки данных. URL: https://www.rbc.ru/society/14/04/2022/6257c5a99a79478b0e7434b1 (дата обращения: 20.05.2024).

первой и апелляционной инстанций отказали в удовлетворении заявленных требований, сославшись на то, что истцами не доказана принадлежность раскрытых телефонных номеров и «никнеймов» (псевдонимов пользователей) конкретным физическим лицам, а указание адресов доставки без номеров квартир «невозможно соотнести с конкретным человеком»[11]. Вывод судов представляется ошибочным, поскольку он был сделан на основе лишь формального применения законодательства о персональных данных и не касался аспектов, связанных с защитой неприкосновенности частной жизни лица. Судами, в частности, не дана правовая оценка тому, что «цифровые следы», свидетельствующие о сделанных заказах, уже сами по себе являются информацией о частной жизни конкретных индивидов, а соотнесение этих сведений с тем или иным лицом может быть осуществлено и в отсутствие прямого указания на анкетные данные (например, фамилию, имя, отчество или адрес регистрации по месту жительства).

Но не только частные компании – поставщики цифровых услуг становятся обладателями множества цифровых следов, содержащих в себе данные о пользователях. В большинстве стран законодательно установлена обязанность владельцев крупных интернет-сервисов, хостинг-провайдеров и операторов связи предоставлять уполномоченным государственным органам доступ к информационным базам, содержащим цифровые следы. Не является исключением и Российская Федерация. В соответствии с ч. 3 ст. 10.1 Закона об информации организатор распространения информации должен в течение года хранить на территории России информацию (метаданные) обо всех фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков, видео- или иных электронных сообщений пользователей и информацию об этих пользователях (напомним, что каждый пользователь подлежит в соответствии с тем же Законом идентификации). Сами сообщения должны храниться в течение шести месяцев. Данные сведения должны предоставляться органам безопасности и органам, осуществляющим оперативно-разыскную деятельность, путем обеспечения удаленного доступа к информационным системам, эксплуатируемым организаторами распространения информации. Существующее регулирование также предусматривает передачу органам Федеральной службы безопасности информации для декодирования электронных сообщений пользователей[12]. При этом, как подчеркнул Верховный Суд РФ, электронные сообщения граждан в любом случае могут быть предоставлены организаторами распространения информации только

[11] Апелляционное определение Московского городского суда от 12 июля 2023 г. по делу № 33-28022/23. URL: https://mos-gorsud.ru/rs/zamoskvoreckij/services/cases/civil/details/00d96770-14b4-11ed-9053-cb811065760b (дата обращения: 20.05.2024).

[12] Приказ ФСБ России от 19 июля 2016 г. № 432 «Об утверждении Порядка представления организаторами распространения информации в информационно-телекоммуникационной сети “Интернет” в Федеральную службу безопасности Российской Федерации информации, необходимой для декодирования принимаемых, передаваемых, доставляемых и (или) обрабатываемых электронных сообщений пользователей информационно-телекоммуникационной сети “Интернет”».

на основании судебного решения[13]. Для доступа же к метаданным решения суда не требуется: как и в случае с IP-адресами, тайна корреспонденции на них не распространяется.

Следует, однако, подчеркнуть, что метаданные о переписке «могут дать даже еще более полное представление о поведении человека, его социальных отношениях, личных предпочтениях и личности, чем то, что можно было бы узнать из самого содержания частного общения»[14]. По этой причине оборот метаданных также не может быть произвольным и должен осуществляться в рамках установленных законом процедур, гарантирующих уважение частной жизни индивида – хотя и не обязательно предполагающих обязательный судебный контроль. Примечательно, что даже Европейский суд по правам человека признал отсутствие безусловной необходимости получения судебного решения для доступа государства к информации о действиях индивидов в Интернете, если только такая информация не составляет тайну корреспонденции. В то же время Суд подчеркнул, что несудебные органы, принимающие соответствующие решения, должны быть в достаточной степени независимыми от органов, осуществляющих скрытое наблюдение (*surveillance*) за лицами (Watt 2017: 789).

В научной литературе высказываются опасения в связи с появлением у государств возможностей для массового, неизбирательного наблюдения за всеми лицами (в том числе за собственными гражданами) на основе цифровых следов, получаемых от администраций крупных интернет-сервисов (Watt 2017; Westerlund et al. 2021). Эти опасения не лишены оснований: распространение Интернета и появление технологий обработки больших объемов информации (*Big Data*) позволило правительствам и разведкам получать от технологических компаний данные обо всех пользователях глобальной Сети. Например, зарегистрированные в США интернет-гиганты сотрудничают с Агентством национальной безопасности, предоставляя ему данные о пользователях со всего мира в рамках программы массового цифрового слежения *PRISM* (Савельев 2015: 51; Watt 2017: 774). Неудивительно, что после раскрытия Эдвардом Сноуденом в 2013 г. информации о программе и последовавших за этим заявлений должностных лиц США, вынужденных признать ее существование, правительства многих стран стали стремиться оградить своих граждан от слежки со стороны американских спецслужб. В Европейском союзе разоблачения Сноудена послужили катализатором скорейшего принятия и введения в действие Общего регламента ЕС о защите данных (*GDPR*), а также выработки новых принципов сотрудничества Евросоюза и США по вопросам защиты персональных данных граждан ЕС (*Privacy Shield* с 2016 г. и *Data Privacy Framework* – с 2023 г.).

[13] Определение Апелляционной коллегии Верховного Суда РФ от 9 августа 2018 г. № АПЛ18-298.

[14] Право на неприкосновенность личной жизни в цифровой век: Доклад Управления Верховного комиссара Организации Объединенных Наций по правам человека от 30 июня 2014 г. № A/HRC/27/37. URL: https://documents.un.org/doc/undoc/gen/g14/068/73/pdf/g1406873.pdf?token=oQO8SXo74siKBBkNRL&fe=true (дата обращения: 20.05.2024).

Россия, также стремясь ограничить доступ США к цифровым следам, оставляемым российскими гражданами, не стала искать компромиссов с заокеанским партнером, а вслед за Китаем выбрала подход, основанный на принципе государственного суверенитета в информационном пространстве. «Цифровой суверенитет» реализуется, в частности, через требования «приземления» информационных баз с данными о россиянах. Так, персональные данные граждан Российской Федерации начиная с 2015 г. должны храниться, накапливаться и извлекаться с использованием баз данных, находящихся на территории России; трансграничная передача персональных данных возможна лишь с соблюдением условий, предусмотренных Законом о персональных данных. Требования размещения баз данных на территории РФ предъявляются и к действующим в России организаторам распространения информации, в том числе к организаторам сервисов обмена мгновенными сообщениями (мессенджеров). Согласно Закону об информации, исключительно в России должны размещаться технические средства информационных систем, используемых государственными органами и органами местного самоуправления. Владельцами предназначенных для использования на территории России сервисов размещения объявлений, аудиовизуальных сервисов («онлайн-кинотеатров»), а также сервисов авторизации пользователей на сайтах могут быть только российские граждане и юридические лица. В русло суверенизации Интернета и ограничения доступа американских спецслужб к данным о россиянах укладывается и ограничение доступа на территории России к зарегистрированным в США социальным сетям «X» (бывший *Twitter*) и *LinkedIn* в связи с отказом их администраций выполнять требования российского законодательства о «приземлении», а также запрет социальных сетей *Facebook* и *Instagram*[15] – хотя и по иным основаниям.

Впрочем, оправданное с моральной и юридической точек зрения воспрепятствование той или иной страной доступу иностранных (прежде всего американских) разведывательных служб к цифровым следам, оставляемым в Интернете своими гражданами, автоматически не дает ей оснований самой устанавливать тотальную цифровую слежку за собственными гражданами. Как отмечалось выше, предусматриваемые законом ограничения права на неприкосновенность частной жизни должны быть необходимыми (преследовать законную цель) и не иметь чрезмерного характера. Законность, необходимость и соразмерность как критерии правомерности всякого ограничения права закреплены в ч. 3 ст. 55 Конституции Российской Федерации. Государство, согласно ст. 2 Конституции РФ, обязано признавать, соблюдать и защищать права и свободы человека и гражданина. Конституционный Суд РФ не раз подчеркивал, что устанавливаемые законом ограничения прав и свобод не должны носить недифференцированный характер и распространяться на значительно более широкий круг лиц,

[15] Социальные сети *Facebook* и *Instagram* принадлежат компании *Meta Platforms Inc.*, признанной экстремистской, и запрещены на территории Российской Федерации.

чем это необходимо для достижения целей такого ограничения[16]. Применительно к использованию цифровых следов граждан при осуществлении государством своих функций это означает недопустимость сбора и обработки чрезмерного объема данных о слишком широком круге лиц, а также массовой слежки за пользователями – особенно тех, кто не подозревается в совершении преступлений и не представляет непосредственной угрозы безопасности.

Несмотря на явно выраженное намерение конституционного законодателя не допустить массового и неизбирательного ограничения неприкосновенности частной жизни, положения специальных законов оставляют довольно большой простор для получения органами безопасности и органами, осуществляющими оперативно-разыскную деятельность, доступа к цифровым следам российских граждан. Согласно п. 2 с. 2 ст. 7 Федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» одним из достаточных оснований для проведения оперативно-разыскных мероприятий может служить наличие у соответствующего органа сведений о «событиях или действиях (бездействии), создающих угрозу государственной, военной, экономической, информационной или экологической безопасности Российской Федерации». Пространность данной формулировки позволяет осуществлять оперативно-разыскные мероприятия в виде получения компьютерной информации в отношении широкого круга пользователей интернет-сервисов – в том числе тех, кто не является источником угроз.

Еще больше усмотрения предоставлено Федеральной службе безопасности. Пункт «м» ст. 13 Федерального закона от 3 апреля 1995 г. № 40-ФЗ «О Федеральной службе безопасности» предусматривает право органов ФСБ России получать на безвозмездной основе от любых организаций «информацию, необходимую для выполнения возложенных на органы федеральной службы безопасности обязанностей». К обязанностям ведомства Закон, в свою очередь, относит добычу разведывательной информации «в интересах обеспечения безопасности Российской Федерации, повышения ее экономического, научно-технического и оборонного потенциала», информации о событиях или действиях, создающих угрозу терроризма; принятие мер в области противодействия коррупции, незаконному обороту оружия и наркотиков, контрабанде и т. д. В совокупности с довольно простой процедурой направления запросов на предоставление метаданных (не предполагающей ни судебного решения, ни контроля со стороны какого-либо другого органа государственной власти) предельно широкие основания получения информации создают практически безграничные возможности доступа государства к цифровым следам пользователей российских

[16] См., напр.: Постановление Конституционного Суда РФ от 17 мая 1995 г. № 5-П «По делу о проверке конституционности статьи 12 Закона СССР от 9 октября 1989 года "О порядке разрешения коллективных трудовых споров (конфликтов)" (в редакции от 20 мая 1991 года) в части, запрещающей проведение забастовок работниками гражданской авиации, в связи с жалобой Профсоюза летного состава Российской Федерации».

интернет-сервисов. Если добавить к этому цифровые следы, оставляемые в банках и платежных сервисах, у операторов связи, в транспортных организациях, в системах типа «умный город», при оформлении и использовании электронных средств идентификации (к которым у государственных органов также есть доступ) – получится массив данных, способный рассказать едва ли не все о жизни каждого человека.

Впрочем, оценить масштабы наблюдения за индивидами со стороны российских правоохранительных органов и органов безопасности при помощи цифровых следов не представляется возможным: информация о количестве запросов не раскрывается. Но важным в данном случае является не то, осуществляют или нет массовое слежение за гражданами органы безопасности и органы, осуществляющие оперативно-разыскную деятельность, а то, предусматривает ли закон достаточные гарантии, не допускающие подобных практик. Законодательство Российской Федерации таких гарантий не содержит. Вместе с тем важной гарантией защиты от неизбирательной «цифровой слежки» могло бы стать установление в законодательстве требования о раскрытии количества запросов, направляемых администрациям российских интернет-сервисов правоохранительными органами и органами безопасности РФ. Механизмом контроля могло бы быть и санкционирование запросов надзорным органом – например, прокуратурой, к задачам которой относится, в частности, надзор за соблюдением прав и свобод человека и гражданина.

В зарубежной литературе высказывается точка зрения, что вероятность массового цифрового слежения снижает уровень доверия граждан к правоохранительным органам и органам безопасности (Westerlund et al. 2021). В российском контексте данная гипотеза не получает подтверждения. По данным ВЦИОМ, доверие к полиции растет на протяжении последних лет: и в 2023 г. 66% опрошенных россиян указали, что доверяют полиции (в 2022 г. уровень доверия составлял 62%). Наиболее высокий уровень доверия к полиции – у молодежи и у высокообеспеченных граждан (до 75% опрошенных)[17]. Работу служб госбезопасности большинство россиян также оценивает положительно: согласно данным Фонда «Общественное мнение» по результатам социологического исследования, проведенного в 2018 г., 66% опрошенных россиян указали, что положительно оценивают деятельность спецслужб[18]. При этом говорить о том, что российские интернет-пользователи безразлично относятся к сохранности своих данных, нельзя: в 2024 г. 68 % опрошенных пользователей глобальной Сети указали, что опасаются за сохранность личной информации в Интернете[19]. Вместе с тем,

[17] Профессия: полицейский. URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/professija-policeiskii (дата обращения: 20.05.2024).

[18] Отношение к российским службам государственной безопасности. URL: https://bd.fom.ru/pdf/d04gb2018.pdf (дата обращения: 20.05.2024).[40] Там же. П. 3 мотивировочной части.

[19] Цифровая самооборона. URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/cifrovaja-samooborona (дата обращения: 20.05.2024).

по данным проведенного НИУ ВШЭ в 2020 г. исследования, 36 % опрошенных согласились с тем, что их не беспокоит, что их действия в Интернете кем-то записываются и анализируются (при этом более половины опрошенных все же не согласились с этим утверждением, а каждый десятый затруднился с ответом)[20]. Такие результаты социологических исследований могут свидетельствовать о том, что российские интернет-пользователи одобряют действия правоохранительных органов и спецслужб, в том числе связанные с получением доступа к их личной информации во имя безопасности, либо не видят в этом существенных угроз для своей приватности. Возможно, сказывается и то, что значительное число интернет-пользователей (по данным некоторых исследований – до 84 %) демонстрируют цифровой пессимизм: они «чувствуют бессилие перед возрастающими рисками утраты контроля над их данными в сети»[21]. Во всяком случае действия государственных органов по контролю интернет-пользователей обретают в глазах россиян легитимность. Несмотря на высказанное выше предложение законодательно закрепить гарантии недопустимости массового цифрового слежения, следует констатировать, что в российском обществе устойчивый запрос на изменение законодательного регулирования в этой части в настоящее время не сформирован.

Если доступ государства к цифровым следам человека еще можно объяснить интересами национальной безопасности, то произвольное использование цифровых следов коммерческими организациями в собственных целях вряд ли может иметь убедительное юридическое обоснование. Владельцы крупных интернет-сервисов обладают технической возможностью контролировать действия своих пользователей, сопоставимой с возможностями государств. Администрации маркетплейсов и торговых сетей знают о заказах и поисковых запросах покупателей, владельцы социальных сетей – об интересах пользователей и о связях между ними, а поставщикам услуг электронной почты и сервисов коротких сообщений доступна информация из переписки пользователей. Так, еще в 2015 г. в ходе рассмотрения одного из дел Московским городским судом было установлено, что ООО «Гугл» – российское юридическое лицо компании *Google* – «проводит мониторинг в том числе электронных писем» с целью размещения контекстной рекламы на страницах электронной почты *Gmail* исходя из содержания писем конкретного пользователя. Суд посчитал такие действия нарушающими ч. 2 ст. 23 Конституции РФ, гарантирующей право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений[22].

В отличие от государств, которые могут законодательно требовать предоставление им доступа к цифровым следам интернет-пользователей

[20] Готовы ли пользователи рунета делиться персональными данными? URL: https://issek.hse.ru/news/450602433.html (дата обращения: 20.05.2024).

[21] Там же.

[22] Апелляционное определение Московского городского суда от 16 сентября 2015 г. по делу № 33-30344. URL: https://www.mos-gorsud.ru/mgs/services/cases/appeal-civil/details/0715f6a5-4062-4baa-a7c2-45a4c178f4e0 (дата обращения: 20.05.2024).

в публичных интересах, администрации интернет-сервисов получают право обрабатывать оставленные пользователями данные только с их согласия, в том числе на условиях, указанных в пользовательских соглашениях и политиках конфиденциальности. В литературе, однако, справедливо критикуется институт информированного согласия с точки зрения его способности защитить данные о пользователях в эпоху «больших данных». Как отмечает А.И. Савельев, в момент получения согласия невозможно представить исчерпывающий объем информации о возможных способах и целях обработки данных, сам же субъект, дающий согласие, не всегда может адекватно воспринять информацию (Савельев 2015: 55). К тому же около половины пользователей вообще не читают юридические документы, размещаемые на сайтах, в том числе политики конфиденциальности, еще 8% не знают о существовании таких документов (Назаров 2022: 99). Поэтому согласие на деле оказывается не таким уж «информированным». Скорее оно представляет собой рутинную процедуру, осуществляемую пользователем, который понимает, что для достижения результата (регистрации на сайте, активации приложения, оформления заказа в интернет-магазине и т.д.) он вынужден такое согласие дать.

С учетом возможности мгновенного тиражирования и передачи данных и существования огромного множества организаций, осуществляющих сбор, передачу и обработку персональной информации, индивид не способен взаимодействовать с каждой из них и отслеживать использование ею оставленных им когда-то цифровых следов. Даже если цели и способы обработки предоставляемой пользователем информации определены в пользовательском соглашении или политике конфиденциальности и не предполагают передачу полученных данных третьим лицам, на практике проследить дальнейшее движение цифровых следов, в том числе их попадание к другим лицам или использование за рамками первоначально очерченных целей, практически невозможно. Этим часто пользуются поставщики различных электронных услуг, предоставляющие имеющиеся у них пользовательские данные банкам и другим организациям, а также осуществляющие обработку имеющихся у них цифровых следов для решения собственных коммерческих задач, в том числе для продвижения своих услуг и позиционирования на рынке.

Примеры подобного использования цифровых следов нашли подтверждение в судебной практике. Например, в решении по делу А40-14902/2016 арбитражным судом было установлено, что интернет-провайдер предоставлял технические данные о пользовательских устройствах и сведения о просматриваемых активными пользователями веб-страницах (“*clickflaw*”) организациям-партнерам без согласия пользователей. А в деле А40-18827/2017 арбитражными судами рассматривался спор между администрацией социальной сети и правообладателем сервиса, осуществляющего автоматизированный сбор и анализ данных открытых аккаунтов пользователей этой социальной сети с целью последующего предоставления полученных результатов заинтересованным лицам, в том числе Национальному банку кредитных историй.

Одним из механизмов, позволяющих пользователям ограничить оборот связанной с ними информации в Интернете, является т.н. «право на забвение». Однако содержание данного права в России существенно отличается от того, как оно понимается, в частности, в Европейском союзе. Согласно ст. 17 GDPR под «правом на забвение» (“*right to be forgotten*”) понимается право субъекта персональных данных требовать от контроллера данных «незамедлительного удаления» персональных данных – например, при отзыве согласия на обработку или при исчерпании цели, с которой производилась обработка. Указанное право распространяется на любые сведения, относящиеся к субъекту данных, в том числе содержащиеся в цифровых следах. В России же закон «О персональных данных» не предусматривает права на удаление персональных данных в качестве самостоятельного права субъекта данных. В отдельных случаях закреплена лишь обязанность оператора прекратить обработку персональных данных – например, при отзыве субъектом согласия на обработку персональных данных, если при этом отсутствуют иные основания для их обработки, или при выявлении факта неправомерной обработки (ст. 21). «Правом на забвение» в России принято называть возможность лица требовать от оператора поисковой системы исключения из поисковой выдачи ссылок на интернет-страницы, содержащие неактуальную или недостоверную информацию о нем или распространяемую с нарушением закона (ч. 1 ст. 10.3 Закона об информации). Очевидно, что и содержание права, и механизм его осуществления, и правовые последствия здесь совсем иные. Удаления сведений о заявителе в данном случае не происходит: исключается лишь возможность поиска таких сведений, размещенных в открытом доступе, посредством поисковой системы. Сама же информация о лице остается доступной для использования (Карасев и др. 2019: 104-105).

Несмотря на периодически возникающие споры, связанные с неправомерной обработкой цифровых следов человека частными субъектами, отечественное законодательное регулирование в этой сфере остается крайне фрагментарным и распространяется в основном лишь на те сведения, которые относятся к персональным данным. Законодательной новеллой стало появление в Законе об информации статьи 10.2-2 (введена Федеральным законом от 31 июля 2023 г. № 408-ФЗ), регулирующей отношения по использованию т.н. рекомендательных технологий. В основе рекомендательных технологий лежат инструменты предикативной аналитики, позволяющей прогнозировать посредством интеллектуального анализа данных поведение субъекта на основе анализа его предыдущих действий, а также поведения других субъектов со схожими характеристиками (Рувинский 2023: 129). Если на интернет-сайте используются рекомендательные технологии (например, на маркетплейсах, предлагающих покупателю «рекомендуемые товары», или на новостных агрегаторах, формирующих подборку новостей для конкретного пользователя), владелец сайта должен предупредить об этом пользователя, проинформировав его о том, какие сведения берутся для формирования индивидуальных рекомендаций и какие методы и процессы сбора и обработки этих сведений применяются. Впрочем, закон

не предусматривает права пользователя отказаться от использования в отношении него рекомендательных технологий или запретить обрабатывать те или иные сведения о нем. Вероятно, цифровые следы – слишком ценная для бизнеса и государства информация, чтобы позволить индивиду выбирать по своему усмотрению – делиться ею или нет.

Заключение. Цифровые следы как явление, обусловленное цифровизацией общества и развитием технологий «больших данных», открыли широкие возможности для государств и коммерческих структур «подсмотреть» за частной жизнью каждого индивида и использовать полученную информацию для решения собственных задач. Чем активнее пользуются граждане интернет-сервисами, чем глубже проникают информационные технологии в повседневную жизнь каждого человека, тем больше остается цифровых следов. И тем сильнее соблазн увидеть то, на что прежде смотреть не дозволялось. При всем многообразии цифровых следов человека и различиях в правовом режиме их отдельных разновидностей потребность в защите неприкосновенности частной жизни человека обусловливает необходимость взглянуть на них как на целостное явление, требующее согласованного механизма законодательного регулирования.

В литературе высказываются в целом справедливые суждения, что в цифровой век приватность, а тем более анонимность становятся во многом относительными (Кузнецова 2020; Назаров 2022). Отчасти это действительно так: частная жизнь человека в цифровом мире не станет снова такой, какой она была до появления Интернета. Однако ни цифровизация общества, ни стремление государств и частных структур использовать ее преимущества не должны нивелировать ценность естественных прав человека, в том числе на сохранение определенной степени приватности. В цифровом мире неприкосновенность частной жизни становится уязвимой как никогда ранее: жизнедеятельность каждого человека, его поступки, интересы, пристрастия, отношения, взгляды, убеждения и даже мысли могут быть раскрыты, проанализированы и оценены по оставленным им цифровым следам. Причем многие цифровые следы оставляются неосознанно или случайно; иногда оставление цифрового следа является вынужденным – например при получении государственной услуги в электронной форме, при обращении в банк или при покупке билета на поезд или самолет. На основе данных, полученных из цифровых следов, может быть смоделирован «цифровой двойник» человека, его «цифровая тень». Посредством систем интеллектуального анализа данных может быть спрогнозировано его поведение, а рекомендательные технологии определят его дальнейшие поступки. В результате человек в определенном смысле перестает принадлежать себе, а его частную жизнь уже нельзя назвать в полной мере «частной».

Задача законодательного регулирования состоит в том, чтобы сохранить ценность частной жизни и установить справедливые гарантии охраны ее неприкосновенности. В цифровом мире сделать это крайне нелегко: пока ни одно государство не создало удовлетворительного правового механизма, который в достаточной степени охранял бы частную жизнь индивидов

от постороннего вторжения в условиях новой реальности. Вероятно, первым шагом к установлению справедливого баланса должно быть признание того, что любой цифровой след человека является источником информации о его частной жизни. Из этой презумпции должно исходить правовое регулирование сбора, хранения, передачи и использования всех цифровых данных, так или иначе связанных с личностью. Эту же презумпцию должны использовать суды при рассмотрении споров, связанных с обработкой цифровых следов.

В целях сохранения определенной степени контроля индивида над своей приватностью представляется необходимым, чтобы владельцы интернет-сайтов не просто информировали пользователей о сборе технической информации посредством «куки»-файлов или об использовании рекомендательных технологий, а предоставляли бы им возможность отказаться от сообщения тех или иных сведений или в целом от применения инструментов цифрового профилирования. Одновременно следует кратно повысить размеры штрафов для владельцев крупных интернет-сервисов в случае утечки пользовательских данных или их незаконной передачи другим лицам. В настоящее время негативные финансовые последствия утечек несопоставимо мизерные в сравнении с теми доходами, которые интернет-гиганты получают от использования цифровых следов.

Значительно более деликатным является вопрос о пределах доступа государства к цифровым следам, оставленным своими гражданами – как в Интернете, так и при взаимодействии с другими компьютерными сетями и информационными системами. Здесь сталкиваются разнонаправленные интересы: с одной стороны, интерес индивида в сохранении определенной степени приватности, с другой – публичный интерес, связанный с общественной потребностью в безопасности. В любом государстве органы, обеспечивающие безопасность, действуют на основе принципа конспирации и сочетают в своей работе методы гласного и негласного получения информации. Их деятельность по сбору и анализу цифровых следов граждан по понятным причинам, вероятно, никогда не станет полностью публичной и открытой. Однако это не должно влечь за собой вседозволенность и произвол, в том числе бесконтрольное массовое тайное слежение за гражданами. Поэтому правовое регулирование в этой сфере должно предусматривать механизмы подотчетности и контроля.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

Буйнов Д.О. 2023. Развитие научных подходов к понятию «цифровые следы» как объекта экспертного исследования // Законы России: опыт, анализ, практика. № 3. С. 17–22.

Виловатых А.В. 2020. Манипулирование социальным поведением в условиях цифровой среды // Научный журнал «Дискурс-Пи». Т. 17, № 2. С. 149–164. DOI 10.24411/1817-9568-2020-10210

Виноградова Е.В. и др. 2021. Цифровой профиль: понятие, механизмы регулирования и проблемы реализации / Е.В. Виноградова, Т.А. Полякова, А.В. Минбалеев // Правоприменение. Т. 5, № 4. С. 5–19. DOI 10.52468/2542-1514.2021.5(4).5-19

Даниленко И.А., Васильев Н.В. 2020. Соблюдение конституционных прав личности на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки, почтовых, телеграфных и иных сообщений при осмотре мобильного устройства (российский и зарубежный опыт) // Вестник Университета имени О.Е. Кутафина (МГЮА). № 10. С. 150–157. DOI 10.17803/2311-5998.2020.74.10.150-157

Дупан (Гутникова) А.С. (ред.) 2016. Новая парадигма защиты и управления персональными данными в Российской Федерации и зарубежных странах в условиях развития систем обработки данных в сети Интернет / под ред. А.С. Дупан (Гутниковой). Москва : Издат. дом Высш. шк. экономики. 344 с.

Жарова А.К. 2016. О соотношении персональных данных с IP-адресом. Российский и зарубежный опыт // Вестник УрФО. Безопасность в информационной сфере. № 1. С. 61–67.

Иванова К.А. 2020. Право граждан на защиту геолокации и конфиденциальность в сети Интернет // Актуальные проблемы российского права. Т. 15, № 9. С. 32–38. DOI 10.17803/1994-1471.2020.118.9.032-038

Карасев А.Т. и др. 2019. Цифровизация правоотношений и ее влияние на реализацию отдельных конституционных прав граждан в Российской Федерации / А.Т. Карасев, О.А. Кожевников, В.А. Мещерягина // Антиномии. Т. 19, №. 3. С. 99–119. DOI 10.24411/2686-7206-2019-10016

Кузнецова С.С. 2020. Право на анонимность в сети Интернет: актуальные вопросы реализации и защиты // Российское право: образование, практика, наука. № 5. С. 33–41. DOI 10.34076/2410-2709-2020-5-33-41

Лазарева Л.В. 2023. Цифровые следы: понятие, нормативное регулирование, исследование // Расследование преступлений: проблемы и пути их решения. № 3. С. 129–136. DOI 10.54217/2411-1627.2023.41.3.015

Назаров М.М. 2022. Приватность в сети и цифровая покорность: исследование аудитории интернета // Вестник Института социологии. Т. 13, № 3. С. 87–107. DOI 10.19181/vis.2022.13.3.832

Романовский Г.Б. 2001. Право на неприкосновенность частной жизни. Москва : МЗ-Пресс. 312 с.

Ромашов П.А. 2019. К вопросу о праве на неприкосновенность частной жизни в цифровой век // Пермский юридический альманах. № 2. С. 103–118.

Рувинский Р.З. 2023. Регулирование на основе данных: от верховенства права к публичным программам лояльности // Антиномии. Т. 23, № 1. С. 123–147. DOI 10.17506/26867206_2023_23_1_123

Савельев А.И. 2015. Проблемы применения законодательства о персональных данных в эпоху «больших данных» (Big Data) // Право. Журнал Высшей школы экономики. № 1. С. 43–66.

Талапина Э.В. 2018. Защита персональных данных в цифровую эпоху: российское право в европейском контексте // Труды Института государства и права Российской академии наук. Т. 13, № 5. С. 117–150.

Фатьянов А.А. 2008. Воля как правовая категория // Государство и право. № 4. С. 5–12.

Черданцев А.Ю. 2019. Цифровые следы как криминалистический феномен // Вестник Академии Следственного комитета Российской Федерации. № 4. С. 178–180.

Watt E. 2017. The Right to Privacy and the Future of Mass Surveillance // The International Journal of Human Rights. Vol. 21, № 7. P. 773–799. DOI 10.1080/13642987.2017.1298091

Westerlund M. et al. 2021. The Acceptance of Digital Surveillance in an Age of Big Data / M. Westerlund, D.A. Isabelle, S. Leminen // Technology Innovation Management Review. Vol. 11, iss. 3. P. 32–44.

References

Buinov D.O. Advancement of Scientific Approaches to Definition "Digital Footprints" as an Object of Forensic Investigation, *Zakony Rossii: opyt, analiz, praktika*, 2023, no. 3, pp. 17–22. (in Russ.).

Cherdantsev A.Y. Digital Traces as a Criminalistic Phenomenon, *Vestnik Akademii Sledstvennogo komiteta Rossiiskoi Federatsii*, 2019, no. 4, pp. 178–180. (in Russ.).

Danilenko I.A., Vasiliev N.V. Compliance with the constitutional rights of an individual to privacy, personal and family secrets, secrecy of correspondence, postal, telegraph and other messages when examining a mobile device (Russian and foreign experience), *Courier of Kutafin Moscow State Law University (MSAL)*, 2020, no. 10, pp. 150–157. DOI 10.17803/2311-5998.2020.74.10.150-157 (in Russ.).

Dupan (Gutnikova) A.S. (ed.) *Novaya paradigma zashchity i upravleniya personal'nymi dannymi v Rossiyskoy Federatsii i zarubezhnykh stranakh v usloviyakh razvitiya sistem obrabotki dannykh v seti Internet* [A new paradigm of personal data protection and management in the Russian Federation and foreign countries in the context of the development of data processing systems on the Internet], Moscow, Izdatel'skiy dom Vysshey shkoly ekonomiki, 2016, 344 p. (in Russ.).

Fatyanov A.A. *Volya kak pravovaya kategoriya* [Will as a legal category], *State and Law*, 2008, no. 4, pp. 5–12. (in Russ.).

Ivanova K.A. Citizens' Right to Protection of Geolocation and Privacy on the Internet, *Actual problems of Russian law*, 2020, vol. 15, no. 9, pp. 32–38. DOI 10.17803/1994-1471.2020.118.9.032-038 (in Russ.).

Karasev A.T., Kozhevnikov O.A., Misuragina V.A. Digitalization of legal relations and its impact on the implementation of certain constitutional rights of citizens in the Russian Federation, *Antinomies*, 2019, vol. 19, iss. 3, pp. 99–119. DOI 10.24411/2686-7206-2019-10016 (in Russ.)

Kuznetsova S.S. The right to anonymity on the Internet: currend issues of implementation and protection, *Russian law: education, practice, research*, 2020, no. 5, pp. 33–41. DOI 10.34076/2410-2709-2020-5-33-41 (in Russ.).

Lazareva L.V. Digital Footprints: Concept, Regulation, Research, *Rassledovanie prestuplenii: problemy i puti ikh resheniia*, 2023, no. 3, pp. 129–136. DOI 10.54217/2411-1627.2023.41.3.015 (in Russ.).

Nazarov M.M. Online Privacy and Digital Submission: A Study of the Internet Audience, *Bulletin of the Institute of Sociology*, 2022, vol. 13, no. 3, pp. 87–107. DOI 10.19181/vis.2022.13.3.832 (in Russ.).

Romanovsky G.B. *Pravo na neprikosnovennost' chastnoy zhizni* [The right to privacy], Moscow, MZ-Press, 2001, 312 p. (in Russ.).

Romashov P.A. Privacy Issues in the Digital Age, *Perm Legal Almanac*, 2019, no. 2, pp. 103–118. (in Russ.).

Ruvinsky R.Z. Data-Driven Regulation: From the Rule of Law to Public Loyalty Programs, *Antinomies*, 2023, vol. 23, iss. 1, pp. 123–147. DOI 10.17506/26867206_2023_23_1_123 (in Russ.).

Savelyev A.I. The Issues of Implementing Legislation on Personal Data in the Era of Big Data, *Law. Journal of the Higher School of Economics*, 2015, no. 1, pp. 43–66. (in Russ.).

Talapina E.V. Personal Data Protection in the Digital Age: Russian Law in the European Context, *Proceedings of the Institute of State and Law of the RAS*, 2018, vol. 13, no. 5, pp. 117–150. (in Russ.).

Vilovatykh A.V. Manipulation of Social Behavior Under the Digitalization of Social Environment, *Discourse-P*, 2020, vol. 17, no. 2, pp. 149–164. DOI 10.24411/1817-9568-2020-10210 (in Russ.).

Vinogradova E.V., Polyakova T.A., Minbaleev A.V. Digital profile: concept, regulatory mechanisms and problems of implementation, *Law Enforcement Rewiew*, 2021, vol. 5, no. 4, pp. 5–19. DOI 10.52468/2542-1514.2021.5(4).5-19 (in Russ.).

Watt E. The Right to Privacy and the Future of Mass Surveillance, *The International Journal of Human Rights*, 2017, vol. 21, no. 7, pp. 773–799. DOI 10.1080/13642987.2017.1298091

Westerlund M., Isabelle D.A., Leminen S. The Acceptance of Digital Surveillance in an Age of Big Data, *Technology Innovation Management Review*, 2021, vol. 11, iss. 3, pp. 32–44.

Zharova A.K. The Relation of Personal Datawith the IP Address. A Study Russian's and Foreign Experience, *Journal of the Ural Federal District. Information Security*, 2016, no. 1, pp. 61–67. (in Russ.).

ИНФОРМАЦИЯ ОБ АВТОРЕ

Артур Николаевич Мочалов
кандидат юридических наук, доцент, доцент кафедры конституционного права Уральского государственного юридического университета им. В.Ф. Яковлева, г. Екатеринбург, Россия;
ORCID: 0000-0003-2502-559X;
ResearcherID: S-3195-2016;
SPIN-код: 9766-7829;
E-mail: artur.mochalov@usla.ru

INFORMATION ABOUT THE AUTHOR

Artur N. Mochalov
Candidate of Law, Associate Professor, Department of Constitutional Law, Ural State Law University named after V.F. Yakovlev, Ekaterinburg, Russia;
ORCID: 0000-0003-2502-559X;
ResearcherID: S-3195-2016;
SPIN-код: 9766-7829;
E-mail: artur.mochalov@usla.ru