УДК 342

ПРАВОВОЙ АСПЕКТ ЦИФРОВЫХ СЛЕДОВ КАК СТРУКТУРНОГО ЭЛЕМЕНТА ЦИФРОВОЙ ЛИЧНОСТИ

А. В. КЛЕБАНОВ
(Представлено: канд. юрид. наук, доц. И. В. ШАХНОВСКАЯ)

В статье рассматриваются вопросы определения цифрового следа личности, исследуются имеющиеся научные подходы в юридических науках по данной проблематике. Автор проводит анализ международного и национального законодательства, являющегося основой для определения цифрового следа как элемента структуры цифровой личности в целом. В статье предлагается классификация цифровых следов на активные и пассивные, а также обосновывается «криминалистическое» и «комплексное» понимание данной правовой категории.

С возникновением и распространением глобальной сети человечество вступило в новую эру информационных технологий. Интернет значительно упростил нашу жизнь, предоставив беспрецедентные возможности для обмена информацией, общения, обучения и ведения бизнеса. Однако с его развитием возникли и новые проблемы, связанные с защитой личных данных, конфиденциальности и прав пользователей в цифровом пространстве. В связи с этим, в современной юриспруденции всё чаще фигурирует такое понятие как «цифровой след» личности. В основном этот термин используется в криминалистике при выявлении преступлений, связанных с киберпространством. Само определение «цифрового следа» имеет многогранное значение и различные трактовки, зависящие от подхода к рассмотрению искомого термина. В контексте данной статьи автор будет использовать «комплексный» подход, рассматривая цифровой след как структурный элемент цифровой личности человека.

Данный подход предполагает, что цифровым следом называется совокупность информации, оставляемой субъектом в виртуальном пространстве при совершении им каких-либо действий в интернет-среде [1, с. 19]. Существует несколько по своему характеру видов цифрового следа: активный цифровой след (пользователь сам оставляет информацию о себе и осознаёт это) и пассивный (данные о пользователе собираются и сохраняются непреднамеренно без воли субъекта, например, его история поиска) [2, с. 393]. Активный цифровой след формируется в результате осознанных действий пользователя, таких как публикации в социальных сетях, заполнение форм, отправка сообщений или оставление комментариев. Пользователь в этом случае осознаёт, что предоставляет определённую информацию о себе, и может частично контролировать её содержание и объем. Пассивный цифровой след, напротив, создаётся без прямого участия пользователя и зачастую без его ведома. Это могут быть данные о посещённых веб-сайтах, истории поиска, файлы cookie, данные о местоположении, IP-адрес и другая информация, автоматически собираемая и обрабатываемая различными сервисами и платформами. Важным аспектом пассивного цифрового следа является то, что пользователь не всегда может осознавать весь объём данных, которые собираются о нем, и тем более влиять на их последующее использование. Обе эти формы цифрового следа имеют правовые последствия, поскольку могут быть использованы для профилирования, анализа поведения или даже нарушения прав на конфиденциальность и частную жизнь. Ввиду этого цифровой след является одним из основополагающих элементов современной криминалистики в сфере киберпреступлений. Криминалистическая трактовка понятия «цифрового следа» представляет из себя следующее: «любая криминалистически значимая компьютерная информация, сведения (сообщения, данные), находящиеся в электронно-цифровой форме, зафиксированные на материальном носителе с помощью электромагнитных взаимодействий либо передающиеся по каналам связи посредством электромагнитных сигналов» [3, с. 172]. Данное определение ставит вопрос о новом понимании цифрового следа: учитывая, что цифровой след может существовать не только в цифровом пространстве, но и на материальном носителе, такой подход создаёт неопределённости во взаимодействии с цифровым следом. Некоторые авторы даже разделяют термин на две составных части: сам цифровой след (существующий на материальном носителе), а также его составная часть виртуальный след (существующий исключительно в виртуальном пространстве). Такое разграничение позволяет достаточно точно определить природу цифрового следа и способы взаимодействия с ним. Цифровой след, существующий на материальном носителе, содержит в себе данные, которые могут быть извлечены с физических устройств, таких как жесткие диски, флеш-накопители, серверы или другие виды носителей информации. Эти данные фиксируются и хранятся в виде файлов, логов и других структурированных записей, и их можно изучить с помощью традиционных методов компьютерной криминалистики. Виртуальный след, напротив, существует исключительно в онлайн-пространстве и включает в себя действия, которые происходят в реальном времени в сети: взаимодействия в социальных медиа, электронная переписка, веб-трафик, облачные хранилища и другие формы цифровой активности. Виртуальные

следы труднее поддаются фиксации и восстановлению, так как они могут быть быстро изменены или удалены, а доступ к ним часто требует специальных разрешений или сотрудничества с интернет-сервисами.

Вышеуказанное свидетельствует о сложностях правового регулирования взаимодействия с цифровыми следами, о необходимости в углубленном изучении и анализе правовых норм, связанных с деятельностью субъектов, направленной на получение информации о цифровых следах, ставит вопрос о некой черте, которая существует между безопасностью общества и правами человека, существующем в этом обществе. «Криминалистическая» трактовка цифрового следа является наиболее развитой в научном плане, а также распространённой как на бытовом, так и на юридическом уровне. Цифровой след играет важную роль при расследовании киберпреступлений. Получаемая при его рассмотрении информация может использоваться для доказательства в суде, а также для профилактики и пресечения преступной деятельности в виртуальном пространстве. Что немаловажно, сбор и агрегация цифрового следа человека должна быть строго регламентирована законодательством, дабы (вспоминая о правах цифровой личности)[3] компенсировать урон правам и свободам человека в киберпространстве.

Правовая регулировка цифрового следа в законодательстве многих в первую очередь связана в первую очередь с персональными данными пользователя. Термин «цифровой след» в нормативных правовых актах не употребляется. Одним из наиболее известных нормативных правовых актов, который затрагивает процесс сбора информации о цифровых следах человека является Общий регламент о защите персональных данных, внедрённый в Европейском Союзе в 2018 году (далее – Регламент) [4]. Нормы Регламента устанавливают ограничения для субъектов-держателей веб-сайтов, а также иных лиц при сборе и обработке персональных данных пользователей. Наиболее примечательным в контексте данной работы моментом является статья 22 Регламента [4]. Норма регулирует автоматизированный сбор информации, и принятие решений на её основе, включая профилирование субъекта (любая форма автоматической обработки персональных данных, заключающаяся в использовании персональных данных для оценки определенных личных аспектов физического лица, в частности, для анализа или предугадывания аспектов его результативности в работе, его экономического положения, здоровья, личных предпочтений, интересов, надежности, поведения и перемещений) [5], устанавливает ограничения на использование пассивного цифрового следа, в частности, требование на согласие субъекта (пункт (C) части искомой статьи), возможность субъекта вмешиваться в процесс использования (часть 2 данной статьи). В случае нарушения прав и свобод, субъект может возразить против дальнейшей обработки своих персональных данных (статья 21 регламента), или воспользоваться указанным в данном акте «правом на забвение». Данное право регулируется статьёй 17 акта, оно заключается в возможности субъекта запросить удаления своих персональных данных у «контролёра» данных, при этом в статье указываются основания, при которых запрос обязан быть удовлетворён, например, незаконная обработка данных, исполнения целей, для которых эти данные обрабатывались и т.д. Вышеописанные нормы позволяют сделать вывод о стремлении законодателя сохранить баланс между обработкой данных для определённых целей и защитой прав и свобод субъектов. В определённом виде данные нормы повсеместно введены в информационные законодательства разных стран. Так, приводя более близкое к нашим странам законодательство, можно взять как пример Закон Республики Беларусь «О защите персональных данных». Данный закон также устанавливает права субъекта при обработке его персональных данных, имеет перечень мер, при которых возможна автоматизированная обработка данных без согласия субъекта (статья 6), регулирует право на отзыв своих персональных данных и их возможное удаление (статья 13) [5].

Таким образом, в эпоху стремительного развития информационных технологий и повсеместного использования глобальной сети Интернет цифровой след стал неотъемлемой частью жизни человека в цифровом пространстве. Исходя из анализа научных подходов можно выделить два типа цифровых следов – криминалистический и комплексный (которого и придерживается автор). Оба из них уникальны, хотя и имеют свои особенные черты. На наш взгляд, данные подходы могут быть интегрированы между собой, сохраняя как криминалистическую ценность цифрового следа, так и рассматривая его как составную часть цифровой личности человека. Современное правовое регулирование направлено на поддержание баланса, позволяя «контролёрам» информации собирать и агрегировать персональные данные пользователя (включая анализ его цифровых следов), но и предоставляя субъектам правовые возможности влиять на обработку этих данных. Законодательные нормы должны обеспечивать как безопасность общества в целом, так и защиту прав личности, формируя в то же время правовые рамки, которые бы позволяли эффективно использовать цифровые технологии при соблюдении интересов каждого человека.

ЛИТЕРАТУРА

1. Степанов, О.А, Степанов, М.М. Правовое регулирование генезиса цифровой личности [Электронный ресурс] / О.А Степанов, М.М. Степанов // Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации, г. Москва, Россия. – 2022. – С. 19–32.

2. Осанова, А.С. О проблемах обеспечения безопасности цифровой личности / А.С. Осанова // Актуальные проблемы авиации и космонавтики: сборник материалов VII Международной научно-практической конференции, посвященной Дню космонавтики: в 3 томах. Том 2; Под общей редакцией Ю. Ю. Логинова. Красноярск, 2021. – С. 393–395.
3. Переверзева Е. С., Комов А. В. Виртуальные и цифровые следы: новый подход в понимании // Вестник Санкт-Петербургского университета МВД России. – 2021. – № 1 (89). – С. 172–178.
4. Рассолов И. М. Право и Интернет. Теоретические проблемы. – Москва: Норма, 2009. – 383 с.
5. Общий регламент по защите данных (GDPR) [Электронный ресурс]: Регламент (ЕС) 2016/679 Европейского парламента и Совета от 27 апреля 2016 года о защите физических лиц в отношении обработки персональных данных и о свободном обращении таких данных. – Режим доступа: https://gdpr-text.com/ru/. – Дата доступа: 06.10.2024.
6. О персональных данных [Электронный ресурс]: Закон Республики Беларусь от 7 мая 2021 г. № 99-З с изм. и доп. от 1 июня 2022 г. // Национальный правовой Интернет-портал Республики Беларусь. – Режим доступа: https://pravo.by/document/?guid=12551&p0=H12100099. – Дата доступа: 14.10.2024.