УДК 343.98

Востриков Г.А.,
кандидат юридических наук,
старший преподаватель кафедры уголовного права и процесса
ФГБОУ ВО «Средне-Волжского института (филиала)
Всероссийского государственного университета юстиции
(РПА Минюста России)
Россия, г. Саранск
Бульдяева К.А.,
студент,
5 курс, факультет высшего образования
ФГБОУ ВО «Средне-Волжского института (филиала)
Всероссийского государственного университета юстиции
(РПА Минюста России)
Россия, г. Саранск

КРИМИНАЛИСТИЧЕСКИЕ И ПРОЦЕССУАЛЬНЫЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ ЦИФРОВЫХ СЛЕДОВ В РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ ПРОТИВ ЖИЗНИ И ЗДОРОВЬЯ

Аннотация: *В статье рассматривается роль цифровых следов как криминалистически значимых доказательств при расследовании преступлений против жизни и здоровья. Анализируются их уголовно-процессуальные и криминалистические аспекты. Особое внимание уделяется проблемам, связанным с использованием шифрования и анонимных сетей. Рассматривается влияние современных технологий на работу с цифровыми следами и сравниваются правовые подходы к их использованию в России и за рубежом.*

Ключевые слова: *цифровые следы, криминалистика, электронные доказательства, расследование преступлений, процессуальные аспекты, доказательственная ценность.*

Annotation: *The article examines the role of digital footprints as criminalistically significant evidence in the investigation of crimes against life and health. Their criminal procedural and criminalistic aspects are analyzed. Special attention is paid to the problems associated with the use of encryption and anonymous networks. The influence of modern technologies on working with digital footprints is considered and legal approaches to their use in Russia and abroad are compared.*

Keywords: *digital footprints, criminology, electronic evidence, crime investigation, procedural aspects, evidentiary value.*

Цифровой след представляет собой информацию, оставленную субъектом в информационно-технологической среде, которая может быть использована как криминалистически значимая. В контексте расследования преступлений против жизни и здоровья такие следы включают записи с видеонаблюдения, данные мобильной связи, метаданные сообщений и звонков, телеметрию и лог-файлы коммуникаций. Ученые отмечают, что цифровые следы становятся важной частью криминалистической деятельности в эпоху цифровизации [1, с. 146].

С позиций уголовно-процессуального права они выступают как вид электронных доказательств, играющих существенную роль в установлении фактов, например, местоположения участника, времени события, коммуникаций между сторонами и обстоятельств причинения вреда. При расследовании преступлений против жизни и здоровья цифровые следы позволяют восстановить путь перемещения подозреваемого или потерпевшего, зафиксировать момент коммуникации или отключения связи,

установить использование мобильных приложений, фиксирующих местоположение и время, а также проанализировать запись видеонаблюдения с места происшествия, предоставляя дополнительную версию или подтверждение действий [2, с. 47]. Они дополняют классические доказательства, но не заменяют их. Однако важно оценивать пределы, в которых цифровой след может быть отнесен к событию преступления, поскольку метаданные устройства отражают его пребывание в районе происшествия, но не всегда доказывают причинение вреда.

С криминалистической точки зрения цифровую информацию классифицируют на данные компьютерных носителей, сетевые логи, мобильные данные и метаданные [3, с. 251]. Фиксация, изъятие и исследование таких следов требуют соблюдения криминалистической тактики, включающей выемку носителей информации, создание копий, анализ журналов, восстановление удаленных данных и сопоставление с другими следами.

Критически важно соблюдать правовые и методические требования: обеспечение цепочки обращения доказательств, документирование каждого этапа и привлечение экспертов. В делах о преступлениях против жизни и здоровья это означает обеспечение сохранности устройств, исследование геолокационных данных и воспроизведение сообщений или звонков, связанных с преступлением [4, с. 105].

С процессуальной точки зрения использование цифровых следов регулируется уголовно-процессуальным законодательством РФ, однако исследователи отмечают недостаточную детализацию терминологии и порядка обращения с такими доказательствами в УПК РФ. Ключевое значение имеют законность получения, фиксирование, допустимость доказательств и неприкосновенность прав участников процесса [5, с. 565].

Судебная практика демонстрирует разный подход к природе цифровых доказательств. В Приговоре Ленинского районного суда г. Омска № 1-

536/2018 от 01.11.2018 по делу № 1-536/2018 цифровые доказательства сыграли ключевую и многослойную роль, став одним из краеугольных камней как обвинения, так и защиты.

Прежде всего, цифровые доказательства подтвердили мотив и характер угроз со стороны потерпевшего (В.А.А.). ФИО3 в своих показаниях неоднократно ссылался на то, что ему было известно об агрессивном поведении и угрозах В.А.А. от М.С.А. Цифровые доказательства, а именно переписка в социальной сети «Одноклассники», стали объективным и вещественным подтверждением этих слов. Судом были исследованы конкретные сообщения, в которых В.А.А. прямо угрожал ФИО3. Эти цифровые улики переводили заявления защиты из разряда голословных в разряд доказанных фактов. Они демонстрировали, что угрозы были реальными, конкретными и направленными именно на ФИО3, создавая у него обоснованные опасения за свою безопасность еще до ночи происшествия.

Кроме того, цифровые доказательства подтвердили факт наличия конфликтных отношений и агрессивного состояния потерпевшего. Даже те сообщения, которые суд не счел прямыми угрозами, помогали воссоздать психологический портрет В.А.А. и атмосферу напряженности, которая царила между ним, его бывшей женой и ФИО3.

Во-вторых, цифровые доказательства сыграли важную процессуальную роль в фиксации действий потерпевшей (В.А.А.) сразу после инцидента. Аудиозапись разговора В.А.А. с оператором скорой помощи, который был тщательно исследован. Это цифровое доказательство фиксировало первичную, непосредственную реакцию очевидца и косвенно подтверждало версию ФИО3 о том, что он действовал в состоянии обороны, а также то, что В.А.А. сама воспринимала происходящее именно как нападение на них с последующей обороной.

Помимо этого, суд не ограничился простым приобщением переписки и аудиозаписей. Было назначено и проведено специальное филологическое исследование, которое детально проанализировало смысл и контекст всех сообщений и разговоров. Эта экспертиза объективно установила наличие в переписке угроз в адрес ФИО3 и подтвердила, что слова В.А.А. в разговоре с оператором свидетельствуют о ее личном присутствии при событиях.

В итоге, хотя суд и квалифицировал действия ФИО3 как превышение пределов необходимой обороны, цифровые доказательства сыграли решающую роль в смягчении его участи. Они позволили суду установить исключительную противоправность и агрессивность поведения потерпевшего, что было прямо признано смягчающим обстоятельством. Без этих доказательств версия ФИО3 об угрозах могла бы остаться неподтвержденной, а картина произошедшего выглядела бы как бытовая драка между двумя мужчинами без предыстории [6].

В отличие от предыдущего дела в Апелляционном определении Верховного Суда РФ от 17.10.2013 № 50-АПУ13-26 цифровые доказательства не получили признания и не оказали существенного влияния на итоговое судебное решение. Так, К., признанный виновным в совершении преступлений, предусмотренных п. «з» ч. 2 ст. 105, п. «в» ч. 4 ст. 162 УК РФ, указывает на несоответствие вывода суда фактическим обстоятельствам дела, ссылаясь на то, что в ходе осмотра места происшествия не были изъяты планшетный компьютер и смартфон, содержащие сведения, подтверждающие его показания о наличии между ним и погибшей М. интимных отношений и факта приобретения потерпевшей в вечер убийства наркотического вещества. Защита и следствие представляли в суд электронные сообщения и логи интернет-активности, якобы подтверждающие вину подсудимого. Однако суд установил, что порядок их получения и фиксации нарушал процессуальные требования: отсутствовали сведения о времени и условиях изъятия информации, не было доказано, что

цифровые данные не подвергались изменениям после копирования, а лица, проводившие технические действия, не имели статуса специалистов, предусмотренного уголовно-процессуальным законом. Следовательно, в данном деле цифровые следы, хотя и имели потенциальную доказательственную значимость, были исключены из доказательственной базы по причине несоблюдения процессуальных гарантий их достоверности [7].

Среди проблем использования цифровых следов выделяют технические трудности, такие как шифрование устройств и сложность восстановления данных; процессуальные риски, включая нарушение порядка изъятия и отсутствие эксперта; вопросы достоверности, поскольку цифровой след может не отражать действие лица; а также законодательно-методологическую недостаточность. Неверное толкование цифровых следов в делах о преступлениях против жизни и здоровья может привести к ошибочной квалификации или неправильному установлению виновности.

Для эффективного использования цифровых следов следователю рекомендуется обеспечить раннюю фиксацию цифровых устройств и данных участников с составлением протокола изъятия, привлекать специалистов по цифровым следам для анализа и восстановления данных, сопоставлять цифровые следы с классическими доказательствами, документировать каждый этап работы с доказательствами, учитывать возможность манипуляции данными и подчеркивать ограничения цифровых следов в протоколах, а также разъяснять их техническую природу в суде [8, с. 60].

В целях оптимизации работы правоохранительных органов и обеспечения сохранности цифровых следов предлагаем внедрить универсальную модель управления цифровыми следами, которая представляет собой циклическую систему из шести этапов: сбор, классификация, оценка, контроль, реакция и обратная связь.

На первом этапе осуществляется идентификация и агрегирование всех доступных цифровых следов из различных источников – устройств, сетевых сервисов, социальных платформ. Далее данные классифицируются по ключевым параметрам (субъект, содержание, время, место, контекст), что обеспечивает их структурирование и сопоставимость. На этапе оценки анализируются ценность и риски следов, включая угрозы конфиденциальности, достоверность и репутационные последствия. Контроль подразумевает внедрение технических и организационных мер защиты, анонимизацию, ограничение доступа и соблюдение нормативных требований. Реакция включает практическое использование следов в аналитике и управлении либо нейтрализацию выявленных рисков. Завершающая стадия – обратная связь – предполагает анализ эффективности проведенных действий и корректировку процедур, что делает алгоритм адаптивным к изменяющимся технологическим и правовым условиям. Такой подход обеспечивает целостное, этически и юридически обоснованное управление цифровыми следами.

Использование криптографических методов шифрования и анонимных сетевых инфраструктур создает фундаментальные осложнения в процессе доказывания – как в смысле юридической «доказательности» (верификации фактов, установления субъектов, фиксации цепочек событий), так и в криптографическом смысле (доказательства корректности протокола, соблюдения свойств безопасности). Проблема проявляется на нескольких уровнях.

Во-первых, шифрование и анонимизация ставят под вопрос возможность установления происхождения, авторства и маршрута данных. Когда сообщение передано через анонимную сеть и зашифровано, становится существенно труднее установить, кто именно был отправителем или получателем, и каким образом проходил маршрут. В российских исследованиях подчеркивается, что изоляция отправителя/получателя

посредством маршрутизации и шифрования – ключевой признак анонимных сетей: «без маршрутизации легко определяются отправитель/получатель, без шифрования легко определяется передаваемое сообщение» [9]. В юридическом контексте это означает, что доказательство, например, факта передачи сообщения нужному адресату либо совершения действия конкретным лицом – становится сильно затруднено.

Во-вторых, шифрование препятствует трактовке содержимого и проверки целостности в тех случаях, где требуется раскрытие информации или публичное подтверждение. С одной стороны, шифрование защищает конфиденциальность, с другой – затрудняет аудит, поскольку для независимой верификации невозможно раскрывать ключи или содержимое без нарушения приватности. В российских работах ученых-правоведов отмечается: применение электронно-цифровой подписи и шифрования в системах не всегда обеспечивает корректное решение задачи анонимности и подлинности [10]. Это порождает ситуацию, когда доказательство в юридическом смысле оказывается либо неполным, либо требует раскрытия информации, противоречащей приватности.

Третья группа проблем связана с утечками метаданных и компромиссами между анонимностью и проверяемостью. Даже если содержание зашифровано и маршрут скрыт, существуют косвенные каналы – время передачи, размер пакета, характер маршрута – которые могут быть использованы для деанонимизации или для получения доказательств происхождения/маршрута. Российская публикация указывает, что анонимность – сложный многофакторный термин, и системы скрытых сетей включают комбинацию маршрутизации и шифрования, но не гарантируют абсолютной невозвратимости следов [9]. В юридической практике это означает, что расследование может требовать корреляции таких косвенных элементов, что усложняет как доказывание обвинительной версии, так и защиту.

Четвертый аспект – правовые и процессуальные ограничения получения и использования доказательств в сетях с анонимностью и шифрованием. В контексте российской уголовно-правовой практики отмечается, что электронные доказательства часто признаются недопустимыми из-за нарушения процедур (например, цепочки хранения, квалифицированной электронной подписи) – особенно в случаях, где используются анонимные сети и зашифрованное общение [11, с. 69]. Таким образом, доказательность в таких условиях ставится под сомнение не только технически, но и процедурно.

Наконец, существует конфликт между требованием сильной анонимности и необходимостью доказуемости. Если система проектируется с целью абсолютной анонимности, то, как правило, проверяемость и возможность аудита оказываются ограниченными. Есть исследования, указывающие, что не существует универсальной схемы, одновременно гарантирующей максимальную анонимность, минимальные утечки метаданных и полную доказательность действий. В российской практике аналогичные выводы: законодательство и технические решения пока не обеспечивают баланса между правом на анонимность и нуждой в доказательствах [12, с. 81].

В итоге, можно констатировать, что применение шифрования и анонимных сетей требует от системы доказывания адаптации: необходимо учитывать, что традиционные подходы к фиксации, маршрутизации и атрибуции данных могут оказаться неприменимыми или неполноценными.

Современные технологии, включая методы искусственного интеллекта (ИИ), генерирующие данные (дип-фейки), автоматический анализ больших массивов логов, облачную криминалистику, меняют методику работы с цифровыми следами. Например, исследования отмечают рост «синтетических реалий» – сгенерированных ИИ медиа, которые могут подменять или фальсифицировать цифровые доказательства [13].

В криминалистике это требует специальных экспертных методов проверки подлинности аудио/видео (например, анализ метаданных, исследования структуры файла, сравнение с известными образцами), внедрения автоматизированных инструментов фильтрации и анализа больших массивов данных (мессенджеры, геолокации, телеметрия), что позволяет быстрее выделять значимые цифровые следы [14, с. 47].

Также ИИ может быть использован следователем для предобработки данных, но требует контроль эксперта и пояснение в суде: каким образом обрабатывались данные, была ли проверка алгоритма, исключены ли ошибки/предвзятость.

Методика работы с цифровыми следами должна адаптироваться, например, стандарты создания «образа» устройства, расчет хеш-значений и цепочка обращения могут сопровождаться автоматизированными средствами, но следователь должен понимать технологию, чтобы объяснить суду, как обеспечена достоверность и отсутствие манипуляций.

Из этого следует, что ИИ и современные технологии не только расширяют возможности использования цифровых следов, но и добавляют новые риски и требования к экспертизе, законности и интерпретации.

В России и за рубежом подходы к использованию цифровых следов и электронных доказательств существенно отличаются по правовой основе, процедурам и правовой защите.

Если рассматривать с точки зрения контроля субъектом данных, в Германии субъект данных обладает реальным контролем и правом на удаление цифровых следов; в США ключевые права обеспечены через процедуры и судебные гарантии; в России предпринимаются попытки усилить контроль со стороны пользователя (например, удаление следов), но система еще недостаточно развита [15].

В России цифровые следы используются и бизнесом (реклама), и государством (надзор); в Германии в целях защиты данных и ограничения

вмешательства государства [16, с. 9]; в США – бизнес активно использует данные, но государственный доступ ограничен юридическими процедурами.

Германия трактует цифровые следы как личный актив и элемент цифрового суверенитета; США менее акцентируют ресурсный аспект; Россия активно движется в сторону использования больших данных, включая цифровые следы, в управлении и экономике. Например, есть замечания, что пользователь не может полностью отказаться от обработки своих цифровых следов в коммерческих целях [17].

Таким образом, подход Германии характеризуется правовой зрелостью и ориентацией на защиту личности, в то время как Россия сосредоточена на управленческом использовании цифровых следов, а США – на судебно-процедурной защите доступа к ним.

Таким образом, цифровые следы отличаются противоречивой природой цифровых следов как доказательств в уголовном процессе. С одной стороны, они обладают уникальным потенциалом для установления обстоятельств преступлений против жизни и здоровья через анализ геолокации, метаданных и коммуникаций. С другой – их доказательственная ценность ограничена технологическими барьерами (шифрование, анонимизация), процессуальными рисками (нарушения при изъятии) и новыми угрозами (дипфейки). Эффективное использование цифровых следов требует разработки унифицированных методик работы, адаптации законодательства и профессиональной подготовки следователей, способных обеспечить баланс между интересами правосудия и защитой цифровых прав личности.

Литература:

1. Россинская Е.Р. К вопросу об инновационном развитии криминалистической науки в эпоху цифровизации // Юридический вестник Самарского университета. – 2019. – № 4. – С. 144-151.

2. Корнакова С.В. Электронные доказательства в российском уголовном процессе: проблемные вопросы / С.В. Корнакова, Е.В. Чигрина // Юридический вестник Самарского университета. – 2025. – № 2. – С. 44-50.

3. Цимбал В.Н. Виды цифровой криминалистически значимой информации, получаемой в ходе расследования преступлений // Вестник ВГУ. Серия: Право. – 2021. – № 3. – С. 249-255.

4. Пряник К.В. Процессуально-криминалистические аспекты работы следователя с носителями электронной информации // Вестник Сибирского юридического института МВД России. – 2017. – № 2. – С. 103-107.

5. Смирнова К.А., Цифровые доказательства в уголовном процессе / К.А. Смирнова, Н.Н. Смирнов // Право и управление. – 2024. – № 5. – С. 564-566.

6. Приговор Ленинского районного суда г. Омска № 1-536/2018 от 01.11.2018 по делу № 1-536/2018 // Доступ из базы судебных решений «СудАкт».

7. Апелляционное определение Верховного Суда РФ от 17.10.2013 № 50-АПУ13-26 // Доступ из базы судебных решений «СудАкт».

8. Валькирия Н.И. Использование цифровых следов в деятельности по установлению лица, совершившего преступление // Уриминалистика: вчера, сегодня, завтра. – 2023. – № 4. – С. 56-66.

9. Структурный анализ сетевой анонимности // Хабр. – URL: https://habr.com/ru/articles/697458/ (дата обращения: 18.10.2025).

10. Биржи данных как движок экономики данных // Хабр. – URL: https://hbr.com/ru/companies/idx/articles/962598/ (дата обращения: 18.10.2025).

11. Перинов Н.П. Электронные доказательства в сфере уголовного судопроизводства Российской Федерации: правовые основы, проблемы и перспективы // Актуальные исследования. – 2025. – № 16 (251). – С. 67-71.

12. Куфлева В.Н. Проблемы квалификации преступлений, связанных с использованием шифрования информации и обеспечением анонимности в сети Интернет / В.Н. Куфлева, А.Л. Литовченко // Общество: политика, экономика, право. – 2021. – № 9. – С. 80-83.

13. В РФ за I квартал 2025 года выявили более 60 уникальных дипфейков // ТАСС. – URL: https://tass.ru/obschestvo/23621185 (дата обращения: 18.10.2025).

14. Корнакова С.В. Электронные доказательства в российском уголовном процессе: проблемные вопросы / С.В. Корнакова, Е.В. Чигрина // Юридический вестник Самарского университета. – 2025. – Т. 11. – № 2. – С. 44-50.

15. Каждый оставляет в интернете цифровой след. Как его контролировать // РБК Новости. – URL: https://www.rbc.ru/education/01/11/2025/6905e34e9a794740fa0ace53 (дата обращения: 18.10.2025).

16. Бродовски Д. Цифровые доказательства в немецком уголовном процессе на стадиях предварительного расследования, рассмотрения дела по существу и ревизии / Я. Маттиас, Д. Бродовски // Российское право: образование, практика, наука. – 2020. – № 3. – С. 4-18.

17. Мочалов А.Н. Цифровые следы человека и неприкосновенность частной жизни // Антиномии. – 2024. – Т. 24. – № 4. – С. 164-189.