**Дата поступления рукописи в редакцию: 19.07.2026 г.**
**Дата принятия рукописи в печать: 01.09.2026 г.**
DOI: 10.24412/2224-9133-2026-8-407-415

***КРАВЦОВА Анастасия Николаевна,***
*кандидат юридических наук, доцент кафедры уголовного и публичного права Московского университет «Синергия»,*
*e-mail: korneeva-nas@mail.ru*

# *ЦИФРОВЫЕ СЛЕДЫ КРИМИНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ В ВИРТУАЛЬНОМ ПРОСТРАНСТВЕ КАК ОСНОВА ФОРМИРОВАНИЯ ДОКАЗАТЕЛЬСТВ: ПРОБЛЕМЫ ДОПУСТИМОСТИ И ДОСТОВЕРНОСТИ*

***Аннотация.*** *Статья посвящена исследованию процессуального режима формирования доказательств на основе цифровых следов, возникающих в результате криминальной деятельности в виртуальном пространстве. Последовательно анализируются понятие и типология цифрового следа, его соотношение с закреплёнными частью 2 статьи 74 УПК РФ видами доказательств, механизм собирания и процессуального удостоверения электронных данных, а также критерии проверки их допустимости и достоверности. Стоит отметить, что отдельный интерес представляет проблема атрибуции цифрового следа конкретному лицу – центральный вопрос доказывания по делам в отношении дроповодов. Как показывает практика, не менее значим порядок использования результатов оперативно-розыскной деятельности, полученных в информационно-телекоммуникационной среде. Обосновывается вывод: цифровой след не образует самостоятельного вида доказательств и вводится в уголовное дело через уже существующие процессуальные формы, однако его материальная природа предопределяет специфику проверки – она носит преимущественно технико-верификационный, а не оценочно-логический характер. Обращает на себя внимание тот факт, что закон не устанавливает ни требований к фиксации неизменности электронных данных, ни минимального стандарта их атрибуции.*

***Ключевые слова:*** *цифровой след; электронные доказательства; допустимость; достоверность; атрибуция; хеш-значение; дроп; дроповод; компьютерно-техническая экспертиза; оперативно-розыскная деятельность.*

***KRAVTSOVA Anastasia Nikolaevna,***
*Candidate of Law, Associate Professor of the Department of Criminal and Public Law, Moscow University Synergy*

# *DIGITAL TRACES OF CRIMINAL ACTIVITY IN VIRTUAL SPACE AS THE BASIS OF EVIDENCE FORMATION: PROBLEMS OF ADMISSIBILITY AND RELIABILITY*

***Annotation.*** *The article is devoted to the study of the procedural regime for the formation of evidence based on digital traces arising from criminal activity in the virtual space. The concept and typology of the digital trace, its relationship with the types of evidence enshrined in part 2 of article 74 of the Code of Criminal Procedure of the Russian Federation, the mechanism for collecting and procedural certification of electronic data, as well as the criteria for checking their admissibility and reliability are consistently analyzed. It is worth noting that the problem of attribution of the digital trace to a specific person is of particular interest - the central issue of evidence in cases regarding droppers. As practice shows, the procedure for using the results of operational-search activities obtained in the information and telecommunication environment is no less significant. The conclusion is justified: the digital trace does not form an independent type of evidence and is*

*introduced into the criminal case through the already existing procedural forms, however, its material nature predetermines the specifics of the check - it is mainly technical and verification, and not of an evaluative and logical nature. Noteworthy is the fact that the law does not establish either the requirements for fixing the invariability of electronic data, or the minimum standard for their attribution.*

***Key words:*** *digital footprint; electronic evidence; admissibility; reliability; attribution; hash value; drop; dropovod; computer technical expertise; operational-search activities.*

Введение

Право на защиту от преступных посягательств, вытекающее из статей 2, 45 и 52 Конституции Российской Федерации, важно не само по себе, а как реально работающий механизм [1]. Он должен обеспечивать установление обстоятельств содеянного посредством доказательств, полученных законным способом и не вызывающих обоснованных сомнений в своей достоверности. И здесь гарантия обретает практическое содержание. По данным официальной статистики МВД России, преступления, совершаемые с использованием информационно-телекоммуникационных технологий, составляют свыше трети всех зарегистрированных деяний, а их абсолютное число превышает 750 тыс. в год. Парадоксально, но именно в этом сегменте, где следовая картина технически насыщена и детализирована, доля дел, направленных в суд, остаётся минимальной. Причина не в отсутствии следов, а в неспособности правоприменителя преобразовать их в допустимые и достоверные доказательства.

Особенно рельефно проблема проявляется по делам о деятельности так называемых дропов и дроповодов. В криминалистической литературе установлено, что «дроп» – физическое лицо, предоставляющее собственные персональные данные, банковские карты либо счета для проведения незаконных финансовых операций, тогда как «дроповод» выступает организатором и координатором соответствующих схем [10. С. 187; 11. С. 224]. Такая деятельность квалифицируется по совокупности статей 159, 174, 174.1, 187, а при наличии устойчивой организованной структуры – и статьи 210 Уголовного кодекса Российской Федерации [3].

Специфика указанной категории дел состоит в том, что дроповод физически не соприкасается ни с потерпевшим, ни с предметом преступления. Он не оставляет ни следов рук, ни следов обуви, ни биологических следов. Единственным материальным носителем информации о его действиях выступает цифровой след – запись в журнале авторизации, транзакционный лог, метаданные файла, сообщение в мессенджере, «отпечаток» устройства. На практике это значит, что вся система доказывания опирается на объекты, которые невидимы, легко модифицируемы, зачастую расположены за пределами юрисдикции Российской Федерации и не имеют прямой, самоочевидной связи с личностью обвиняемого.

Правовое регулирование данной сферы отличается дуализмом. Материально-правовая основа противодействия легализации преступных доходов сформирована Федеральным законом от 07.08.2001 № 115-ФЗ [5], а также принятым в 2025 г. комплексом мер по противодействию преступлениям, совершаемым с использованием информационных и коммуникационных технологий [7]. Процессуальный же режим обращения с электронными данными остаётся фрагментарным: он рассредоточен между статьями 81, 82, 84, 164.1, 183, 185, 186.1 УПК РФ и не образует системного института [2]. Эта двойственность порождает главную черту исследуемой проблематики: материально-правовое реагирование опережает процессуальное обеспечение.

Цель настоящего исследования – определить процессуальную природу цифровых следов криминальной деятельности в виртуальном пространстве, выявить проблемы их допустимости и достоверности на примере уголовных дел в отношении дроповодов и сформулировать научно обоснованные предложения по изменению УПК РФ и Федерального закона от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности». В процессе работы применялись системно-структурный метод – при исследовании соотношения цифрового следа и видов доказательств; формально-юридический – при анализе норм УПК РФ; сравнительно-правовой – при обращении к зарубежным моделям обеспечения сохранности компьютерных данных; а также методы контент-анализа материалов следственной практики по делам о дропах и дроповодах.

Обсуждение и результаты

Какова процессуальная природа цифрового следа? Ответ на этот вопрос предопределяет всё последующее рассуждение, и уклониться от него нельзя. Действующая часть 2 статьи 74 УПК РФ содержит закрытый перечень видов доказательств: показания подозреваемого, обвиняемого, потерпевшего, свидетеля; заключение и показания эксперта и специалиста; вещественные доказательства; протоколы следственных и судебных действий; иные документы [2]. Электронные данные в этом перечне не упомянуты. Следовательно, цифровой след как таковой доказательством не является – он приобретает дока-

зательственное значение исключительно после облечения в одну из перечисленных форм. Практика выработала четыре канала такого облечения. Первый – вещественное доказательство: сам электронный носитель (телефон, ноутбук, флешнакопитель, SIM-карта), изъятый и осмотренный в порядке статей 81, 164.1, 176–177 УПК РФ. Второй – иной документ: выписка по счёту, ответ оператора связи, справка антифрод-подразделения кредитной организации. Третий – протокол следственного действия: протокол осмотра интернетстраницы либо содержимого мессенджера с приложением распечаток. Четвёртый – заключение эксперта по результатам судебной компьютернотехнической экспертизы.

Такая конструкция внешне работоспособна, однако содержит принципиальный дефект. Вещественное доказательство по своей природе – предмет, сохраняющий следы преступления в неизменном виде; иной документ – носитель, удостоверяющий сведения и изготовленный вне рамок процесса. Цифровые данные не соответствуют ни одной из этих характеристик в полной мере: они существуют независимо от конкретного носителя, копируются без утраты качества, изменяются без видимых признаков вмешательства и уничтожаются дистанционно. Е.Р. Россинская справедливо отмечает, что информационно-компьютерные объекты обладают самостоятельным гносеологическим статусом, требующим адекватного процессуального оформления [12. С. 41]. В.А. Мещеряков и О.Ю. Цурлуй, развивая учение об электронно-цифровом отображении, указывают на то, что подведение таких объектов под классические категории неизбежно влечёт утрату части их доказательственных свойств [13. С. 165].

Отсюда первое предложение. Часть 2 статьи 74 УПК РФ надлежит дополнить пунктом 3.1 следующего содержания: «электронные (цифровые) данные, полученные, зафиксированные и приобщённые к материалам уголовного дела в порядке, установленном настоящим Кодексом». Одновременно УПК РФ следует дополнить статьёй 84.1 «Электронные (цифровые) данные», раскрывающей их понятие, а равно требования к получению и удостоверению. Возражение о том, что достаточно расширительного толкования статей 81 и 84 УПК РФ, не может быть признано решающим. Толкование не восполняет отсутствие требований к фиксации неизменности данных, а именно эти требования определяют судьбу доказательства при проверке его достоверности.

Обратимся к типологии цифровых следов, характерных для деятельности дроповода. Развивая предложенную в криминалистической литературе классификацию [10. С. 189; 14. С. 175], представляется возможным выделить шесть групп. Транзакционные следы – сведения о движении денежных средств: даты, суммы, реквизиты плательщиков и получателей, идентификаторы операций, данные о пополнении и обналичивании. Их доказательственная ценность состоит в возможности реконструировать финансовую архитектуру схемы и выявить узловые счета, контролируемые организатором.

Аутентификационные следы – журналы авторизации в системах дистанционного банковского обслуживания и на интернет-платформах: IP-адреса, метки времени, идентификаторы сессий, cookie-файлы, «отпечатки» устройств и браузеров, сведения о моделях устройств и версиях операционных систем. Именно эта группа приобретает решающее значение для атрибуции.

Коммуникационные следы – переписка в мессенджерах и социальных сетях, сообщения в закрытых чатах, обращения к телеграм-ботам, голосовые сообщения. Они позволяют установить факт организаторской роли, содержание указаний, распределение ролей внутри группы.

Документальные следы – фотографии и сканы паспортов дропов, таблицы учёта карт, реестры реквизитов, шаблоны инструкций. Их метаданные фиксируют авторство, дату создания и модификации, а порой и геолокацию съёмки.

Геолокационные и биллинговые следы – данные о соединениях абонентских устройств, привязка к базовым станциям, сведения о совпадении местонахождения устройства и места совершения банкоматных операций.

Следы систем противодействия мошенничеству – результаты работы антифрод-модулей кредитных организаций: маркеры нетипичного поведения, сработавшие правила, отметки о приостановлении операций.

Существенно, что доказательственное значение приобретает не отдельный след, а их корреляция. Изолированный IP-адрес не изобличает никого; совпадение же IP-адреса, «отпечатка» устройства, времени входа, геолокации абонентского устройства и последующей транзакции образует ту совокупность, которая позволяет ставить вопрос об атрибуции. Механизм следообразования в виртуальной среде подчинён закономерностям, требующим установления причинной связи между действием и его цифровым отображением [15. С. 209].

Перейдём к проблематике допустимости. Согласно части 3 статьи 7 и статье 75 УПК РФ доказательства, полученные с нарушением требований Кодекса, юридической силы не имеют. Применительно к цифровым следам можно выделить четыре проблемы.

Первая – изъятие электронных носителей информации. Статья 164.1 УПК РФ устанавливает специальный порядок: изъятие производится с участием специалиста, а по ходатайству закон-

ного владельца или обладателя информации осуществляется копирование данных на предоставленный носитель. Смысл нормы – минимизировать вред от изъятия и одновременно обеспечить сохранность содержимого. Между тем в делах о дроповодах наблюдается системное нарушение: телефоны и ноутбуки изымаются в ходе личного досмотра при задержании, без участия специалиста, без описания состояния устройства (включено либо выключено, наличие блокировки, режим полёта), без помещения в экранирующую упаковку. Последствие предсказуемо: сторона защиты ставит вопрос о возможности дистанционного удаления или модификации данных в интервале между изъятием и осмотром, и опровергнуть это утверждение процессуальными средствами оказывается затруднительно.

Вторая – осмотр содержимого устройства. Формально осмотр предмета производится по правилам статей 176–177 УПК РФ и не требует судебного решения. Однако содержимое смартфона включает переписку, охраняемую статьёй 23 Конституции Российской Федерации, и Конституционный Суд Российской Федерации неоднократно указывал на недопустимость произвольного доступа к сведениям, составляющим тайну сообщений. Возникает коллизия: доступ к переписке, передаваемой по каналам связи, требует судебного решения (статьи 185, 186, 186.1 УПК РФ), тогда как доступ к той же переписке, сохранённой в памяти устройства, судебного контроля не предполагает. Логического обоснования такому различию найти невозможно – содержание охраняемой тайны от места хранения не зависит.

В связи с изложенным предлагается дополнить УПК РФ статьёй 185.1 «Осмотр информации, содержащейся в электронном устройстве или на электронном носителе», предусмотрев, что исследование сведений о сообщениях, соединениях, а равно личных данных владельца производится на основании судебного решения, принимаемого в порядке статьи 165 УПК РФ; в случаях, не терпящих отлагательства, допускается производство осмотра с последующим уведомлением суда в течение трёх суток.

Третья – сведения, охраняемые банковской и телефонной тайной. Выемка предметов и документов, содержащих информацию о вкладах и счетах граждан в кредитных организациях, производится на основании судебного решения (часть 3 статьи 183 УПК РФ), получение сведений о соединениях между абонентами – в порядке статьи 186.1 УПК РФ. Практика между тем демонстрирует устойчивое стремление подменить эти процедуры направлением «запроса о предоставлении информации» в порядке части 4 статьи 21 УПК РФ. Полученные таким путём выписки по счетам дропов формально приобщаются как иные документы, но при надлежаще выстроенной позиции защиты подлежат исключению как полученные в обход установленного порядка. Итог: доказательство, объективно достоверное, утрачивается по причине процессуальной небрежности.

Четвёртая – результаты оперативно-розыскной деятельности. В силу статьи 89 УПК РФ и статьи 11 Федерального закона от 12.08.1995 № 144-ФЗ такие результаты могут использоваться в доказывании при условии соблюдения требований закона [4]. Особую проблему создаёт оперативно-розыскное мероприятие «получение компьютерной информации», включённое в перечень статьи 6 названного Закона, но не обеспеченное ни законодательным описанием содержания, ни регламентацией порядка производства и документирования. Отсутствие нормативной формы неизбежно ведёт к спорам о том, чем именно данное мероприятие отличается от снятия информации с технических каналов связи и допустимо ли его проведение без судебного решения. Предлагается дополнить статью 6 Федерального закона «Об оперативно-розыскной деятельности» нормой, определяющей получение компьютерной информации как совокупность действий по негласному доступу к информации, обрабатываемой техническими средствами, с указанием на обязательность судебного решения при затрагивании прав, предусмотренных статьями 23 и 24 Конституции Российской Федерации, и на обязательность фиксации хеш-значений полученных данных.

Отдельного внимания заслуживают материалы, происходящие из иностранных информационных сервисов. Значительная часть коммуникации дроповодов осуществляется в мессенджерах, серверы которых расположены за пределами Российской Федерации, а операторы не исполняют запросы российских правоохранительных органов. Формирование доказательств в такой ситуации осуществляется опосредованно: через изъятые устройства дропов, через осмотр аккаунтов с использованием предоставленных участниками схемы паролей, через показания соучастников. Каждый из этих путей уязвим. Осмотр аккаунта, произведённый с ведома одного из участников переписки, не нарушает тайну сообщений в отношении этого лица, но затрагивает права его собеседника, что требует самостоятельной процессуальной оценки.

Теперь о достоверности. Здесь необходимо провести разграничение, которое в правоприменительной практике систематически игнорируется. Допустимость характеризует законность способа получения доказательства; достоверность – соответствие содержащихся в нём сведений действительности. Смешение этих свойств недопустимо, поскольку влечёт различные процессу-

альные последствия: недопустимое доказательство исключается из совокупности безусловно, недостоверное – оценивается судом по правилам статьи 88 УПК РФ наряду с иными доказательствами. Между тем в постановлениях об отказе в удовлетворении ходатайств об исключении цифровых данных нередко указывается на их «достоверность», хотя оспаривался порядок получения, – и наоборот.

Проверка достоверности цифрового следа распадается на две относительно самостоятельные задачи: установление аутентичности данных и установление их атрибуции. Аутентичность есть тождественность представленных суду данных тем данным, которые существовали в момент их фиксации. Технически эта задача решена давно: вычисление криптографической хеш-функции (контрольной суммы) образа носителя позволяет достоверно установить факт любого, даже однобитового изменения. Однако процессуальной обязанности вычислять и фиксировать хеш-значение действующий УПК РФ не предусматривает. В результате в протоколах осмотра указывается количество изъятых файлов, но не указывается их контрольная сумма, и любое последующее утверждение о неизменности данных остаётся недоказуемым.

Предлагается дополнить статью 166 УПК РФ частью 8.1: «При производстве следственных действий, связанных с изъятием, копированием или осмотром электронных данных, в протоколе указываются наименование и версия использованных программно-технических средств, точное время начала и окончания действия с указанием часового пояса, а также значения криптографических хеш-функций созданных копий (образов) данных». Корреспондирующим образом статью 164.1 УПК РФ следует дополнить положением о том, что копирование информации осуществляется способом, исключающим её модификацию, с обязательным вычислением хеш-значений исходных данных и полученной копии.

Особую практическую значимость имеет судьба так называемых скриншотов. Распечатка изображения экрана, приобщённая к протоколу осмотра, юридически представляет собой производный объект, отделённый от первоисточника и не сохраняющий метаданных. Она не позволяет установить ни подлинность содержания, ни отсутствие монтажа, ни даже принадлежность аккаунта. Как показывает практика, приговоры, опирающиеся преимущественно на скриншоты переписки, наиболее уязвимы при апелляционном и кассационном пересмотре. Значит, скриншот может использоваться исключительно как иллюстрация к результатам исследования исходного контейнера данных, но не как самостоятельное основание вывода о виновности.

Атрибуция – центральная и наиболее трудная задача доказывания по делам о дроповодах. Требуется установить, что конкретное действие в виртуальном пространстве совершено конкретным физическим лицом. Между тем цифровой след фиксирует не человека, а устройство, аккаунт либо сетевой адрес, и каждое из этих звеньев допускает разрыв связи с личностью.

IP-адрес не идентифицирует пользователя: применение технологии трансляции сетевых адресов означает, что за одним внешним адресом одновременно находятся десятки и сотни абонентов. Использование VPN-сервисов, анонимизирующих сетей и цепочек прокси-серверов дополнительно разрывает связь между действием и его инициатором. Аккаунт может быть зарегистрирован на подставные данные; SIM-карта – оформлена на лицо, не осведомлённое о её использовании; устройство – принадлежать третьему лицу.

Как преодолевается этот разрыв? Исключительно через построение совокупности взаимно подкрепляющих цифровых следов. Опыт расследования дел рассматриваемой категории позволяет выделить наиболее результативные приёмы.

Во-первых, выявление операционных ошибок субъекта. Дроповод, использующий средства анонимизации при работе с дроп-аккаунтами, в бытовой активности их, как правило, не применяет. Совпадение «отпечатка» устройства, версии операционной системы, набора установленных шрифтов и языковых настроек при обращении к дроп-аккаунту и к персональному аккаунту в социальной сети образует технически верифицируемую связь [10. С. 190].

Во-вторых, установление финансовой связности. Пополнение баланса SIM-карт, оформленных на подставных лиц, со счёта, контролируемого подозреваемым, оплата хостинга или прокси-сервиса с его банковской карты – типичные и практически неизбежные точки соприкосновения анонимной и легальной идентичностей.

В-третьих, корреляция геолокационных данных. Совпадение зоны действия базовой станции, обслуживавшей абонентское устройство подозреваемого, с местом расположения банкомата, в котором осуществлялось обналичивание, подтверждённое видеозаписью, обладает высокой доказательственной силой.

В-четвертых, анализ метаданных документальных следов. Фотографии паспортов дропов, обнаруженные в облачном хранилище, содержат сведения о модели устройства съёмки и, при неотключённой геометке, о координатах места съёмки.

В-пятых, исследование коммуникативного профиля. Устойчивые лексические и орфографические особенности, специфический жаргон криминальной среды («прогон», «выкатать кар-

ту», «залив»), характерные приветственные и завершающие формулы подлежат установлению посредством судебной лингвистической экспертизы. Значимость такого анализа возрастает в тех случаях, когда коммуникация внутри группы насыщена идеологическими маркерами, выполняющими функцию кодового сигнала и средства внутригрупповой идентификации [11. С. 228].

Возникает вопрос: каков минимальный стандарт атрибуции? Представляется, что вывод о совершении действия конкретным лицом не может основываться на единственном техническом признаке, каким бы убедительным он ни казался. Требуется совокупность, включающая не менее трёх независимых по источнику происхождения групп цифровых следов, подкреплённых заключением эксперта. Данное положение целесообразно закрепить в разъяснениях Пленума Верховного Суда Российской Федерации.

Отсюда следующее предложение: статью 196 УПК РФ надлежит дополнить пунктом, устанавливающим обязательное назначение судебной компьютерно-технической экспертизы в случаях, когда вывод о причастности лица к преступлению основывается на данных о его действиях в информационно-телекоммуникационной сети. При комплексном характере задачи – установлении финансовой архитектуры схемы – целесообразно назначение комплексной компьютерно-технической и финансово-экономической экспертизы.

Существенным дефектом действующего регулирования следует признать отсутствие механизма срочного обеспечения сохранности компьютерной информации. Данные об авторизациях, сессиях и соединениях хранятся операторами связи и организаторами распространения информации в течение ограниченных сроков, установленных статьёй 64 Федерального закона «О связи» и статьёй 10.1 Федерального закона от 27.07.2006 № 149-ФЗ [6]. К моменту, когда следователь получает судебное решение и направляет запрос, значительная часть данных нередко уже уничтожена в плановом порядке. Зарубежный опыт предлагает решение: институт предписания о сохранении данных (data preservation order), закреплённый, в частности, статьёй 16 Конвенции о киберпреступности, участником которой Российская Федерация не является, но методологическая ценность конструкции от этого не умаляется.

Предлагается дополнить УПК РФ статьёй 186.2 «Требование о сохранении компьютерной информации», предусмотрев право следователя, дознавателя своим постановлением, не требующим судебного решения, обязать оператора связи, организатора распространения информации либо кредитную организацию обеспечить неизменность и сохранность определённого объёма данных на срок до девяноста суток с возможностью однократного продления. Принципиально, что требование о сохранении не влечёт доступа к содержанию данных – оно лишь блокирует их уничтожение, а последующее получение осуществляется в общем порядке, включая судебный контроль. Такая конструкция обеспечивает баланс между эффективностью расследования и защитой прав, гарантированных статьями 23 и 24 Конституции Российской Федерации.

Организационно-техническая составляющая проблемы не менее значима, чем нормативная. Развивая высказанную в литературе идею о государственной системе учёта доказательственных данных [11. С. 229], представляется целесообразным создание единого криминалистического депозитария цифровых доказательств – защищённой информационной системы, обеспечивающей хранение образов носителей с фиксацией хеш-значений, журналирование всех обращений к ним и невозможность внесения изменений. Данное решение одновременно снимает проблему сохранности вещественных доказательств, предусмотренную частью 4 статьи 82 УПК РФ, и обеспечивает возможность проверки аутентичности данных на любой стадии процесса, включая кассационную.

Одновременно необходимо учитывать риски. Введение обязательного хеш-протоколирования и депозитарного хранения без соответствующего технического обеспечения следственных подразделений неизбежно приведёт к формальному исполнению новых требований. Расследование, проводимое с использованием личного ноутбука следователя и произвольно выбранного программного обеспечения, не способно обеспечить ни воспроизводимость результатов, ни их процессуальную состоятельность. Соответственно, необходим федеральный минимальный стандарт технического обеспечения следственных подразделений, включающий сертифицированные программно-аппаратные средства криминалистического копирования с блокировкой записи, средства экранирования изымаемых устройств, лицензионное программное обеспечение для анализа образов носителей и защищённые каналы взаимодействия с кредитными организациями и операторами связи. Финансирование данного стандарта не может зависеть от бюджетной обеспеченности региона, что предполагает создание механизма федерального софинансирования.

Материально-правовой аспект также требует корректировки. Действующая практика квалифицирует деятельность дроповода преимущественно по статье 187 УК РФ, однако диспозиция этой нормы ориентирована на неправомерный оборот средств платежей и не охватывает организацию сети подконтрольных счетов, равно как

и вербовку дропов в качестве самостоятельного деяния. Обсуждаемые в 2025 г. законодательные инициативы о криминализации дропперства заслуживают поддержки, однако их реализация должна сопровождаться уточнением процессуального инструментария: без надёжного механизма формирования цифровых доказательств новые составы останутся неприменимыми.

Наконец, целесообразно принятие постановления Пленума Верховного Суда Российской Федерации, в котором надлежит изложить систематизированные разъяснения по следующим вопросам: понятие электронных (цифровых) данных и порядок их приобщения к материалам уголовного дела; требования к протоколированию действий с электронными носителями, включая фиксацию хеш-значений; критерии допустимости данных, полученных из иностранных информационных сервисов; минимальный стандарт атрибуции цифрового следа конкретному лицу; разграничение оснований признания цифровых данных недопустимыми и оценки их как недостоверных; правила оценки распечаток и изображений экрана, не сопровождаемых исследованием первоисточника.

Обобщение правоприменительной практики позволяет выделить три типичные ошибки. Первая – подмена судебного порядка получения охраняемых законом сведений направлением запроса. Вторая – формальная фиксация факта изъятия электронного носителя без описания его состояния и без обеспечения неизменности данных. Третья – обоснование атрибуции единственным техническим признаком, чаще всего IP-адресом. Их устранение требует как точечной корректировки УПК РФ, так и повышения квалификации правоприменителя, но не создания обособленного «цифрового» процесса, что лишь усложнило бы систему процессуального регулирования без соразмерного положительного эффекта.

Итог: цифровой след способен стать полноценной основой обвинения, но лишь при условии технически верифицируемой фиксации и многоканальной атрибуции.

Заключение

Каковы реальные пределы доказательственного значения цифровых следов в уголовных делах о деятельности дроповодов? Проведенное исследование позволяет очертить эти пределы достаточно четко.

Цифровой след не образует самостоятельного вида доказательств и вводится в уголовное дело исключительно через формы, предусмотренные частью 2 статьи 74 УПК РФ, – вещественное доказательство, иной документ, протокол следственного действия либо заключение эксперта. Иных вариантов действующий закон не предусматривает. Вместе с тем материальная природа электронных данных – их отделимость от носителя, копируемость без утраты качества, скрытая модифицируемость – не соответствует признакам ни одной из существующих форм в полной мере, что обусловливает необходимость нормативного закрепления электронных (цифровых) данных как самостоятельного источника доказательств.

Проверка допустимости цифрового следа концентрируется вокруг четырёх узлов: соблюдения специального порядка изъятия электронных носителей, наличия судебного контроля при доступе к охраняемым законом сведениям, законности использования результатов оперативно-розыскной деятельности и правомерности получения данных из иностранных информационных сервисов. Парадоксально, но даже объективно достоверная информация о движении денежных средств утрачивает юридическую силу, если получена в обход процедуры, установленной частью 3 статьи 183 УПК РФ.

Проверка достоверности распадается на установление аутентичности и установление атрибуции. Первая задача технически разрешима посредством криптографического хеширования, однако процессуальной обязанности его производить закон не устанавливает. Вторая задача принципиально не может быть решена на основании единственного технического признака: вывод о совершении действия конкретным лицом требует совокупности не менее трёх независимых по источнику групп цифровых следов, подкреплённых заключением эксперта. На практике это значит, что успех доказывания по делам о дроповодах определяется не объёмом изъятой информации, а качеством выявленных корреляций между анонимной и легальной идентичностями подозреваемого.

Совершенствование доказательственного режима требует взаимосвязанных процессуальных и организационных изменений. Речь идёт о дополнении части 2 статьи 74 УПК РФ пунктом 3.1 и введении статьи 84.1; о закреплении в статьях 164.1 и 166 УПК РФ обязательного хеш-протоколирования; о введении статьи 185.1 УПК РФ, устанавливающей судебный порядок осмотра информации, содержащейся в электронном устройстве; о введении статьи 186.2 УПК РФ о требовании к сохранению компьютерной информации; о дополнении статьи 196 УПК РФ основанием обязательного назначения компьютерно-технической экспертизы; о нормативной регламентации оперативно-розыскного мероприятия «получение компьютерной информации»; о создании единого криминалистического депозитария цифровых доказательств и установлении федерального минимального стандарта технического обеспечения следственных подразделений.

Введение новых процессуальных требований при неизменности материально-технической базы способно превратить их в формальность. Поправки к УПК РФ должны вступать в силу одновременно с утверждением методики криминалистического исследования электронных носителей, оснащением следственных подразделений сертифицированными программно-аппаратными средствами и организацией профессиональной подготовки следователей. В противном случае усиление требований к форме приведёт не к повышению надёжности доказывания, а к увеличению числа дел, прекращённых за недостаточностью доказательств, – то есть к результату, противоположному целям реформы. Итог очевиден: без синхронного технологического и кадрового обеспечения любые процессуальные новеллы рискуют остаться декларацией.

**Список литературы:**

[1] Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 01.07.2020 № 11-ФКЗ, от 06.10.2022) // СПС «Гарант».

[2] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 26.07.2026 г.) // Собрание законодательства Российской Федерации. 2001. № 52 (ч. I). Ст. 4921.

[3] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 26.07.2026 г.) // Собрание законодательства Российской Федерации. 1996. № 25. Ст. 2954.

[4] Федеральный закон от 12.08.1995 № 144-ФЗ (ред. от 01.04.2025 г.) «Об оперативно-розыскной деятельности» // Собрание законодательства Российской Федерации. 1995. № 33. Ст. 3349.

[5] Федеральный закон от 07.08.2001 № 115-ФЗ (ред. от 10.06.2026) «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» // Собрание законодательства Российской Федерации. 2001. № 33 (ч. I). Ст. 3418.

[6] Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 26.06.2026 г.) «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации. 2006. № 31 (ч. I). Ст. 3448.

[7] Федеральный закон от 01.04.2025 № 41-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» (о дополнительных мерах противодействия преступлениям, совершаемым с использованием информационных и коммуникационных технологий) // Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru (дата обращения: 28.07.2026).

[8] Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 (ред. от 15.12.2022) «О судебной практике по делам о мошенничестве, присвоении и растрате». URL: https://www.consultant.ru/document/cons_doc_LAW_284098/ (дата обращения: 28.07.2026).

[9] Постановление Пленума Верховного Суда РФ от 07.07.2015 № 32 (ред. от 26.02.2019) «О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем». URL: https://www.consultant.ru/document/cons_doc_LAW_181916/ (дата обращения: 28.07.2026).

[10] Алымов, Д. В. Криминалистическая характеристика типовых следов преступника, осуществляющего криминальную деятельность в виртуальном пространстве (на примере дроповодов) / Д. В. Алымов, К. Г. Балашов, А. Ю. Дериглазова // Вестник Томского государственного университета. – 2024. – № 506. – С. 185-192. doi: 10.17223/15617793/506/23.

[11] Петрищева, Н. С. Некоторые особенности учета идеологического компонента при расследовании преступлений на примере деятельности «дропов» и «дроповодов» / Н. С. Петрищева, Д. М. Носов, К. Г. Балашов // Вестник Томского государственного университета. – 2026. – № 523. – С. 268-275. doi: 10.17223/15617793/523/29.

[12] Россинская, Е. Р. Концепция цифровых следов в криминалистике / Е. Р. Россинская // Криминалистика: вчера, сегодня, завтра. – 2019. – № 4 (12). – С. 38-47.

[13] Мещеряков, В. А. О понятии электронно-цифрового отображения в цифровой криминалистике / В. А. Мещеряков, О. Ю. Цурлуй // Российское правосудие. – 2022. – № 1. – С. 162-171.

[14] Переверзева, Е. С. Виртуальные и цифровые следы: новый подход в понимании / Е. С. Переверзева, А. В. Комов // Вестник Санкт-Петербургского университета МВД России. – 2021. – № 1 (89). – С. 172–178. doi: 10.35750/2071-8284-2021-1-172-178.

[15] Грибунов, О. П. Криминалистическая теория причинности в контексте установления механизма следообразования: философские и теоретические аспекты / О. П. Грибунов // Вестник Томского государственного университета. – 2019. – № 446. – С. 207-211.

**References:**

[1] The Constitution of the Russian Federation (adopted by popular vote on 12.12.1993) (taking into account the amendments made by the Laws of the Russian Federation on amendments to the Constitution of the Russian Federation dated

30.12.2008 No. 6-FKZ, dated 30.12.2008 No. 7-FKZ, dated 05.02.2014 No. 2-FKZ, dated 01.07.2020 No. 11-FKZ, dated 06.10.2022 ) // SPS "Garant.".

[2] Code of Criminal Procedure of the Russian Federation dated 18.12.2001 No. 174-FZ (as amended on 26.07.2026 ) // Collection of Legislation of the Russian Federation. 2001. No. 52 (part I). Art. 4921.

[3] Criminal Code of the Russian Federation dated 13.06.1996 No. 63-FZ (as amended on 26.07.2026 ) // Collection of Legislation of the Russian Federation. 1996. № 25. Art. 2954.

[4] Federal Law of 12.08.1995 No. 144-FZ (as amended on 01.04.2025) "On Operational Search Activities "// Collection of Legislation of the Russian Federation. 1995. № 33. Art. 3349.

[5] Federal Law No. 07.08.2001 of 115-FZ (as amended 10.06.2026) "On Combating Legalization (Laundering) of Proceeds from Crime and Financing of Terrorism "// Collection of Legislation of the Russian Federation. 2001. No. 33 (part I). Art. 3418.

[6] Federal Law of 27.07.2006 No. 149-FZ (as amended on 26.06.2026) "On Information, Information Technologies and Information Protection "// Collection of Legislation of the Russian Federation. 2006. No. 31 (part I). Art. 3448.

[7] Federal Law of 01.04.2025 No. 41-FZ "On Amendments to Certain Legislative Acts of the Russian Federation" (on additional measures to counter crimes committed using information and communication technologies ) // Official Internet portal of legal information. URL: http://pravo.gov.ru (access date: 28.07.2026).

[8] Decision of the Plenum of the Supreme Court of the Russian Federation of 30.11.2017 No. 48 (ed. 15.12.2022) "On judicial practice in cases of fraud, embezzlement and embezzlement." URL: https ://www.consultant.ru/document/cons_ doc_ LAW_ 284098/( accessed: 28.07.2026).

[9] Resolution of the Plenum of the Supreme Court of the Russian Federation of 07.07.2015 No. 32 (ed. 26.02.2019) "On judicial practice in cases of legalization (laundering) of money or other property acquired by criminal means, and on the acquisition or sale of property knowingly obtained by criminal means." URL: https ://www.consultant.ru/document/cons_ doc_ LAW_ 181916/( accessed: 28.07.2026).

[10] Alymov, D. V. Forensic characteristics of typical traces of a criminal carrying out criminal activities in virtual space (using the example of droppers )/D. V. Alymov, K. G. Balashov, A. Yu. Deriglazova // Bulletin of Tomsk State University. – 2024. – № 506. - S. 185-192. doi: 10.17223/15617793/506/23.

[11] Petrishcheva, N. S. Some features of taking into account the ideological component when investigating crimes using the example of the activities of "drops" and "drops "/N. S. Petrishcheva, D. M. Nosov, K. G. Balashov // Bulletin of Tomsk State University. – 2026. – № 523. - S. 268-275. doi: 10.17223/15617793/523/29.

[12] Rossinskaya, E.R. The concept of digital traces in forensics/E.R. Rossinskaya // Forensics: yesterday, today, tomorrow. – 2019. – № 4 (12). - S. 38-47.

[13] Meshcheryakov, V. A. On the concept of electronic digital display in digital forensics/ V. A. Meshcheryakov, O. Yu. Tsurluy // Russian Justice. – 2022. – № 1. - S. 162-171.

[14] Pereverzeva, E. S. Virtual and digital traces: a new approach in understanding/E. S. Pereverzeva, A. V. Komov // Bulletin of St. Petersburg University of the Ministry of Internal Affairs of Russia. – 2021. – № 1 (89). - S. 172-178. doi: 10.35750/2071-8284-2021-1-172-178.

[15] Gribunov, O. P. Forensic theory of causality in the context of establishing the mechanism of trace formation: philosophical and theoretical aspects/O. P. Gribunov // Bulletin of Tomsk State University. – 2019. – № 446. - S. 207-211.