

УДК 343.98

**ТЕОРЕТИКО-ПРАВОВЫЕ ОСНОВЫ КРИМИНАЛИСТИЧЕСКОГО  
УЧЕНИЯ О «ЦИФРОВЫХ СЛЕДАХ»****Торопов Сергей Александрович,**

доцент кафедры уголовно-процессуального права  
Крымского филиала ФГБОУВО «РГУП им. В.М. Лебедева»  
кандидат юридических наук, доцент  
г. Симферополь, Россия,  
E-mail: sergei5714@mail.ru

**Кузнецов Владислав Владимирович,**

студент Крымского филиала ФГБОУВО «РГУП им. В.М. Лебедева»  
г. Симферополь, Россия,  
E-mail: kou.vlad2005@yandex.ru

**Аннотация**

Статья посвящена исследованию теоретико-правовой природы «цифровых следов» как объекта криминалистического познания. Авторами проведён критический анализ доктринальных подходов к терминологии, обосновывающий приоритетность дефиниции «цифровой след». Акцентируется внимание на отсутствии надлежащей законодательной регламентации анализируемой категории и предлагаются пути устранения данного правового пробела. В частности, обоснована необходимость закрепления понятия «цифровой след» в Федеральном законе «О персональных данных», а также дополнения ч. 2 ст. 74 УПК РФ новым видом доказательств – «результатами исследования «цифровых следов», в целях обеспечения единообразия следственной практики и совершенствования механизма доказывания.

**Ключевые слова:** цифровизация, преступное событие, «цифровой след», «виртуальный след», «электронно-цифровой след», электронный носитель.

**THEORETICAL AND LEGAL FOUNDATIONS OF THE CRIMINALISTICS  
DOCTRINE ON «DIGITAL FOOTPRINTS»****Toropov Sergey Alexandrovich,**

Associate Professor of the Department of Criminal Procedure Law  
of the Crimean branch of the Federal State Budgetary Educational Institution of Higher Education  
«Russian State University of Justice named after V.M. Lebedev»  
Candidate of Legal Sciences, Associate Professor  
Simferopol, Russia,  
E-mail: sergei5714@mail.ru

**Kuznetsov Vladislav Vladimirovich,**

student of the Crimean branch

of the Federal State Budgetary Educational Institution of Higher Education

«Russian State University of Justice named after V.M. Lebedev»

Simferopol, Russia,

E-mail: kou.vlad2005@yandex.ru

---

## ABSTRACT

---

The article is devoted to the study of the theoretical and legal nature of «digital traces» as an object of forensic knowledge. The authors conducted a critical analysis of the doctrinal approaches to terminology, substantiating the priority of the definition of «digital trace». Attention is focused on the lack of proper legislative regulation of the analyzed category, and ways to eliminate this legal gap are proposed. In particular, the need to enshrine the concept of «digital trace» in the Federal Law «On Personal Data» has been substantiated, as well as the addition of a new type of evidence to Part 2 of Article 74 of the Criminal Procedure Code of the Russian Federation: «the results of the examination of digital traces», in order to ensure uniform investigative practices and improve the mechanism of proof.

---

**Keywords:** digitalization, criminal event, «digital trace», «virtual trace», «electronic-digital trace», electronic medium.

---

Современный этап развития криминалистической деятельности характеризуется зависимостью от оперативного доступа к цифровой информации. Социальные сети и облачные хранилища данных стали одним из основных источников юридически значимых сведений, позволяющих не только идентифицировать участников правонарушений, но и исследовать механизм преступного деяния.

Одним из закономерных последствий цифровизации криминальной среды стало формирование нового объекта криминалистического познания – специфической категории юридически значимых данных, обозначаемых в современной доктрине как «цифровые следы» [12, с. 902]. Широкое распространение подобного рода данных сопряжено с рядом критических проблем.

В отличие от материальных следов, «цифровые следы» характеризуются высокой степенью изменчивости и значительной зависимостью от владельцев соответствующих телекоммуникационных платформ [25, с. 160]. Для криминалистики это означает необходимость переосмысления совершаемых в цифровой среде преступлений не как единичного акта, а как части более широкой, комплексной системы, включающей в себя генерацию, передачу, хранение и, в конечном итоге, обнаружение следов, которые, в силу специфики своего происхождения, приобретают совершенно новую форму [22, с. 203]. Правовая природа «цифровых следов» делает невозможным их анализ вне контекста задействованной информационной системы, что требует от криминалистики принципиально иного методологического подхода к их исследованию.

Для обеспечения концептуальной целостности работы представляется необходимым обратиться к анализу правовой природы «цифровых следов». При этом важно указать, что в современной криминалистической доктрине отсутствует единство в терминологическом обозначении рассматриваемого феномена. Так, учёные В. А. Мещеряков, В. Ю. Агибалов и А. Б. Смушкин обосновывают целесообразность использования термина «виртуальный

след» [13, с. 94; 1, с. 34-35; 21, с. 43]. Исследователь В. В. Борисов аргументирует применение понятия «информационный след» [4, с. 164]. Учёные В. Б. Вехов, А. В. Шебалин и В. В. Поляков, в свою очередь, оперируют категорией «электронно-цифровой след» [6, с. 4; 15, с. 125].

Принимая во внимание наличие и иных интерпретаций, представляется необходимым обосновать целесообразность использования понятия «цифровой след», как наиболее полно отражающего специфику исследуемого явления.

При анализе термина «виртуальный след» важно учитывать его семантику. Слово «виртуальный» в своём исходном значении подразумевает «не имеющий физического воплощения или воспринимаемый иначе, чем реализован» [30, с. 62-63]. Утверждение, что след является «виртуальным», с технической точки зрения является ошибочным, поскольку физический носитель и зафиксированное на нём состояние данных реальны и воспроизводимы. В этой связи применение данной дефиниции к объекту, обладающему материальной основой (например, доменом на HDD, в кейлоггере и др.), не только противоречит его методологической природе, но и создаёт предпосылки для психологического и юридического обесценивания, придавая ему «оттенок иллюзорности».

Критика термина «информационный след», в свою очередь, обосновывается его абстрактностью. В криминалистике категория «информация» носит универсальный характер: практически любой материальный след является её носителем (отпечатки пальцев содержат данные о папиллярном узоре, биологические объекты – генетическую информацию, следы обуви – информацию о морфологии подошвы и т.д.). В этой связи использование термина «информационный след» для обозначения цифровых данных представляется методологически некорректным, так как он нивелирует его видовую специфику. Ключевое различие в данном контексте заключается в способе фиксации, а не в содержании конкретных данных. Поэтому для целей уголовного судопроизводства приоритетное значение имеет технологический аспект: цифровая специфика рассматриваемого следа предопределяет особый алгоритм работы с ним, который существенно отличается от порядка исследования иных объектов.

Использование термина «электронно-цифровой след», в свою очередь, представляется семантически избыточным. Учитывая, что любая цифровая информация опосредована электронной компонентной базой, термин «электронный» не несёт дополнительной смысловой нагрузки. Иными словами, признак «цифровой» уже подразумевает использование электронных средств, делая приставку «электронно-» излишней. Принцип обеспечения терминологической точности обуславливает необходимость отказа от подобного рода плеоназмов: подобно тому, как отпечаток пальца не нуждается в дополнительной биофизической квалификации, понятие «цифровой след» является самодостаточным и исчерпывающим определением.

В конечном счёте использование дефиниции «цифровой след» обеспечит унификацию национальной терминологии с общепринятой международной практикой и представленной в ней эквивалентами – «Digital footprint и Digital trace».

В свете вышесказанного, видится необходимость закрепления на законодательном уровне именно термина «цифровой след». Прилагательное «цифровой» в данном контексте является не просто описательной, но и сущностной характеристикой, обозначающей специфический способ кодирования информации – двоичную (цифровую) систему исчисления. Это важное отличие, позволяющее дифференцировать такие следы от данных, представленных в аналоговых форматах (например, на фотоплёнке или аудиокассете и др.). Более того, сам термин «цифровой» уже прочно интегрирован в правовое поле, что подтверждается устоявшимися понятиями, такими как «цифровые права» (ст. 141.1), «цифровые активы» [8; 29]. Подобная преэминентность способствует

формированию единого терминологического поля для органов различного уровня, исключая риск неоднозначного толкования.

Переходя к содержательной характеристике понятия «цифровой след», необходимо отметить отсутствие единого подхода к пониманию его сущности как в теории криминалистики, так и в действующем законодательстве. Указанное обстоятельство вполне закономерно, учитывая новизну данной правовой категории. В контексте сказанного, актуализируется необходимость всестороннего содержательного исследования категории «цифровой след».

Рассмотрение доктринальных подходов к определению понятия «цифровой след» невозможно без обращения к позиции учёных-криминалистов Е. Р. Россинской и И. А. Рядовского. Исследователи определяют данную дефиницию как «криминалистически значимую компьютерную информацию о событиях или действиях, отражённую в материальной среде в процессе её возникновения, обработки, хранения и передачи» [18].

Предлагаемая формулировка акцентирует внимание на информационной составляющей следа и его неразрывной связи с материальным носителем, что обеспечивает её соответствие традиционным криминалистическим концепциям следообразования [24, с. 330]. При этом следует указать, что особую роль в структуре дефиниции играет категория «криминалистической значимости». Использование данного критерия позволяет сузить объем рассматриваемых данных до таких, которые обладают доказательственным значением. Подобный подход соответствует фундаментальному принципу доказывания в рамках уголовного судопроизводства – принципу относимости доказательств.

В продолжение анализа подходов к определению понятия «цифровой след», заслуживает внимания концепция учёного А. А. Бесонова. По его мнению, «цифровой след» определяется как информация, зафиксированная в цифровом формате. К источникам такого следа он относит электронно-вычислительные машины, иные цифровые устройства технологической природы, средства мобильной связи, а также различные носители цифровой информации. Центральными признаками, выделяемыми авторами, являются его причинно-следственная связь с событием преступления и способность служить установлению обстоятельств его совершения и идентификации преступника [3, с. 47].

Наряду с выработкой теоретических подходов к определению сущности «цифровых следов», в научной литературе получили развитие различные подходы к их классификации. Рассмотрим отдельные из них. Так, ввиду специфики «цифровых следов», их классическое деление на материальные и идеальные вызывает активные дискуссии в научном сообществе. Аргументы в пользу материальной природы таких следов основаны на факте их фиксации на физическом носителе и опосредованном характере их восприятия (необходимость использования программно-аппаратных комплексов для их изъятия и фиксации). В тоже время, признание «цифровых следов» материальными представляется спорным, поскольку они обладают признаками, присущими и идеальным следам: высокой волатильностью, зависимостью от формата данных и отсутствием неразрывной связи с конкретным носителем информации.

В продолжение научной полемики, учёные В. Б. Вехов, Б. П. Смагоринский и С. А. Ковалев обосновали концепцию «невидимых материальных следов» [5, с. 18]. Аналогичного подхода придерживаются ученые Д. В. Бахтеев и Е. В. Смахтин. По мнению исследователей, к «цифровым следам» применимы критерии материальности, поскольку они неразрывно связаны с физическими характеристиками носителей информации – например, с уровнем намагниченности участка поверхности жёсткого диска [2, с. 65].

В конечном счёте непрекращающиеся научные дискуссии привели к формированию в криминалистической доктрине позиции, согласно которой «цифровые следы» занимают промежуточное положение между материальными и идеальными. В связи с этим, учёные

В. О. Головин и В. О. Давыдов предложили расширение традиционной классификации путём введения третьей категории следов [9, с. 255]. Такой подход, на наш взгляд, представляется наиболее методологически обоснованным, поскольку сводит к минимуму противоречия, возникающие при попытке включить «цифровые следы» в рамки устоявшейся классификации, что в конечном счёте приводит к игнорированию присущих им специфических особенностей.

Помимо всего прочего, необходимо также обратиться к проекту Концепции комплексного регулирования (правового регулирования) отношений, возникающих в связи с развитием цифровой экономики, предложенной Институтом законодательства и сравнительного правоведения при Правительстве РФ.

Пункт 4.7 концепции закрепляет классификацию «цифровых следов» на активные и пассивные. Данная классификация, наряду с сопутствующими разъяснениями, имплицитно указывает на сущность «цифровых следов» как данных, формируемых пользователем в информационных системах и порождаемых работой программного обеспечения [10].

Активный «цифровой след» является результатом осознанных, волевых действий субъекта, направленных на размещение или передачу информации в цифровой среде. Формирование активного «цифрового следа» также происходит при заполнении пользователем онлайн-форм (например, при подписке на рассылки) или при выражении согласия на использование файлов cookie.

Пассивный «цифровой след», в свою очередь, формируется в автоматическом режиме независимо от прямого волеизъявления пользователя в процессе его взаимодействия с информационными системами. К данной категории относятся сведения, собираемые программными средствами в фоновом режиме: данные о сессиях, IP-адресах, геолокации, статистике посещений веб-ресурсов и др. [23, с. 294].

В качестве ещё одного классификационного критерия «цифровых следов» выступает способ доступа к ним, позволяющий дифференцировать их на локальные и удалённые [11, с. 345].

Локальный доступ предполагает непосредственное физическое взаимодействие с носителем информации, что обеспечивает реализацию комплекса криминалистических мероприятий: от обнаружения и фиксации до изъятия и последующего исследования объектов.

В случае с удалёнными следами доступ к информации возможен исключительно посредством телекоммуникационных сетей. Подобная специфика исключает возможность изъятия носителя в традиционном криминалистическом понимании, обуславливая необходимость применения иных процессуальных приёмов, таких как удалённое копирование данных или дистанционная фиксация содержимого [19, с. 223].

Предложенные в доктрине классификации «цифровых следов», как отмечалось, не являются исчерпывающими. При этом они объективно необходимы для формирования целостного представления об изучаемом явлении. Многообразие критериев классификации «цифровых следов» отражает сложность и динамичность данного объекта криминалистического познания. Несмотря на отсутствие единого, универсально признанного подхода, представленная систематизация имеет важное прикладное значение. Она позволяет правоприменителю оперативно определять тактику работы с различными видами «цифровых следов»: от выбора средств поиска и способов фиксации до оценки их доказательственного значения. В конечном счёте, классификация выступает необходимым инструментом, преобразующим теоретические знания в практико-ориентированные методы криминалистического расследования преступлений.

Переходя к анализу законодательства, необходимо констатировать, что правовая природа «цифровых следов» на данный момент не получила единообразного законодательного определения. Законодатель ещё не успел сформировать позицию относительно их природы, вследствие этого данная сфера характеризуется неурегулированностью.

Интересно, что нормативное признание понятия «цифровой след» находит отражение в ведомственных актах. В этой связи необходимо выделить профессиональный стандарт, утвержденный Министерством труда и социальной защиты РФ, который содержит понятие «цифровой след» [16]. Введение должностей «техник по сбору «цифрового следа» и «специалист по сбору «цифрового следа» свидетельствует о признании данной категории в качестве объекта профессиональной деятельности. В разделе 3.4.1 документа детально регламентированы трудовые функции специалиста, такие как «проектирование и моделирование процессов и алгоритмов потоков данных «цифрового следа» человека (группы людей) и ИКС», «проектирование процесса передачи и хранения данных «цифрового следа» и др.

Анализ специального законодательства также демонстрирует наличие правового пробела в отношении нормативной регламентации «цифровых следов». Вместе с тем, в научной литературе предлагаются подходы, основанные на расширительном толковании положений ряда федеральных законов (далее – ФЗ), что в некоторой степени позволяет восполнить данный пробел применительно к изучаемой категории.

Как указывает учёный А. Н. Мочалов, к «цифровым следам» в полной мере применимы нормы, регулирующие распространение информации [14, с. 169]. В качестве примера можно привести положения ФЗ от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» [27].

В тоже время при наличии в «цифровом следе» персональных данных (анкетных сведений из профиля пользователя, IP-адресов и др.) к нему применяются положения ФЗ от 27.07.2006 №152-ФЗ «О персональных данных» в части порядка обработки таких данных с учётом обязательных условий, среди которых – наличие согласия субъекта, соответствие заявленным целям и обеспечение защиты от несанкционированного доступа [20].

К слову, предложенная интерпретация положений настоящего ФЗ находит своё подтверждение в европейском законодательстве, в частности, в п. 18 преамбулы Общего регламента ЕС о защите данных (GDPR) [17]. Данный документ закрепляет, что сетевые идентификаторы могут оставлять следы, которые в сочетании с уникальными идентификаторами и другой полученной серверами информацией могут в дальнейшем использоваться для отождествления физических лиц. Вместе с тем, акт детально регламентирует пределы использования подобных данных, а также определяет их правовую квалификацию.

Исходя из вышесказанного, можно констатировать наличие правового «парадокса». В то время как профессиональная деятельность, связанная с работой с «цифровыми следами», активно институционализируется (о чём свидетельствует разработка соответствующих профессиональных стандартов), а судебная практика последовательно накапливается, сама правовая категория «цифровой след» по-прежнему лишена чёткого законодательного регулирования. Законодательство в его текущем виде не позволяет должным образом урегулировать правовое положение «цифровых следов», ввиду чего распространение на них положений существующих актов возможно преимущественно за счёт расширительного толкования.

Следует отметить, что вопрос о необходимости нормативной регламентации «цифрового следа» регулярно актуализируется на экспертных мероприятиях. Показательным примером служит инициатива учёного Э. Л. Сидоренко, озвученная

26.10.2023 г. на II Международной конференции «Цифровые международные отношения – 2023». Эксперт предложила законодательно закрепить статус «цифрового следа», определив его в качестве объекта правовой охраны [7].

Учитывая вышеизложенное, в целях преодоления правовой неопределённости представляется необходимым закрепить понятие «цифровой след». Опираясь на результаты проведённого анализа, предлагается следующая формулировка данной дефиниции: «цифровой след» – это зафиксированная в электронной форме информация, возникающая в результате взаимодействия субъекта с информационно-телекоммуникационными системами, а также в ходе автоматизированного функционирования программно-аппаратных средств, отражающая параметры активности пользователя». Первоначально нормативное закрепление предлагаемой дефиниции целесообразно осуществить в рамках ФЗ от 27.07.2006 №152-ФЗ «О персональных данных» [28]. Такой подход обусловлен тем, что значительный объем сведений, формирующих «цифровой след», обладает конфиденциальным характером, что напрямую связано с предметом регулирования настоящего закона и необходимостью защиты прав субъектов от несанкционированного доступа.

В тоже время в контексте совершенствования уголовно-процессуального законодательства, исходя из специфики изученной категории, представляется целесообразным дополнить ч. 2 ст. 74 УПК РФ новым видом доказательств – «результаты исследования «цифровых следов» [26]. Предлагаемая формулировка может быть следующей: «в качестве доказательств признаются данные, полученные из информационно-телекоммуникационных сетей (в том числе из социальных сетей, облачных хранилищ, мессенджеров и электронных почтовых сервисов), содержащие сведения, имеющие значение для установления обстоятельств совершения преступления, личности подозреваемого (обвиняемого), мотивов и иных подлежащих доказыванию фактов, при условии их процессуального закрепления в порядке, установленном настоящим Кодексом».

Подводя итог, следует констатировать: существующая нормативная база не всегда соответствует новым технологическим реалиям, что создаёт некоторый правовой пробел в вопросах работы с «цифровыми следами». Анализ показал, что без законодательного закрепления данной категории правоприменитель остаётся ограниченным в возможности полноценного использования доказательственного потенциала информации, получаемой в результате исследования «цифровых следов».

Резюмируя изложенное, можно прийти к выводу о необходимости комплексного совершенствования законодательства, во-первых, путём закрепления дефиниции «цифровой след» в структуре ФЗ от 27.07.2006 №152-ФЗ «О персональных данных», что обеспечит системную охрану прав граждан при обороте таких данных, а во-вторых, посредством процессуального закрепления «результатов исследования «цифровых следов» в качестве самостоятельного вида доказательств в ч. 2 ст. 74 УПК РФ. Реализация данных предложений позволит устранить неопределённость в квалификации «цифровых следов», создаст условия для единообразия следственной и судебной практики, а также обеспечит надёжную защиту прав субъектов в цифровом пространстве.

#### **Список литературы:**

1. Агибалов В. Ю. Виртуальные следы в криминалистике и уголовном процессе / В. Ю. Агибалов. – Москва: Юрлитинформ, 2012. 152 с.
2. Бахтеев Д. В. Криминалистические особенности производства процессуальных действий с цифровыми следами / Д. В. Бахтеев, Е. В. Смахтин // Российский юридический журнал. 2019. № 6(129). С. 61-68.

3. Бессонов А. А. О некоторых возможностях современной криминалистики в работе с электронными следами / А. А. Бессонов // Вестник Университета имени О. Е. Кутафина. 2019. № 3 (55). С. 46-52.
4. Борисов В. В. Об особенностях фиксации информационных следов в практике защиты информации / В.В. Борисов // Известия ЮФУ. Технические науки. 2009. №5. С. 164-168.
5. Вехов В. Б. Электронные следы в системе криминалистики / В. Б. Вехов, Б. П. Смагоринский, С. А. Ковалев // Судебная экспертиза. 2016. № 2(46). С. 10-19.
6. Вехов В. Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки / В. Б. Вехов. – Волгоград: МВД России, 2008. 404 с.
7. В России предложили принять закон о «цифровом следе». – Текст: электронный // Сетевое издание «74.ru»: [сайт]. – URL: <https://74.ru/text/world/2023/10/26/72850130/> (дата обращения:11.04.2026).
8. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ (ред. от 31.07.2025) // Собрание законодательства РФ. 05.12.1994. № 32. Ст. 3301.
9. Давыдов В. О. Значение виртуальных следов в расследовании преступлений экстремистского характера / В. О. Давыдов, А. Ю. Головин // Известия ТулГУ. Экономические и юридические науки. 2016. №3-2. С. 254-259.
10. Концепции комплексного регулирования (правового регулирования) отношений, возникающих в связи с развитием цифровой экономики. – Текст: электронный // URL: <https://clc.li/усKsd> (дата обращения:11.04.2026).
11. Кушнарев А. С. Цифровые следы в криминалистике, их использование при расследовании преступлений / А. С. Кушнарев // Вопросы российской юстиции. 2024. №32. С. 338-351.
12. Куртбединова Л. Р. Возможности использования ИИ в судебно-экспертной деятельности / Л. Р. Куртбединова, Е. С. Туманова, С. А. Торопов // Охрана и защита прав и законных интересов в современном праве: Сборник статей по результатам IV международной научно-практической конференции, Симферополь, 13 декабря 2024 года. – Симферополь: ООО «Издательство Типография «Ариал», 2025. С. 899-904.
13. Мещеряков В. А. Преступления в сфере компьютерной информации: основы теории и практики / В. А. Мещеряков. – Воронеж: Воронежский государственный университет, 2002. 408 с.
14. Мочалов А. Н. Цифровые следы человека и неприкосновенность частной жизни / А. Н. Мочалов // Антиномии. 2024. № 4. С. 164-189.
15. Поляков В. В. К вопросу об использовании понятия «виртуальные следы» и «электронно-цифровые следы» в криминалистике / В. В. Поляков, А. В. Шебалин // Актуальные проблемы борьбы с преступлениями и иными правонарушениями. 2013. № 13-1. С. 123-125.
16. Приказ Минтруда России от 09.07.2021 № 462н «Об утверждении профессионального стандарта Специалист по моделированию, сбору и анализу данных цифрового следа». – Текст: электронный // Судебные и нормативные акты РФ: [сайт]. – URL:

<https://sudact.ru/law/prikaz-mintruda-rossii-ot-09072021-n-462n/> (дата обращения: 11.04.2026).

17. Регламент Европейского Парламента и Совета Европейского Союза 2016/679 от 27 апреля 2016 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных / General Data Protection Regulation / GDPR). – Текст: электронный // СПС «Гарант»: [сайт]. – URL: <https://base.garant.ru/71936226/> (дата обращения: 11.04.2026).
18. Россинская Е. Р. Концепция цифровых следов в криминалистике // Аубакировские чтения: материалы международной научно-практической конференции, Алматы, 19 февраля 2019 года / Е. Р. Россинская, И. А. Рядовский. – Алматы: Қазақстан Республикасы ИМ М. Есболатов атындағы Алматы академиясының ҒЗЖРБЖҰБ, 2019. – Текст: электронный // НЭБ eLIBRARY.RU: [сайт]. – URL: <https://elibrary.ru/item.asp?id=39322850> (дата обращения: 11.04.2026).
19. Рудик М. В. Несовершеннолетний как субъект преступлений в сфере компьютерной информации / М. В. Рудик, С. А. Торопов // Евразийский юридический журнал. 2016. № 3(94). С. 222-225.
20. Серова А. А. Цифровой след как объект правовой охраны: правовые и этические аспекты / А.А. Серова // Молодой ученый. 2026. № 4 (607). – Текст: электронный // URL: <https://moluch.ru/archive/607/132813> (дата обращения: 11.04.2026).
21. Смушкин А. Б. Виртуальные следы в криминалистике / А. Б. Смушкин // Законность. 2012. № 8(934). С. 43-45.
22. Торопов С. А. Актуальные вопросы борьбы с преступностью в сфере компьютерной информации / С. А. Торопов, Д. А. Сафонов // Личность в информационном пространстве: проблемы и перспективы исследования: Монография / Под редакцией С. А. Буткевича. – Симферополь: Полипринт, 2020. С. 198-207.
23. Торопов С. А. Анализ причин и условий, способствующих совершению преступлений в сфере компьютерной информации / С. А. Торопов, А. В. Пономарев, Т. Ю. Новикова // Евразийский юридический журнал. 2022. № 9(172). С. 294-295.
24. Торопов С. А. Возможности использования искусственного интеллекта для решения задач судебной экспертизы / С. А. Торопов // Охрана и защита прав и законных интересов в современном праве: Сборник статей по результатам III международной научно-практической конференции, Симферополь, 15 декабря 2023 года. – Симферополь: Общество с ограниченной ответственностью «Издательство Типография «Ариал», 2024. С. 328-333.
25. Торопов С. А. Перспективы использования искусственного интеллекта и робототехники в деятельности правоохранительных органов / С. А. Торопов, А. В. Пономарев // Охрана и защита прав и законных интересов в современном праве: Сборник статей по результатам IV международной научно-практической конференции, Симферополь, 13 декабря 2024 года. – Симферополь: Общество с ограниченной ответственностью «Издательство Типография «Ариал», 2025. С. 158-163.

26. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 08.03.2026) // Собрание законодательства РФ. 24.12.2001. № 52. Ст. 4921.
27. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 29.12.2025) «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ. 31.07.2006. №31. Ст. 3448.
28. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 24.06.2025) «О персональных данных» // Собрание законодательства РФ. 31.07.2006. №31. Ст. 3451.
29. Федеральный закон от 31.07.2020 № 259-ФЗ (ред. от 15.12.2025) «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» Собрание законодательства РФ. 03.08.2020. № 31. Ст. 5018.
30. Хохлов Д. Г. Введение в системное программирование: Учебное пособие / Д. Г. Хохлов, З. Х. Захарова. – Казань: Изд-во Казан. гос. техн. ун-та, 2005. 163 с.

### References:

1. Agibalov V. Yu. Virtual traces in criminalistics and criminal procedure / V. Yu. Agibalov. Moscow: Yurlitinform, 2012. 152 p.
2. Bakhteev D. V. Criminalistic features of the production of procedural actions with digital traces / D. V. Bakhteev, E. V. Smakhtin // Russian Law Journal. 2019. No. 6(129). pp. 61-68.
3. Bessonov A. A. On some possibilities of modern criminalistics in working with electronic traces / A. A. Bessonov // Bulletin of the O. E. Kutafin University. 2019. No. 3 (55). pp. 46-52.
4. Borisov V. V. On the features of fixing information traces in the practice of information protection / V.V. Borisov // Izvestiya SFU. Technical sciences. 2009. No. 5. pp. 164-168.
5. Vekhov V. B. Electronic traces in the system of criminalistics / V. B. Vekhov, B. P. Smagorinsky, S. A. Kovalev // Forensic examination. 2016. No. 2(46). pp. 10-19.
6. Vekhov V. B. Fundamentals of criminalistic teaching on the study and use of computer information and its processing tools / V. B. Vekhov. – Volgograd: The Ministry of Internal Affairs of Russia, 2008. 404 p.
7. In Russia, it was proposed to adopt a law on the "digital footprint". – Text: electronic // Online publication "74.ru": [website]. – URL: <https://74.ru/text/world/2023/10/26/72850130> / (date of request:04/11/2026).
8. The Civil Code of the Russian Federation (part one) dated 11/30/1994 No. 51-FZ (as amended on 07/31/2025) // Collection of Legislation of the Russian Federation. 05.12.1994. No. 32. St. 3301.
9. Davydov V. O. The importance of virtual footprints in the investigation of crimes of an extremist nature / V. O. Davydov, A. Y. Golovin // Izvestiya TulsU. Economic and legal sciences. 2016. No. 3-2. pp. 254-259.
10. Concepts of complex regulation (legal regulation) of relations arising in connection with the development of the digital economy. – Text: electronic // URL: <https://clc.li/ycKsd> (date of request:04/11/2026).

11. Kushnarev A. S. Digital footprints in criminology, their use in the investigation of crimes / A. S. Kushnarev // Issues of Russian justice. 2024. No. 32. pp. 338-351.
12. Kurtbedinova L. R. Possibilities of using AI in forensic expertise / L. R. Kurtbedinova, E. S. Tumanova, S. A. Toropov // Protection and protection of rights and legitimate interests in modern law: Collection of articles based on the results of the IV International Scientific and Practical Conference, Simferopol, December 13, 2024. Simferopol: Arial Printing House, LLC, 2025. pp. 899-904.
13. Meshcheryakov V. A. Crimes in the field of computer information: fundamentals of theory and practice / V. A. Meshcheryakov. Voronezh: Voronezh State University, 2002. 408 p.
14. Mochalov A. N. Digital traces of a person and the inviolability of private life / A. N. Mochalov // Antinomies. 2024. No. 4. pp. 164-189.
15. Polyakov V. V. On the use of the concepts of "virtual footprints" and "electronic digital footprints" in criminology / V. V. Polyakov, A.V. Shebalin // Actual problems of combating crimes and other offenses. 2013. No. 13-1. pp. 123-125.
16. Order of the Ministry of Labor of the Russian Federation dated 07/09/2021 No. 462n "On approval of the professional standard Specialist in Modeling, Collecting and analyzing Digital Footprint data". – Text: electronic // Judicial and regulatory acts of the Russian Federation: [website]. – URL: <https://sudact.ru/law/prikaz-mintruda-rossii-ot-09072021-n-462n/> (date of request:11.04.2026).
17. Regulation of the European Parliament and of the Council of the European Union 2016/679 of April 27, 2016 on the protection of individuals with regard to the processing of personal data and on the free circulation of such data, as well as repealing Directive 95/46/EC (General Data Protection Regulation /GDPR). – Text: electronic // SPS "Garant": [website]. – URL: <https://base.garant.ru/71936226/> (date of request:11.04.2026).
18. Rossinskaya E. R. The concept of digital footprints in criminalistics // Aubakirov readings: proceedings of the international scientific and practical conference, Almaty, February 19, 2019 / E. R. Rossinskaya, I. A. Ryadovsky. – Almaty: Kazakhstan Republikasy II M. Esbolatov atyndagy Almaty akademiya syn Gzzhrbzhub, 2019. – Text: electronic // eLIBRARY.RU: [website]. URL: <https://elibrary.ru/item.asp?id=39322850> (date of request:11.04.2026).
19. Rudik M. V. A minor as a subject of crimes in the field of computer information / M. V. Rudik, S. A. Toropov // Eurasian Law Journal. 2016. No. 3(94). pp. 222-225.
20. Serova A. A. Digital footprint as an object of legal protection: legal and ethical aspects / A.A. Serova // Young Scientist. 2026. No. 4 (607). – Text: electronic // URL: <https://moluch.ru/archive/607/132813> (date of request:04/11/2026).
21. Smushkin A. B. Virtual traces in criminology / A. B. Smushkin // Legality. 2012. No. 8(934). pp. 43-45.
22. Toropov S. A. Actual issues of combating crime in the field of computer information / S. A. Toropov, D. A. Safonov // Personality in the information space: problems and prospects of research: Monograph / Edited by S. A. Butkevich. Simferopol: Polyprint, 2020. pp. 198-207.
23. Toropov S. A. Analysis of the causes and conditions contributing to the commission of crimes in the field of computer information / S. A. Toropov, A.V. Ponomarev, T. Y. Novikova // Eurasian Law Journal. 2022. No. 9(172). pp. 294-295.

24. Toropov S. A. Possibilities of using artificial intelligence to solve problems of forensic examination / S. A. Toropov // Protection and protection of rights and legitimate interests in modern law: Collection of articles based on the results of the III International Scientific and Practical Conference, Simferopol, December 15, 2023. – Simferopol: Limited Liability Company "Publishing House Printing House "Arial", 2024. pp. 328-333.
25. Toropov S. A. Prospects of using artificial intelligence and robotics in the activities of law enforcement agencies / S. A. Toropov, A.V. Ponomarev // Protection and protection of rights and legitimate interests in modern law: Collection of articles based on the results of the IV International Scientific and Practical Conference, Simferopol, December 13, 2024. – Simferopol: Limited Liability Company "Publishing House Printing House "Arial", 2025. pp. 158-163.
26. Criminal Procedure Code of the Russian Federation No. 174-FZ dated December 18, 2001 (as amended on 03/08/2026) // Collection of Legislation of the Russian Federation. 12/24/2001. No. 52. Art. 4921.
27. Federal Law of 27.07.2006 No. 149-FZ (as amended on 12/29/2025) "On information, information Technologies and information Protection" // Collection of Legislation of the Russian Federation. 07/31/2006. No. 31. Art. 3448.
28. Federal Law of 27.07.2006 No. 152-FZ (as amended on 06/24/2025) "On personal data" // Collection of Legislation of the Russian Federation. 07/31/2006. No. 31. St. 3451.
29. Federal Law No. 259-FZ dated 07/31/2020 (as amended on 12/15/2025) "On Digital Financial Assets, Digital Currency and on Amendments to Certain Legislative Acts of the Russian Federation" Collection of Legislation of the Russian Federation. 08/03/2020. No. 31. St. 5018.
30. Khokhlov D. G. Introduction to system programming: A textbook / D. G. Khokhlov, 3. X. Zakharova. – Kazan: Publishing House of Kazan State Technical University. University, 2005. 163 p.