

она неполно, односторонне отражает объективный мир. Реконструируя тот или иной предмет действительности идеально, т. е. в мышлении, научная теория абстрагируется от многих свойств его, выделяет только некоторые из них и делает их своими объектами. Исходя из данного признака, можно говорить, что в многогранной деятельности прокурора, осуществляющего надзор в досудебном производстве и уголовное преследование от имени государства, следует вычленять только одну сторону – применение криминалистических знаний, навыков и умений;

непротиворечивость – это условие, которому должна удовлетворять любая теория независимо от характера ее предметной области. Непротиворечивой считается лишь та теория, у которой любые два ее научных положения логически совместимы друг с другом [1, с. 103–106].

Криминалистическое обеспечение деятельности прокурора как частная теория изучает те явления, факты процессы, связи и отношения, которые отражают объективные закономерности, связанные с деятельностью прокурора в уголовном судопроизводстве. В свою очередь, данные закономерности составляют предмет теории криминалистического обеспечения деятельности прокурора. К таким закономерностям относятся закономерности возникновения и сохранения информации о преступлении, отраженной в объективной действительности, включая материалы уголовного дела; закономерности изучения прокурором материалов проверки заявления (сообщения) о преступлении и уголовного дела; закономерности реализации прокурором предоставленных ему процессуальных и надзорных полномочий в сфере уголовного судопроизводства. В предмет теории входят также ее общенаучные проблемы: система, задачи, методы, история развития этой части науки, ее место в системе криминалистики и взаимосвязи с другими науками, понятие, виды, требования, предъявляемые к научным рекомендациям в зависимости от вида преступления прокурору, категориальный аппарат и другие науковедческие вопросы.

Исследование предмета теории криминалистического обеспечения деятельности прокурора в уголовном судопроизводстве должно осуществляться с позиций системного подхода, предполагающего необходимость и возможность выделения отдельных элементов системы, находящихся между собой в определенной взаимосвязи. При этом отдельные элементы предмета названной теории целесообразно упорядочить в некоторые подмножества путем их группировки, осуществляемой путем отбора в пределах того или иного множества фактов, содержащих наибольшее количество информации, и поддаются вычленению без введения для этого каких-либо добавочных правил, кроме операций непо-

средственного «связывания» одних фактов с другими по их подобию или наличию аналогичных признаков. В философии выделяют два типа такого связывания: квантификация и классификация [1, с. 60–63]. Мы полагаем, что квантификация, представляющая собой сведение качественных характеристик к количественным, не применима к рассматриваемым нами явлениям. Следовательно, упорядочение элементов предмета теории должно осуществляться путем их классификации.

Результаты теоретических исследований должны позволить сделать обобщение полученных знаний, логический переход от частного к общему, иначе говоря, провести генерализацию подмножеств, образующих предмет рассматриваемой нами теории.

1. Логика научного исследования / П.В. Копнин [и др.]; отв. ред. П.В. Копнин, М.В. Попович. М., 1965.
2. Добрянов В.С. Методологические приемы теоретического и исторического познания. М., 1968.
3. Поврезнюк Г.И. Криминалистические методы и средства установления личности в процессе расследования преступлений: по материалам стран СНГ. М., 2005.

УДК 343.98

*С.Ю. Скобелин*

## **ЦИФРОВЫЕ СЛЕДЫ ПРЕСТУПЛЕНИЙ И СПОСОБЫ РАБОТЫ С НИМИ**

Компьютеризация жизнедеятельности человека не могла не отразиться на преступности и на способах противодействия этому социальному явлению. Развитие компьютерных технологий, мобильной связи, сети Интернет по всему миру привело к тому, что современный человек уже не мыслит себя без использования электронных технических средств и их возможностей.

Ноутбук, планшет, цифровой браслет (часы), электронная книжка, смартфон или простой сотовый телефон имеются практически у каждого взрослого человека и даже ребенка. Все эти электронные устройства напрямую связаны с окутавшим мир интернетом, часто синхронизированы между собой. Одним из основных способов передачи информации и общения между людьми (текстовые сообщения, звуковые сигналы, изображения, видео) стали программы мгновенного обмена сообщениями – мессенджеры (WhatsApp, Viber, Telegram, Skype, Facebook, Line,

WeChat и др.), социальные сети (ВКонтакте, Instagram, Одноклассники, Facebook, Twitter), электронная почта и др. Жизнедеятельность человека в населенных пунктах, на транспорте, в помещениях, жилых домах и даже в космосе фиксируется с помощью систем цифровой видеозаписи.

Многофункциональность и постоянное совершенствование цифровых устройств, различных программ и приложений только расширяет пользовательские и, соответственно, криминалистические возможности.

В этой связи в криминалистической теории наблюдается тенденция изучения так называемых цифровых (электронных, виртуальных, компьютерных) следов преступной деятельности в следующих основных направлениях:

1. В узком направлении – это предупреждение, раскрытие и расследование собственно преступлений в сфере компьютерной информации (гл. 28 УК РФ).

Данные преступления (неправомерный доступ к компьютерной информации (ст. 272 УК РФ), создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ) и др. чаще являются предикатными для совершения (или сокрытия) других преступлений: хищений, распространения экстремистских материалов, фальсификации итогов голосования и др.

2. В широком направлении – это противодействие киберпреступности (в сфере информационных технологий), то есть не только преступлений, указанных выше, но и совершенных с использованием компьютерных и телекоммуникационных технологий (чаще – сети Интернет и сотовой связи).

Речь идет о доведении с использованием сети Интернет до самоубийства или склонении к самоубийству; дистанционных хищениях в финансово-банковской сфере; призывах к осуществлению террористической, экстремистской деятельности, массовым беспорядкам; сбыте наркотических средств, оружия; обороте порнографических материалов или предметов порнографического содержания, организации азартных игр, преступлениях против половой неприкосновенности несовершеннолетних и др.

При этом темпы роста указанных преступлений колоссальны. Согласно данным ФКУ «Главный информационно-аналитический центр МВД России» в 2018 г. количество подобных преступлений составило 132 733 (7 % от всех зарегистрированных преступлений), это более чем в два раза (112,7 %) превысило аналогичный показатель за 2017 г. А уже в 2019 г., согласно статистическим данным, таких преступлений было зарегистрировано 294 409 (14,5 % в общем числе выявленных преступлений), а это на 70 % превышает аналогичный период 2018 г. Пред-

ставляется, что тенденция увеличения преступлений, совершенных таким способом, будет продолжаться.

Половина таких преступлений – это тяжкие и особо тяжкие (48 %), совершенные с использованием сети Интернет (53 %), а более трети (38,5 %) – с помощью средств мобильной связи. Немало преступлений совершается с использованием расчетных (пластиковых) карт, компьютерной техники, программных средств, фиктивных электронных платежей.

Относительно видов преступной деятельности в основном (79 %) это кражи или мошенничества, а также преступления, связанные с незаконным оборотом (производство, сбыт, пересылка) наркотических средств (9 %). Были выявлены также совершенные рассматриваемым способом следующие преступления: незаконные организация и проведение азартных игр (ст. 171.2 УК РФ), изготовление порнографических материалов (ст. 242, 242.1, 242.2 УК РФ), публичные призывы к осуществлению террористической деятельности (ст. 205.2 УК РФ), публичные призывы к осуществлению экстремистской деятельности (ст. 280 УК РФ).

В то же время анализ следственной практики свидетельствует о том, что цифровые следы в криминалистике следует рассматривать значительно шире. Они актуальны при проведении процессуальных проверок и расследовании любых преступлений независимо от объекта и способа посягательства, категории или формы вины, осведомленности или неосведомленности лица об их оставлении, а также принадлежности тому или иному участнику уголовного процесса (подозреваемый, потерпевший или свидетель). Интерес представляют и цифровые способы доказывания преступной деятельности, использование высокотехнологичной криминалистической техники и специализированных программ для получения значимой для следствия информации при осмотре или проведении экспертных исследований гаджетов пользователей, аналитике большого объема биллинговой информации и пр.

Специфику приобретают и неординарные способы доказывания таких преступлений, объективная сторона которых выражается в распространении какой-либо информации (ст. 110.2, 128.1, 137, 185.1, 179, 283.1 УК РФ), либо публичных призывах к противоправной деятельности (ст. 212, 242, 280, 354.1 УК РФ). Это осмотры социальных сетей пользователей (отправителя – получателя), их электронных устройств и фотофиксация (скриншоты) страниц, на которых отображается количество и адреса отправленных сообщений, фото-видеофайлов, просмотров, лайков, дизлайков, комментариев. Суды и присяжные заседатели положительно воспринимают подобную практику, она достоверна и надежна.

Актуальность раскрытия и расследования преступлений, где в качестве средств и способов совершения используются информационно-

телекоммуникационные технологии, привела к созданию в правоохранительных органах специализированных подразделений: технико-криминалистическое управление, а также специализированные экспертные подразделения в Главном управлении криминалистики (Криминалистическом центре) Следственного комитета Российской Федерации, управления «К» в МВД России и др.

Для борьбы с IT-преступлениями в 2019 г. распоряжением Председателя Следственного комитета Российской Федерации А.И. Бастрыкина в Главном следственном управлении создано специализированное подразделение – отдел по расследованию киберпреступлений и преступлений в сфере высоких технологий. В обосновании необходимости создания данного отдела отмечалась особая специфика и сложность таких преступлений, их неочевидность, межрегиональный и международный характер.

В Московской академии Следственного комитета Российской Федерации тематика и тонкости работы с цифровыми следами включены в учебные планы и рабочие программы дисциплин «Криминалистика», «Фото-видеозапись следственных действий» и «Технико-криминалистическое обеспечение расследования преступлений». Кроме того, студенты, направляемые от следственных органов Следственного комитета России обучаются в МГТУ им. Н.Э. Баумана, где создана специальная кафедра «Цифровая криминалистика».

В современной следственной практике при доказывании виновности (невиновности) подозреваемых чаще всего встречаются следующие цифровые следы:

видеофиксация (как самими преступниками, так и произведенная помимо их воли) подготовки, совершения, сокрытия преступлений;

биллинговая информация о соединениях между абонентами (абонентскими устройствами);

информация, содержащаяся в памяти (облачное хранилище) смартфона, телефона участника уголовного судопроизводства;

криминалистически значимая информация, находящаяся в памяти домашнего (рабочего) компьютера (ноутбука, планшета, моноблока) участника;

метаданные и цифровая информация различных гаджетов, позволяющая определить местонахождение гаджета и его владельца;

социальные сети как источник криминалистически значимой информации;

данные истории браузера пользователя;

данные дистанционного зондирования поверхности Земли;

цифровые данные компьютерных систем авто-мото транспорта в раскрытии и расследовании преступлений (датчики EDR и IV).

Обнаружение, фиксация, изъятие и исследование такой информации имеет свою специфику. Для этого используются современная высокотехнологичная техника (Мобильный криминалист, XRY, UFED), специальные программы для работы с цифровыми следами, тактические особенности получения и последующего использования цифровой информации при доказывании виновности (невиновности) лица в совершении преступления, разработаны рекомендации в повышении эффективности использования следователями цифровых следов в раскрытии и расследовании преступлений.

Грамотное и правильно процессуально оформленное обнаружение, фиксация, изъятие и сохранение цифровой информации в значительной мере способствует оперативному изобличению всех участников преступного события, розыску и задержанию последних, поиску скрытых трупов, похищенного и в целом обеспечению надежной доказательственной базы для органов следствия.

УДК 343.98

*О.А. Славгородская*

### **КРИМИНАЛИСТИЧЕСКОЕ ИЗУЧЕНИЕ СВИДЕТЕЛЯ И ЕГО ПРАВОВОЙ СТАТУС**

Необходимость расширения возможностей раскрытия, расследования и предупреждения преступлений ставит перед криминалистикой задачу поиска новых путей достижения данной цели. И актуальным в сложившейся ситуации становится не только расширение возможностей применения достижений технического характера, но и внимание к изучению объектов, относящихся к уже традиционным, но требующим переосмысления сложившихся подходов. К одному из направлений, расширяющих возможности получения криминалистически значимой информации о расследуемом событии, относится возможность получения сведений от свидетелей. Отношение к человеку как физических, биологических, психологических и социальных свойств, и существующих между ними взаимосвязей представляется устоявшимся и не требующим дополнительного обоснования [1, с. 35].

При рассмотрении полисистемного подхода к изучению участников уголовного судопроизводства в то же время необходимо выделять семь