В помощь лектору

УДК 343.98
DOI: 10.47905/MATGIP.2020.119.3.012

Лекция: Цифровые технологии современной криминалистики

А.И. Бастрыкин*

Аннотация. В данной лекции содержится теоретико-практический материал, отражающий дискуссионные вопросы внедрения цифровых технологий современной науки криминологии в Российской Федерации. Специально показывается, что развитие цифровых технологий предъявляет повышенные требования к обеспечению деятельности следователей при использовании цифровых технологий: при доказывании юридических фактов; оптимизации процессуальных и управленческих процессов, как на стадии возбуждения уголовного дела, так и в ходе расследования преступления; решении проблем, возникающих при внедрении новых информационных технологий в правоприменительную практику.

Автор предлагает внимательно проанализировать действующую нормативную правовую базу с целью ее корректировки в направлении повышения эффективности использования цифровых технологий в современной криминалистике.

Ключевые слова: уголовное законодательство, уголовно-процессуальное право, Следственный комитет, цифровые технологии, криминалистика.

Цифровизация общественных отношений, безусловно, диктует новые, ранее не известные подходы в криминалистической теории и практике. Анализ следственной практики отражает тот факт, что законодатель в данном направлении несколько отстает от развития высоких технологий, и, как следствие, в практической деятельности следователя часто возникают вопросы, требующие как научного обоснования, так и практической апробации и использования.

Данные проблемы вполне можно систематизировать и обозначить основные проблемы цифровизации.

Во-первых, это касается использования цифровых технологий при доказывании юридических фактов.

Речь идёт о современных возможностях сбора доказательственной информации как оперативно-розыскным, так и следственным путем а именно:

* ***Бастрыкин Александр Иванович,*** председатель Следственного комитета Российской Федерации, доктор юридических наук, профессор, Заслуженный юрист Российской Федерации. E-mail: lawinst-spb@mail.ru

✓ **Получения спутниковых фото изображений открытых участков местности за счет дистанционного зондирования поверхности Земли.** На сегодняшний день между Следственным комитетом Российской Федерации и Научным центром оперативного мониторинга Земли (НЦ ОМЗ) Российских космических систем (Роскосмос) заключено соглашение, согласно которому вся актуальная информация синхронизируется и поступает в Главное управление криминалистики (Криминалистический центр) СК России. Таким образом, любой следователь имеет возможность оперативно через электронную почту получить информацию о наличии необходимых кадров в интересующее время в конкретном месте.

Так, в Республике Адыгея, следователем была доказана вина лица в совершении преступлений, предусмотренных ст. 171 УК РФ «Незаконное предпринимательство» и ст. 198 УК РФ «Уклонение физического лица от уплаты налогов, сборов и (или) физического лица – плательщика страховых взносов от уплаты страховых взносов», который отказывался признать факт использования огороженной территории в качестве несанкционированной автостоянки. Фото из космоса не только подтвердили такие противоправные действия на протяжении длительного времени. Но и позволили посчитать количество автомобилей (легковых грузовых), которые парковались на стоянке.

Данные дистанционного зондирования Земли успешно использовались при расследовании фактов диверсионной и иной противоправной деятельности на территории Украины и России гр-ки Савченко Надежды.

✓ **Использование цифровых устройств автотранспорта.** Компьютерные системы автомототранспорта дают следствию достаточно полезную информацию о скорости автомобиля, весе пассажиров и водителя, маршрутах движения и др.

Например, регистратор данных о событии АВТО (EDR ACU) при аварии или при условия, приближенных к аварии, может сохранять (в зависимости от производителя устройства) до 60 аналоговых и 30 конкретных (вкл/выкл) параметров движущегося транспортного средства, многие из которых являются криминалистически значимыми. Среди таких параметров в течение некоторого временного интервала до столкновения (опрокидывания) могут фиксироваться:

– состояние защелки замка ремней безопасности водителя и пассажира, находившегося на переднем сиденье;
– положение рычага переключения передач;
– степень нажатия педали акселератора, тормоза;
– обороты двигателя;
– показания спидометра;
– повороты рулевого колеса;
– состояние систем ABS, ESP, SRS;
– время включения систем экстренного торможения
– сигналы от датчиков света и дождя.

Причем, информация в электронной памяти EDR непрерывно обновляется. При этом объем памяти некоторых моделей EDR позволяет сохранить посекундно регистрируемые данные за период времени, охватывающий

5 секунд до момента столкновения (опрокидывания), и заканчивая 1-й секундой после него.

✓ **Получение данных уличных, транспортных, внутренних видеокамер**. **Видеофиксация самих следственных действий.** Значение видеозаписи следственных действий переоценить сложно. Подобная дополнительная фиксация позволяет:

во-первых, сконцентрироваться следователю именно на сути и целях проведения следственного действия, его тактических приемах, установлении психологического непосредственного контакта с участниками, а не его документальном оформлении в виде механического составления протокола;

во-вторых, наглядно, неограниченное количество раз воспроизвести ход и содержание следственного действия, а не только его результат, акцентировать внимание следователя на ранее не замеченных деталях;

в-третьих, критически относится к изменению показаний лицом, так как подтверждает отсутствие какого-либо воздействия в отношении него, наводящих вопросов, а также фиксирует моральное и физическое состояние последнего;

в-четвертых, фиксировать невербальные реакции участника следственного действия (мимику, ритм и уверенность речи, реакции на поставленные вопросы, положение конечностей и т.п.) при ответе на поставленные следователем или иными участниками вопросы, имеющие значение для уголовного дела, демонстрации неопровержимых улик и пр.;

в-пятых, назначить судебную фоноскопическую и (или) психологическую экспертизы по видеозаписям следственных действий, в том числе на предмет исключения предполагаемого давления на лицо, возможных наводящих вопросов, дачи ложных показаний (психолого-вокалографическую экспертизу, психолого-лингвистическую или психолого-акмеологическую);

в-шестых, проводить следственное действие более эффективно и наступательно, не допускать нарушений законодательства и этических норм со стороны всех его участников;

в-седьмых, демонстрировать в судебном заседании видеозапись следственного действия, в том числе в случае неявки участников на заседание.

✓ **Содержащаяся в памяти цифровых устройств криминалистически значимая информация**. Повсеместное использование как потерпевшими, так и преступниками электронных устройств (сотовых телефонов, смартфонов, планшетных компьютеров, фитнес браслетов, чипированных билетов на транспорт, навигаторов, портативных устройств GPS и пр.) в приготовлении, совершении преступлений, сокрытии его следов, потребовало от криминалистов пересмотра современных возможностей по сбору доказательственной информации. Актуальным стал вопрос, связанный с изъятием, фиксацией и исследованием информации, содержащейся в таких средствах.

Ценность такой информации очевидна для выявления, раскрытия и расследования преступлений, идентификации неопознанных трупов и др. Ведь с помощью данной информации следователь может получить криминалистически важную доказательственную или ориентирующую информацию: определить местонахождение субъекта преступления, его соучастников,

свидетелей, потерпевших в определенное время, ознакомиться с журналом звонков, содержанием СМС-переписок, чатов, изучить журнал браузеров – страниц интернета на которые заходило лицо и т.д.

Получить данную информацию следователь может либо через оператора связи, либо непосредственно из электронного устройства, изъятого у лица.

Первым шагом на пути унификации действующего процессуального законодательства России и его адаптации, современным возможностям операторов мобильной связи в оказании помощи по раскрытию и расследованию преступлений, стало включение в УПК РФ ст. 186.1 – «Получение информации о соединениях между абонентами и (или) абонентскими устройствами» в систему следственных действий.

Сегодня следователи расширяют возможности такого следственного действия указывают в постановлении не только стандартно запрашиваемые сведения об абоненте, собеседнике, типе соединения, его дате, времени и продолжительности, но и азимут (угол между направлением на север (нулевой показатель компаса) и направлением на место нахождения абонента), time energy (время прохождения сигнала от устройства абонента до базовой станции). После получения данной информации следователи-криминалисты выезжают непосредственно к базовой станции и с использованием компаса и карты местности обозначают участок на котором находился проверяемый абонент. Также с помощью датчиков радиоэлектронной разведки устанавливают все базовые станции, на которые мог переключиться телефон пользователя.

Так, например, в республике Дагестан, следователю-криминалисту, работая по факту безвестного исчезновения предпринимателя при помощи азимута последнего соединения и пересечения векторов покрываемости предыдущих соединений удалось установить место его убийства. Тщательный осмотр места происшествия позволил обнаружить утопленное в море тело и выйти на след убийц (дочери пострадавшего и ее парня).

Часто место нахождения, интересующего следственные органы лица удается установить при условии изъятия гаджетов, которые постоянно находятся при этом лице и имеют встроенный приемный и передающий модуль GPS или ГЛОНАС (смартфон, планшет, электронные часы, книги, пульсометр, шагомер, фитнес-браслет, автомобильный регистратор). Данные устройства, при условии активации навигационной функции сохраняют в памяти данные о своем местонахождении (и, скорее всего, местонахождении пользователя). Также устройства пользователя с технологией беспроводной локальной сети WI-FI сохраняют информацию о месте и времени соединения с роутером;

«Помощниками» следствия в этом ключе выступают и медиа-файлы (фото, видео), хранящиеся в различных цифровых устройствах, социальных сетях. Большинство современных фото камер сохраняет данные о широте и долготе того места, где было сделано фотография или видеозапись. Проверить алиби лица можно с помощью изъятых у него билетов на транспорт, карт-пропусков, оснащённых микросхемами, которые срабатывают прикосновением к валидатору в наземном городском транспорте, метро, на проходных в различные учреждения.

Так, в Москве, по метаданным фотографии ковра сделанной похищенным ребенком в квартире насильника, был установлен адрес дома и путем поквартирного обхода квартира преступника. В ходе осмотра квартиры удалось изъять достаточное количество улик, подтверждающих вину лица и подтверждающую многоэпизодность его действий.

Причем поступившие в криминалистические подразделения датчики радиоэлектронной обстановки, а также находящиеся в свободном доступе программы Netmonitor, G-nettrack позволяют следователям самостоятельно или с привлечением специалиста в рамках следственного осмотра (эксперимента) отследить и зафиксировать в конкретном месте или по определенному маршруту базовые станции (2G, 3G,) всех операторов связи и сделать оператору точечный запрос с указанием идентификационных данных станций (LAC, CID – для типа сети 2G, 3G либо TAC и CL – для LTE).

Так, например, в городе Орле следователем-криминалистом было установлено место нахождения разыскиваемого убийцы несовершеннолетней девушки. Получив информацию от оператора связи и выяснив, что преступник соединяется через одни и те же базовые станции был организован выезд на место нахождения данных ретрансляторов, с помощью специализированных программ очерчены границы пребывания лица в условиях плотной застройки. Путем поквартирного обхода с фотографией убийцы, последний был обнаружен и задержан.

Данная информация при условии корректных исходных данных оператора и тщательном анализе (в том числе с использованием аппаратно-программных комплексов, стоящих на вооружении правоохранительных органов) позволяет установить информацию о районе пребывания абонента в определенное время, продолжительность пребывания в данном месте; подтвердить факт его нахождения на местах других (схожих) происшествий; проверить возможность одновременного пребывания подозреваемого и потерпевшего (подозреваемого с включенным телефоном потерпевшего) в одном месте в одно время.

Если же гаджет уже изъят следователем, то у него есть возможность его осмотра с использованием высокотехнологичной криминалистической техники. К примеру, аппаратно-программного комплекса «Мобильный криминалист» либо «UFED» он может ознакомиться и с удаленными данными (журналом звонков, SMS, MMS, данные чатов, фото-видеофайлы, посещаемые интернет-ресурсы), которые помогают правильно выстроить версии по неочевидным преступлениям, доказать вину (невиновность) проверяемого лица, подтвердить приготовительные действия, либо действия по сокрытию следов преступления, установить дополнительного свидетеля или новый противоправный эпизод.

Так, в ходе расследования факта совершения насильственных действий сексуального характера в отношении несовершеннолетней Головановой О.В. (Амурская область) подозреваемые Кузнецов Т.Ш. и Иванищев М.О. свой вину полностью отрицали.

Осмотр с помощью комплекса UFED изъятых у них сотовых телефонов позволил восстановить и скопировать ранее удаленные файлы видео-

записей, на одной из которой был запечатлен процесс совершения преступных действий.

При этом кадр видеозаписи зафиксировал четко видимый номерной знак автомобиля преступников, марку которого и, тем более, номерной знак потерпевшая назвать не могла. В ходе проведенных следственных и оперативно-розыскных мероприятий был установлен Ребров А.М. – основной исполнитель преступления, совершенного в отношении Головановой. Изъятая видеозапись стала решающим доказательством его вины.

Кроме того, применение UFED при осмотре сотовых телефонов, изымаемых по фактам смертельного железнодорожного травмирования, позволило в ряде случаев восстановить удаленные SMS-сообщения, свидетельствующие о суицидальных намерениях граждан.

На вооружении Главного управления криминалистики Следственного комитета Российской Федерации имеется аппаратно-программный комплекс «Сегмент-С», позволяющий проводить аналитическую работу сетей сотовой связи, выявлять возможное периодическое пересечение абонентов, их совместное нахождение, маршруты движения, точки последней регистрации и др.

Широкое распространение получает в криминалистике поисково-аналитическая работа в социальных сетях и изучение интернет-активности пользователя.

Комплекс ЛИС-М позволяет найти конкретного пользователя, наглядно отображает социальный граф пользователей и групп, а также решает такие задачи как поиск общих знакомых подозреваемого, выделение кластеров, вычисление метрик центральности.

Во-вторых, применение цифровых технологий для оптимизации процессуальных и управленческих процессов, как на стадии возбуждения уголовного дела, так и в ходе расследования преступления.

Очевидно, что современное уголовное судопроизводство имеет неуклонную тенденцию перехода в цифровой формат и это неизбежно. Речь идет о тех отечественных и зарубежных нормативных нововведениях касающихся повсеместного использования различных электронных устройств для объективизации и упрощения до следственных проверок, расследования уголовных дел и судебного производства.

Следует признать некоторое отставание отечественного уголовного процесса в данном направлении. Общение со следователями, изучение их повседневной работы свидетельствует о необходимости пересмотра некоторых консервативных подходов. Речь идет о возможности дистанционного (с помощью видеоконференцсвязи) допросов некоторых участников, нецелесообразности дублирования видеозаписи следственного действия и составления протокола, оперативных электронных запросов в порядке ст.21 УПК РФ и многое другое.

Работа следователя, как любая другая, должна идти в ногу со временем. В нашей стране развиваются высокие технологии и технологии искусственного интеллекта, но, к сожалению, не в области юриспруденции. Большая часть используемого программного обеспечения для юристов – это справочные системы (Консультант+, ГАРАНТ и т.д.). Этого, безусловно, не-

достаточно. До сих пор нет качественного и регулярно обновляемого автоматизированного рабочего места (АРМ) следователя, слабо используются технологии виртуальной реальности. Поэтому единственный путь для развития юридического прикладного программного обеспечения – это его разработка организацией самостоятельно. Именно по этому пути пошел и Следственный комитет Российской Федерации.

Информационная система «Электронный паспорт уголовного дела» была введена в действие Распоряжением СК России № 27/108р от 09.04.2014 г. По информации ГСУ по Северо-Кавказскому Федеральному округу на первое полугодие 2016 года в данной информационной системе содержится более 45 000 карточек уголовных дел, 600 учетных записей пользователей, загружено более 300 000 файлов, имеющих отношение к расследованию уголовных дел. Информационная система позволяет в режиме реального времени отслеживать ход расследования уголовного дела, контролировать исполнение указаний по уголовному делу, обеспечивать эффективный процессуальный контроль и планировать расследование уголовного дела.

Роль информационной системы «Электронный паспорт уголовного дела» не может быть преуменьшена. Она позволяет сократить бумажный документооборот и упростить процессуальный контроль расследуемых уголовных дел.

В то же время, как и любое программное обеспечение, оно не лишено недостатков. Большая часть из них проистекает из-за того, что система «Электронный паспорт уголовного дела» действует пока только на территории Южного и Северо-Кавказского федеральных округов. Данная система была разработана сотрудниками Следственного комитета и ими же поддерживается в актуальном и работоспособном состоянии. Масштабирование этой информационной системы на все управления Следственного комитета требует ее доработки. Можно внести ряд предложений по совершенствованию информационной системы «Электронный паспорт уголовного дела»:

1. Внести в информационную систему методические рекомендации и информационные материалы о результатах расследования различных категорий уголовных дел и проведении отдельных следственных действий.

2. Создать «Архив уголовных дел», чтобы при просмотре общего списка уголовных дел, расследуемых конкретным следственным отделом, открывались именно те дела, которые находятся в производстве в настоящий момент.

3. Для обеспечения полноты процессуального контроля расследования уголовных дел на всех стадиях уголовного судопроизводства внести в информационную систему «Электронный паспорт уголовного дела» книгу регистрации сообщений о преступлении каждого территориального следственного отдела в электронном виде.

Также необходимо отметить, что целесообразно расширить базу данных и подключить к ней все следственные управления Следственного комитета Российской Федерации.

В Московской академии Следственного комитета Российской Федерации, созданы все необходимые условия для освоения всех реализуемых обра-

зовательных программ путем целенаправленной организации учебного процесса, выбора форм, методов и средств обучения. Особое внимание уделяется активным формам проведения учебных занятий, которые обеспечивают быстрое усвоение учебного материала и формируют необходимые практические навыки, в том числе с использованием возможностей компьютерного класса.

Поэтому обучение руководителей навыкам работы в системе «Электронный паспорт уголовного дела» в рамках программ повышения квалификации будет способствовать более глубокому изучению всех ее возможностей.

В-третьих, это проблемы, возникающие при внедрении новых информационных технологий в правоприменительной практике.

Прежде всего, остановимся на юридической стороне вопроса, допустимости описанных выше действий следователя.

Действующее отечественное законодательство оставляет открытым вопрос о том, следует ли сотрудникам правоохранительных органов получать судебное решение на осмотр телефонов и содержащейся в них информации участников уголовного судопроизводства. Не оговаривается данная проблема и в Постановлении Пленума Верховного Суда РФ от 1 июня 2017 г. № 19 «О практике рассмотрения судами ходатайств о производстве следственных действий, связанных с ограничением конституционных прав граждан (статья 165 УПК РФ)» [1].

В этой связи среди научной общественности и практических работников есть различные мнения по данному вопросу, а также по вопросу с какой информацией, содержащейся в памяти телефона силовые ведомства вправе знакомиться без судебного решения, а с какой нет. Неоднозначно в этом направлении складывается и судебная практика [2, с. 58].

Некоторые авторы и представители прокуратуры, к примеру, предлагают в ходе осмотра мобильного телефона участников уголовного процесса не ограничиваться лишь внешним осмотром, а обращать внимание и отражать в протоколе технические характеристики, содержание памяти мобильного телефона, информацию об абонентских соединениях, СМС-сообщениях, использовать для осмотра специальные технические средства, позволяющие восстанавливать удаленные данные. Соответствующие указания находят отражение в актах прокурорского реагирования [3, с. 23].

Запрет на вмешательство в личную и семейную жизнь человека, на ознакомление с его корреспонденцией установлен в ст.12 Всеобщей Декларации прав человека, а также в ст. 8 Европейской Конвенции о защите прав человека и основных свобод. Причем в последней Конвенции отдельно подчеркивается *недопущение вмешательства государственных органов в осуществление данных прав*. В тоже время и в той и в другой Конвенции делается оговорка о том, что *в исключительных случаях, установленных законом подобное вмешательство всё-таки возможно*.

В ст. 23 Конституции РФ также провозглашается, что каждый имеет право на *тайну переписки*, телефонных переговоров, почтовых, телеграфных и *иных сообщений. Ограничение этого права допускается только на основании судебного решения*.

Так, отменяя постановление суда первой инстанции, судебная коллегия отметила следующее. При вынесении решения судом первой инстанции не учтены положения ст.23 Конституции РФ, а также требования ст.ст.13, 38 УПК РФ. Осмотр телефона не включает в себя осмотр его содержимого, так как сведения о телефонных соединениях, контактах и СМС-сообщениях защищаются Конституцией РФ.

Несмотря на то, что глава 25 УПК РФ прямо не закрепляет обязанность следователя получать судебное разрешение на осмотр СМС-переписки, эта обязанность вытекает из других норм как уголовно-процессуального закона и положений Конституции РФ, так и из международных норм, закрепленных в Конвенции о защите прав человека и основных свобод, подлежащих безусловному применению в РФ. Осмотр личной переписки, содержащейся в мобильном телефоне подозреваемого, с учетом природы и степени вмешательства фактически идентичен осмотру почтово-телеграфных отправлений либо телеграмм, для которого статьей 185 УПК РФ предусмотрена необходимость вынесения судебного решения.

При осмотре мобильного телефона, следователем подверглись тщательному описанию все соединения между абонентами, а именно между потерпевшим и теми лицами, которому он отправлял СМС-сообщения и от которых получал такие сообщения, вплоть до указания времени соединений, номеров телефонов и имен лиц, которые этими телефонами пользуются. При этом статья 186.1 УПК РФ предусматривает необходимость судебного разрешения на получение информации о соединениях между абонентами и (или) абонентскими устройствами [4].

Судебная коллегия по уголовным делам суда Ямало-Ненецкого автономного округа отметила, что информацией, составляющей охраняемую Конституцией РФ и действующими на территории РФ законами тайну телефонных переговоров, являются любые сведения, передаваемые, сохраняемые и устанавливаемые с помощью телефонной аппаратуры, включая данные о входящих и исходящих сигналах соединения телефонных аппаратов конкретных пользователей связи, поэтому для получения такого рода сведений органами, осуществляющими расследование преступлений, в соответствии с требованиями ст.165, ч.3 ст.183 УПК РФ, необходимо судебное решение.

Однако, как следует из материалов дела, осмотр содержащейся в телефоне информации органами предварительного следствия был проведен без судебного решения.

Согласно ст.75 УПК РФ, доказательства, полученные с нарушением требований УПК РФ, являются недопустимыми, поэтому не имеют юридической силы и не могут быть положены в основу обвинения. Отсюда протокол осмотра предмета подлежит исключению из числа допустимых к оценке доказательств.

Коллегия сделала акцент на том, что права и свободы человека и гражданина *могут быть ограничены федеральным законом только в той мере, в какой это необходимо в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства* (ч. 3 ст. 55 Конституции РФ) [5].

Необходимо отметить, что следователь в связи со спецификой возложенных на него функций по раскрытию и расследованию преступлений, принятий процессуальных решений, как никто другой чаще затрагивает конституционные права и свободы граждан, в том числе право на тайну переписки. При этом, безусловно, это делается в целях защиты прав и законных интересов других лиц (ч. 1 ст. 6 УПК РФ, ч. 4 ст. 1 Закона «О Следственном комитете Российской Федерации), основ конституционного строя, нравственности, здоровья, обеспечения обороны страны и безопасности государства.

Суды, признавая недопустимым доказательством, протоколы осмотра содержащейся в телефоне информации часто ссылались на Определение Конституционного Суда РФ от 02.10.2003 № 345-О № 4 и на ст. 186.1 УПК РФ – «Получение информации о соединениях между абонентами и (или) абонентскими устройствами», что не является правильным. Нужно четко разграничивать ситуации и возникающие правоотношения, когда телефон изъят в ходе проведения следственного действия и находится у следователя от случаев, когда следователь для получения информации обращается к оператору сотовой связи.

Безусловно, законодательство о связи предусматривает тайну связи и защиту информации. Сведения об абонентах и оказываемых им услугах связи, ставшие известными операторам связи в силу исполнения договора об оказании услуг связи, являются информацией ограниченного доступа и подлежат защите в соответствии с законодательством Российской Федерации [6]. *Доступ* к ним возможен не иначе как на основании судебного решения. Причем заметим, что речь и в нормативных актах, и в решении Конституционного суда идет именно о *доступе* к этим сведениям, а не об *ознакомлении* с ними следователя. Ведь следователь, к примеру, получив по судебному решению информацию от оператора о соединениях между абонентами, осматривает представленные документы в соответствии с ч. 5 ст. 186.1 УПК РФ уже без судебного решения, о чем составляет отдельно протокол осмотра документов.

Если же телефон уже изъят и находится у следователя, то его осмотр, который, как представляется, включает в себя и осмотр содержащейся в нем информации (в том числе удаленной) производится без судебного решения.

Здесь многие практики проводят аналогию с изъятыми компьютерами, а также электронными и обычными записными книжками, письмами и пр.

Так, 30 сентября 2014 года Верховным Судом Российской Федерации рассмотрены кассационные жалобы осужденного и его адвоката на приговор Верховного Суда Республики Хакасия в которых, среди прочего, указывалось, что осмотр изъятого у осужденного мобильного телефона, содержащего данные о его телефонных переговорах, проведен с нарушением закона ввиду отсутствия судебного решения.

Оценивая доводы жалоб, Верховный Суд РФ указал, что осмотр мобильного телефона проведен следователем в соответствие со ст. 176 УПК РФ и, вопреки утверждениям осужденного, для этого не требовалось судебного решения [7].

Другой пример. Приморский краевой суд в феврале 2015 года рассматривал апелляционное представление прокурора, не согласившегося с решением районного суда *об отказе в удовлетворении ходатайства следователя о разрешении производства осмотра мобильных телефонов*, изъятых в ходе производства обыска в жилище.

В апелляционном представлении прокурор указал, что из положений ч. 2 ст. 23 Конституции РФ следует, что каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение такого права допускается только на основании судебного решения. Ввиду отсутствия судебного решения на осмотр телефона и получения информации, содержащей тайну переписки, следователь обоснованно обратился в суд с ходатайством о разрешении производства осмотра мобильного телефона, изъятого в ходе обыска в жилище.

Прокурор отметил, что суд, отказывая в удовлетворении ходатайства следователя, *мотивирует свое решение тем, что уголовно-процессуальным законом не предусмотрено получение разрешения на указанное следственное действие и фактически разъясняет возможность осмотра информации, содержащейся в мобильном телефоне*, что повлечет нарушение права лица на тайну переписки, предусмотренное ч. 2 ст. 23 Конституции РФ.

Однако *суд апелляционной инстанции согласился с доводами суда первой инстанции об отсутствии оснований для судебного санкционирования осмотра телефонов.*

Судом установлено, что обыск в жилище подозреваемого с целью отыскания мобильных телефонов и иных средств связи произведен в соответствии с требованиями норм УПК РФ, т.е. на основании судебного решения.

Обосновывая принятое решение, суд указал, что в соответствии со ст. 29 УПК РФ, судебное решение необходимо для производства контроля и записи телефонных и иных переговоров, получения информации о соединениях между абонентами и (или) абонентскими устройствами.

Суд апелляционной инстанции согласился с выводами районного суда о том, что по смыслу закона ***получение судебного решения необходимо*** при производстве оперативно-розыскных либо следственных мероприятий ***для истребования информации, находящейся у оператора связи в целях обеспечения законности ее появления у соответствующего органа,*** осуществляющего уголовное преследование. При этом, суд отметил, что *уголовно-процессуальным законодательством не предусмотрено получение органом, производящим ОРМ либо предварительное следствие судебного решения для производства осмотра, например, протоколов телефонных соединений между абонентами, предоставленных на основании судебного решения.*

По мнению суда апелляционной инстанции, суд обоснованно отказал следователю в разрешении производства осмотра мобильных телефонов, изъятых при обыске в жилище, так как это не предусмотрено уголовно-процессуальным законодательством. При таких обстоятельствах оснований для удовлетворения заявленного следователем ходатайства по мнению суда апелляционной инстанции не имелось, а доводы апелляционного представления о возможном нарушении права лица на тайну переписки, преду-

смотренного ч. 2 ст. 23 Конституции РФ, не основаны на нормах уголовно-процессуального закона, а потому удовлетворению не подлежат [8].

Таким образом, несмотря на неоднозначность поднятого вопроса, следует сделать вывод о том, что в ситуациях, когда сотовый телефон участника уголовного судопроизводства изъят и находится у следователя, получать судебное решение на его осмотр и ознакомление с цифровым содержимым не требуется.

Показательным в данном ключе является Определение Конституционного Суда РФ от 25.01.2018 № 189-О «Об отказе в принятии к рассмотрению жалобы гражданина Прозоровского Дмитрия Александровича на нарушение его конституционных прав статьями 176, 177 и 195 Уголовно-процессуального кодекса Российской Федерации». В данном постановлении Конституционный Суд подчеркнул, что проведение осмотра и экспертизы с целью получения имеющей значение для уголовного дела информации, находящейся в электронной памяти абонентских устройств, изъятых при производстве следственных действий в установленном законом порядке, не предполагает вынесения об этом специального судебного решения [9].

И, наконец**, в-четвертых,** вопросы внедрения цифровых технологий в экспертную деятельность.

Особое место среди судебных экспертиз сегодня заняли информационные технологии. Следствием этого явились, с одной стороны, определенная трансформация экспертного исследования как процесса познания, с другой – значительное расширение его возможностей, а также повышение научной обоснованности получаемых данных. В настоящее время сложилось несколько направлений компьютеризации судебно-экспертной деятельности.

Так, Информационно-поисковая система (ИПС) «Оружие» предназначена для хранения и поиска информации по нарезному оружию; Информационно-поисковая система (ИПС) «Патрон» предназначена для хранения и поиска информации по патронам для нарезного оружия. Генератор экспертных заключений (ГЭЗ) «Клинок» предназначен для создания экспертного заключения по холодному оружию; «Арсенал» – современная мощная компьютерная система, позволяющая автоматизировать всю технологическую цепочку исследований пуль, гильз и их фрагментов: от ввода информации и создания электронной базы данных, проверок и сравнительных исследований до получения экспертного заключения.

Кроме того, цифровые технологии применяются при производстве практически всех существующих судебных экспертиз: лингвистических, видеотехнических, фоноскопических, компьютерно-технических и др.

Современные цифровые технологии в области фиксации аудиовизуальной информации достигли такого уровня развития, что создаются предпосылки для применения этих технологий в криминалистических целях. Цифровые методы фиксации информации во многом превзошли в настоящее время аналоговые средства по качеству записи, воспроизведения и сохранения зафиксированной информации.

Центральным является вопрос о принципиальной допустимости использования ЭВМ при производстве собственно судебно-экспертных исследований и об условиях, при которых это становится возможным.

Ныне не ставится вопрос (в тех случаях, когда эксперт использует компьютер как орудие труда) познал ли он механизм «исследовательской» деятельности машины. Важно другое – надежно ли в техническом смысле работает данная машина и дает ли она верные результаты применительно к технологии осуществляемого процесса, например, применительно к анализу количественных характеристик выделенных признаков.

Несостоятельны и утверждения, будто эксперт не может объяснить ни характер работы ЭВМ, ни принципы формирования «выводов» машины. Дело в том, что любой компьютер работает по четким и однозначным алгоритмам, в принципиальной структуре которых может разобраться любой специалист-предметник. Если не говорить о редчайших сбоях, ЭВМ делает только то, что ей предписано человеком.

Подводя итог, можно отметить то, что экспертные системы не только не предполагают вытеснения человека из каких-либо интеллектуальных сфер деятельности, а наоборот, ориентируются на то, что профессиональные знания специалиста играют весомую роль в экспертных системах. Эта роль состоит в том, чтобы сделать знания одного или нескольких экспертов достоянием любого специалиста в данной области независимо от пространственно-временных ограничений. Немаловажным является и то, что, чем выше степень автоматизации экспертного исследования, тем меньше степень творческого участия эксперта, но с другой стороны при помощи автоматизации эксперт тратит меньше времени на работу и более точен в своих оценках.

Библиографический список

1. Постановление Пленума Верховного Суда РФ от 1 июня 2017 г. № 19 «О практике рассмотрения судами ходатайств о производстве следственных действий, связанных с ограничением конституционных прав граждан (статья 165 УПК РФ)» //Российская газета, 2017, июнь.

2. *Бутенко О.С.* Криминалистические и процессуальные аспекты проведения осмотра мобильных телефонов в рамках предварительного следствия // «Lex Russica». – 2016. – № 4 (113) апрель. – С. 49–60.

3. *Бертовский Л.В.* Расследование преступлений экономической направленности: научно-практическое пособие. – М.: Проспект, 2016. – 305 с.; *Островский С.* Типичные нарушения, выявляемые в ходе надзора за расследованием уголовных дел о хищениях, совершённых с использованием средств мобильной связи // Законность. – 2017. – № 2 (988). – С. 23–26.

4. Кассационное определение судебной коллегии по уголовным делам Омского областного суда от 24 мая 2012 г. по делу № 22К-2225/2012 (Извлечение) // www.consultant.ru

5. Апелляционное определение Судебной коллегии по уголовным делам суда Ямало-Ненецкого автономного округа от 20 января 2014 года по делу № 22-49/2014 (Извлечение) // www.consultant.ru

6. Федеральный закон № 126-ФЗ от 7 июля 2003 года «О связи» (ст.53, ч.3 ст.63) // www.consultant.ru; Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации (ст.16) // www.consultant.ru

7. Кассационное определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 30.09.2014 по делу № 55-014-6 // www.consultant.ru

8. Апелляционное постановление Приморского краевого суда от 02.02.2015 по делу № 22-455/15 // www.consultant.ru

9. Определение Конституционного Суда РФ от 25.01.2018 № 189-О «Об отказе в принятии к рассмотрению жалобы гражданина Прозоровского Дмитрия Александровича на нарушение его конституционных прав статьями 176, 177 и 195 Уголовно-процессуального кодекса Российской Федерации» // www.consultant.ru

Для цитирования: *Бастрыкин А.И.* Лекция: «Цифровые технологии современной криминалистики» // Юридическая мысль. – 2020. – № 3 (119). – С. 161–174. DOI: 10.47905/MATGIP.2020.119.3.012

Lecture: "Digital technologies of modern forensics science"

Alexander I. Bastrykin*

Annotation. This lecture contains theoretical and practical material, reflecting the debatable issues of the introduction of digital technologies of the modern science of criminology in the Russian Federation. It is specially shown that the development of digital technologies imposes increased requirements for ensuring the activities of investigators when using digital technologies: when proving legal facts; optimization of procedural and managerial processes, both at the stage of initiating a criminal case and during the investigation of a crime; solving problems arising from the introduction of new information technologies into law enforcement practice.

The author proposes to carefully analyze the current regulatory legal framework in order to correct it in the direction of increasing the efficiency of using digital technologies in modern criminology.

Key words: criminal legislation, criminal procedural law, Investigative Committee, digital technologies, criminalistics.

The digitalization of public relations, of course, dictates new, previously unknown approaches in forensic theory and practice. The analysis of investigative practice reflects the fact that the legislator in this direction lags somewhat behind the development of high technologies, and, as a consequence, in the investigator's practice, questions often arise that require both scientific substantiation and practical testing and use.

These problems can be systematized and identified the main problems of digitalization.

Firstly, it concerns the use of digital technologies in proving legal facts.

We are talking about modern possibilities of collecting evidence-based information both by operational-search and investigative ways, namely:

✓ **Obtaining satellite photos of images of open areas of the terrain due to remote sensing of the Earth's surface**. To date, an agreement has

* ***Bastrykin Alexander Ivanovich,*** Chairman of the Investigative Committee of the Russian Federation, Doctor of Law, Professor, Honored Lawyer of the Russian Federation. E-mail: lawinst-spb@mail.ru

been concluded between the Investigative Committee of the Russian Federation and the Scientific Center for Operational Monitoring of the Earth (NTs OMZ) of the Russian Space Systems (Roscosmos), according to which all relevant information is synchronized and supplied to the Main Department of Criminalistics (Forensic Center) of the Investigative Committee of Russia. Thus, any investigator has the ability to promptly through e-mail receive information about the availability of the necessary personnel at the time of interest in a specific place.

So, in the Republic of Adygea, the investigator proved the person's guilt in committing crimes under Art. 171 of the Criminal Code of the Russian Federation "Illegal Business" and Art. 198 of the Criminal Code of the Russian Federation "Evasion of an individual from paying taxes, fees and (or) an individual – a payer of insurance premiums from paying insurance premiums", which refused to acknowledge the fact of using the fenced area as an unauthorized parking lot. Photos from space not only confirmed such illegal actions for a long time. But they also allowed to count the number of cars (light trucks) that were parked in the parking lot.

Earth remote sensing data were successfully used in the investigation of the facts of sabotage and other illegal activities on the territory of Ukraine and Russia, Savchenko Nadezhda.

✓ **Use of digital devices in vehicles**. Computer systems of motor vehicles provide the investigators with quite useful information about the speed of the vehicle, the weight of passengers and driver, routes of movement, etc.

For example, the event data recorder AUTO (EDR ACU) in an accident or under conditions close to an accident can store (depending on the manufacturer of the device) up to 60 analog and 30 specific (on / off) parameters of a moving vehicle, many of which are forensically significant. Among such parameters, during a certain time interval before the collision (overturning), the following can be recorded:

– the state of the latch of the driver's and passenger's seat belt buckle in the front seat;
– position of the gear shift lever;
– the degree of pressing the accelerator pedal, brake;
– engine speed;
– readings of the speedometer;
– turns of the steering wheel;
– the state of the ABS, ESR, SRS systems;
– time of activation of emergency braking systems
– signals from light and rain sensors.

Moreover, the information in the electronic memory EDR is continuously updated. At the same time, the memory capacity of some EDR models allows storing per-second data recorded for a period of time covering 5 seconds before the collision (overturning), and ending with 1 second after it.

✓ **Receiving data from street, transport, internal video cameras. Video recording of the investigative actions themselves.** It is difficult to overestimate the value of video recording of investigative actions. This additional fixation allows:

firstly, the investigator should concentrate on the essence and purpose of the investigative action, its tactics, establishing psychological direct contact with the participants, and not documenting it in the form of a mechanical drawing up of a protocol;

secondly, visually, an unlimited number of times to reproduce the course and content of the investigative action, and not only its result, to focus the attention of the investigator on previously unnoticed details;

thirdly, he is critical of the change in the testimony by the person, since it confirms the absence of any influence in relation to him, leading questions, and also fixes the moral and physical state of the latter;

fourthly, to record the non-verbal reactions of the participant in the investigative action (facial expressions, rhythm and confidence of speech, reactions to the questions posed, the position of the limbs, etc.) when answering questions posed by the investigator or other participants that are important for a criminal case, demonstrating irrefutable evidence and so on;

fifth, to appoint a forensic phonoscopic and (or) psychological examination based on video recordings of investigative actions, including for the exclusion of alleged pressure on a person, possible leading questions, giving false testimony (psychological and vocalographic examination, psychological and linguistic or psychological acmeological);

sixth, to carry out the investigative action more effectively and offensively, to prevent violations of the law and ethical norms on the part of all its participants;

seventh, to demonstrate in the court session a video recording of the investigative action, including in the event that the participants did not appear at the session.

✓ **Criminally significant information contained in the memory of digital devices**. The widespread use of electronic devices by both endured and criminals (cellular telephones, smartphones, tablet computers, fitness bracelets, chip tickets for transport, navigators, portable GPS devices, etc.) in the preparation, commission of crimes, concealment traces, demanded from forensic experts to revise modern possibilities for collecting evidence. The issue related to the seizure, fixation and research of information contained in such media has become relevant.

The value of such information is obvious for the detection, disclosure and investigation of crimes, identification of unidentified corpses, etc. After all, with the help of this information, the investigator can obtain criminally important evidentiary or orienting information: to determine the location of the subject of the crime, his accomplices, witnesses, victims at a certain time, get acquainted with the log of calls, the content of SMS correspondence, chats, study the log of browsers – Internet pages visited by a person, etc.

The investigator can obtain this information either through a communications operator or directly from an electronic device seized from the person.

The first step towards the unification of the current procedural legislation of Russia and its adaptation, the modern capabilities of mobile operators in providing assistance in the disclosure and investigation of crimes, was the inclusion of Art. 186.1 – “Obtaining information about connections between subscribers and (or) subscriber devices” in the system of investigative actions.

Today, investigators expand the possibilities of such an investigative action indicate in the resolution not only the standard requested information about the subscriber, the interlocutor, the type of connection, its date, time and duration, but also the azimuth (the angle between the direction to the north (zero compass) and the direction to the place location of the subscriber), time energy (the time the signal travels from the subscriber's device to the base station). After receiving this information, forensic investigators go directly to the base station and, using a compass and a map of the area, designate the area where the verified subscriber was. Also, with the help of electronic reconnaissance sensors, all base stations are installed to which the user's phone could be switched.

So, for example, in the Republic of Dagestan, a forensic investigator, working on the fact of the unknown disappearance of an entrepreneur, using the azimuth of the last connection and the intersection of the coverage vectors of previous connections, managed to establish the place of his murder. A thorough examination of the scene made it possible to find a body drowned in the sea and to track the killers (the victim's daughter and her boyfriend).

Often, the location of the person of interest to the investigating authorities can be established subject to the seizure of gadgets that are constantly with this person and have a built-in receiving and transmitting GPS or GLONAS module (smartphone, tablet, electronic watch, books, heart rate monitor, pedometer, fitness bracelet, car registrar). These devices, provided that the navigation function is activated, store data on their location (and, most likely, the user's location) in memory. Also, user devices with wireless LAN WI-FI technology save information about the place and time of connection with the router;

In this vein, the “assistants” of the investigation are also media files (photos, videos) stored in various digital devices and social networks. Most modern photo cameras save the latitude and longitude of the location where the photo or video was taken. You can check the alibi of a person with the help of tickets for transport seized from him, card-passes equipped with microcircuits that are triggered by touching the validator in surface public transport, metro, at checkpoints to various institutions.

So, in Moscow, according to the metadata of a photograph of a carpet taken by a kidnapped child in the abuser's apartment, the address of the house was established and by way of a round-trip round the criminal's apartment. During the inspection of the apartment, it was possible to seize a sufficient amount of evidence confirming the guilt of the person and confirming the multi-episode nature of his actions.

Moreover, the sensors of the electronic situation received by the forensic departments, as well as the freely available Netmonitor, G-nettrack programs allow investigators to track and fix base stations (2G, 3G,) of all telecom operators and make a point request to the operator indicating the identification data of the stations (LAC, CID – for the type of network 2G, 3G or TAC and CL – for LTE).

For example, in the city of Oryol, a forensic investigator established the location of the wanted murderer of a minor girl. After receiving information from the telecom operator and finding out that the offender is connecting through the same base stations, a visit to the location of these repeaters was organized, with the

help of specialized programs, the boundaries of the person's stay in dense buildings were outlined. Through a door-to-door tour with a photograph of the killer, the latter was discovered and detained.

This information, subject to the operator's correct initial data and careful analysis (including using hardware and software systems in service with law enforcement agencies), allows you to establish information about the subscriber's area of residence at a certain time, the duration of stay in this place; confirm the fact of his presence at the sites of other (similar) incidents; to check the possibility of simultaneous stay of the suspect and the victim (the suspect with the victim's phone on) in one place at the same time.

If the gadget has already been seized by the investigator, then he has the opportunity to examine it using high-tech forensic technology. For example, the hardware and software complex “Oxygen Forensic Suite” or “UFED” can also view deleted data (call log, SMS, MMS, chat data, photo and video files, visited Internet resources), which help correctly build versions of unobvious crimes, prove the guilt (innocence) of the person being checked, confirm the preparatory actions, or actions to hide the traces of the crime, establish an additional witness or a new illegal episode.

So, during the investigation of the fact of committing violent acts of a sexual nature against a minor Golovanova O.V. (Amur Region) suspects Kuznetsov T.Sh. and Ivanishchev M.O. they completely denied their guilt.

Inspection of the cell phones seized from them with the help of the UFED complex made it possible to restore and copy previously deleted video recording files, one of which recorded the process of committing criminal acts.

At the same time, a video frame was recorded by a clearly visible license plate of the criminals' car, the brand of which and, moreover, the license plate the victim could not name. In the course of the investigative and operational-search measures, A.M. Rebrov was identified – the main perpetrator of the crime committed against Golovanova. The seized video became the decisive proof of his guilt.

In addition, the use of UFED when examining cell phones seized on the basis of fatal railway injuries made it possible in a number of cases to restore deleted SMS messages indicating suicidal intentions of citizens.

The Main Department of Criminalistics of the Investigative Committee of the Russian Federation has a hardware and software complex “Segment-S”, which allows carring out analytical work of cellular networks, to identify possible periodic intersection of subscribers, their joint location, traffic routes, points of last registration, etc.

Search and analytical work in social networks and the study of the user's Internet activity are becoming widespread in forensics.

The LIS-M complex allows you to find a specific user, visually displays the social graph of users and groups, and also solves such problems as finding common acquaintances of a suspect, identifying clusters, calculating centrality metrics.

Secondly, the use of digital technologies to optimize procedural and managerial processes, both at the stage of initiating a criminal case and during the investigation of a crime.

It is obvious that modern criminal justice has a steady trend towards digitalization and this is inevitable. We are talking about those domestic and foreign regulatory innovations concerning the widespread use of various electronic devices for objectification and simplification to investigative checks, criminal investigations and court proceedings.

It should be admitted that the domestic criminal process lags behind in this direction. Communication with investigators, study of their daily work indicates the need to revise some conservative approaches. We are talking about the possibility of remote (using videoconferencing) interrogations of some participants, the inappropriateness of duplicating a video recording of an investigative action and drawing up a protocol, operational electronic requests in accordance with Article 21 of the Criminal Procedure Code of the Russian Federation, and much more.

The work of an investigator, like any other, must keep pace with the times. High technologies and technologies of artificial intelligence are developing in our country, but, unfortunately, not in the field of jurisprudence. Most of the software used for lawyers is help systems (Consultant +, GARANT, etc.). This is definitely not enough. Until now, there is no high-quality and regularly updated automated workplace (AWS) for the investigator; virtual reality technologies are poorly used. Therefore, the only way to develop legal application software is to develop it by an organization independently. The Investigative Committee of the Russian Federation also took this path.

The information system “Electronic passport of a criminal case” was put into effect by Order of the Investigative Committee of Russia No. 27 / 108r dated 09.04.2014. According to the information of the State Investigative Committee of the North Caucasus Federal District, for the first half of 2016, this information system contains more than 45,000 cards of criminal cases, 600 user accounts, uploaded over 300,000 files related to criminal investigations. The information system allows real-time monitoring of the progress of the investigation of a criminal case, monitoring the execution of instructions in a criminal case, ensuring effective procedural control and planning the investigation of a criminal case.

The role of the information system “Electronic passport of a criminal case” cannot be underestimated. It allows you to reduce paperwork and simplify procedural control over investigated criminal cases.

At the same time, like any software, it is not without flaws. Most of them stem from the fact that the system “Electronic passport of a criminal case” is operating so far only on the territory of the South and North Caucasian Federal Districts. This system was developed by the employees of the Investigative Committee and is maintained by them in an up-to-date and efficient state. Scaling this information system to all departments of the Investigative Committee requires its completion. A number of proposals can be made to improve the information system “Electronic passport of a criminal case”:

1. Introduce methodological recommendations and information materials into the information system on the results of the investigation of various categories of criminal cases and the conduct of certain investigative actions.

2. Create an “Archive of Criminal Cases” so that when viewing the general list of criminal cases investigated by a specific investigative department, exactly those cases that are currently being processed are opened.

3. In order to ensure the completeness of procedural control over the investigation of criminal cases at all stages of criminal proceedings, add to the information system "Electronic passport of a criminal case" a book for registering messages about a crime of each territorial investigation department in electronic form.

It should also be noted that it is advisable to expand the database and connect all the investigative departments of the Investigative Committee of the Russian Federation to it.

At the Moscow Academy of the Investigative Committee of the Russian Federation, all the necessary conditions have been created for the development of all educational programs being implemented through the purposeful organization of the educational process, the choice of forms, methods and teaching aids. Particular attention is paid to active forms of conducting training sessions, which ensure the rapid assimilation of educational material and form the necessary practical skills, including using the capabilities of a computer class.

Therefore, training managers in the skills of working in the “Electronic passport of a criminal case” system within the framework of advanced training programs will contribute to a deeper study of all its capabilities.

Thirdly, these are the problems that arise during the introduction of new information technologies in law enforcement practice.

First of all, let us dwell on the legal side of the issue, the admissibility of the actions of the investigator described above.

The current domestic legislation leaves open the question of whether law enforcement officers should receive a court decision to inspect the phones and the information contained in them of the participants in criminal proceedings. This problem is not specified in the Resolution of the Plenum of the Supreme Court of the Russian Federation of June 1, 2017 No. 19 “On the practice of consideration by the courts of petitions for the production of investigative actions related to the restriction of the constitutional rights of citizens (Article 165 of the Criminal Procedure Code of the Russian Federation)” [1].

In this regard, among the scientific community and practical workers, there are different opinions on this issue, as well as on the question of which information contained in the phone's memory the law enforcement agencies have the right to get acquainted with without a court decision, and which not. Judicial practice is also ambiguous in this direction [2, p. 58].

Some authors and representatives of the prosecutor's office, for example, suggest that during the examination of the mobile phone of the participants in the criminal process not to be limited only to an external examination, but to pay attention to and reflect in the protocol the technical characteristics, the contents of the memory of the mobile phone, information about subscriber connections, SMS messages, use special technical means for inspection, allowing you to recover deleted data. The relevant indications are reflected in the acts of the prosecutor's response [3, p. 23].

The prohibition on interference in a person's personal and family life, on familiarization with his correspondence is established in Article 12 of the Universal Declaration of Human Rights, as well as in Art. 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms. More-

over, the last Convention separately emphasizes *the prevention of interference by state bodies in the exercise of these rights.* At the same time, in both Conventions, *a reservation is made that in exceptional cases established by law such interference is still possible.*

In Art. 23 of the Constitution of the Russian Federation also proclaims that everyone has the right *to privacy of correspondence, telephone conversations, postal, telegraph and other messages. Limitation of this right is allowed only on the basis of a court decision.*

So, canceling the ruling of the court of first instance, the panel of judges noted the following. When making a decision, the court of the first in-station did not take into account the provisions of Article 23 of the Constitution of the Russian Federation, as well as the requirements of Articles 13, 38 of the Criminal Procedure Code of the Russian Federation. Inspection of the phone does not include inspection of its contents, since information about telephone connections, contacts and SMS messages are protected by the Constitution of the Russian Federation.

Despite the fact that Chapter 25 of the Criminal Procedure Code of the Russian Federation does not directly enshrine the duty of the investigator to obtain judicial permission to inspect SMS correspondence, this duty follows from other norms of both the criminal procedure law and the provisions of the Constitution of the Russian Federation, and from international norms enshrined in the Convention on the protection of human rights and fundamental freedoms, subject to unconditional application in the Russian Federation. Inspection of the personal correspondence contained in the suspect's mobile phone, taking into account the nature and degree of interference, is virtually identical to the inspection of postal and telegraph items or telegrams, for which Article 185 of the Criminal Procedure Code of the Russian Federation provides for the need for a court decision.

When examining a mobile phone, the investigator thoroughly described all connections between subscribers, namely between the victim and those persons to whom he sent SMS messages and from whom he received such messages, up to indicating the time of connections, phone numbers and names of persons who they use these phones. At the same time, article 186.1 of the Criminal Procedure Code of the Russian Federation provides for the need for judicial permission to obtain information about connections between subscribers and (or) subscriber devices [4].

The Judicial Collegium for Criminal Cases of the Yamalo-Nenets Autonomous District Court noted that the information that constitutes the secrecy of telephone conversations protected by the Constitution of the Russian Federation and laws in force on the territory of the Russian Federation is any information transmitted, stored and installed using telephone equipment, including information about incoming and outgoing signals for connecting the telephone sets of specific communication users, therefore, in order to obtain this kind of information by the authorities investigating crimes, in accordance with the requirements of Article 165, Part 3 of Article 183 of the Code of Criminal Procedure of the Russian Federation, a court decision is required.

However, as follows from the materials of the case, the examination of the information contained in the telephone by the bodies of the preliminary investigation was carried out without a court decision.

According to Article 75 of the Criminal Procedure Code of the Russian Federation, evidence obtained in violation of the requirements of the Code of Criminal Procedure of the Russian Federation is inadmissible; therefore, it has no legal force and cannot be used as the basis for an accusation. Hence, the protocol of the inspection of the object is subject to exclusion from the number of evidence admissible for assessment.

The Collegium emphasized that human and civil rights and freedoms can be limited by federal law only to the extent necessary in order to protect the foundations of the constitutional order, morality, health, rights and legitimate interests of others, to ensure the country's defense and security state (part 3 of article 55 of the Constitution of the Russian Federation) [5].

It should be noted that the investigator, due to the specifics of the functions assigned to him for the disclosure and investigation of crimes, the adoption of procedural decisions, more often than anyone else affects the constitutional rights and freedoms of citizens, including the right to privacy of correspondence. At the same time, of course, this is done in order to protect the rights and legitimate interests of other persons (part 1 of article 6 of the Criminal Procedure Code of the Russian Federation, part 4 of article 1 of the Law "On the Investigative Committee of the Russian Federation", the foundations of the constitutional order, morality, health, ensuring the country's defense and state security.

The courts, recognizing as inadmissible evidence, the protocols of the examination of the information contained in the telephone, often referred to the Definition of the Constitutional Court of the Russian Federation dated 02.10.2003 No. 345-O No. 4 and to Art. 186.1 of the Code of Criminal Procedure of the Russian Federation – "Obtaining information about connections between subscribers and (or) subscriber devices", which is not correct. It is necessary to clearly distinguish between situations and emerging legal relationships when the phone is seized during the course of an investigative action and is kept by the investigator from cases when the investigator turns to a cellular operator to obtain information.

Of course, the legislation on communications provides for the secrecy of communications and the protection of information. Information about subscribers and the communication services provided to them, which became known to communication operators by virtue of the execution of the contract for the provision of communication services, is information of limited access and is subject to protection in accordance with the legislation of the Russian Federation [6]. Access to them is possible only on the basis of a court decision. Moreover, it should be noted that both in the normative acts and in the decision of the Constitutional Court it is precisely about access to this information, and not about familiarizing the investigator with it. After all, the investigator, for example, having received information from the operator about connections between subscribers by a court decision, examines the submitted documents in accordance with Part 5 of Art. 186.1 of the Code of Criminal Procedure of the Russian Federation already without a court decision, about which a separate protocol of examination of documents is drawn up.

If the phone has already been confiscated and is in the possession of the investigator, then its examination, which seems to include the examination of

the information contained in it (including deleted information), is carried out without a court decision.

Here many practitioners draw an analogy with confiscated computers, as well as electronic and ordinary notebooks, letters, etc.

So, on September 30, 2014, the Supreme Court of the Russian Federation considered the cassation appeals of the convict and his lawyer against the verdict of the Supreme Court of the Republic of Khakassia, which, among other things, indicated that the examination of the mobile phone seized from the convict, containing data on his telephone conversations, was carried out with violation of the law due to the absence of a court decision.

Evaluating the arguments of the complaints, the Supreme Court of the Russian Federation indicated that the examination of the mobile phone was carried out by the investigator in accordance with Art. 176 of the Code of Criminal Procedure of the Russian Federation and, contrary to the assertions of the convicted person, this did not require a court decision [7].

Another example. In February 2015, the Primorsky Regional Court considered an appeal by a prosecutor who did not agree with the decision of the district court *to refuse to satisfy the investigator's request for permission to inspect mobile phones seized during a search of a home.*

In the appeal, the prosecutor indicated that from the provisions of Part 2 of Art. 23 of the Constitution of the Russian Federation it follows that everyone has the right to privacy of correspondence, telephone conversations, postal, telegraph and other messages. Limitation of such a right is allowed only on the basis of a court decision. In the absence of a court decision to inspect the telephone and to obtain information containing confidentiality of correspondence, the investigator reasonably applied to the court for permission to inspect the mobile phone seized during the search in the home.

The prosecutor noted that the court, refusing to satisfy the request of the investigator, *motivates its decision by the fact that the criminal procedure law does not provide for obtaining permission for the specified investigative action and actually explains the possibility of examining the information contained in the mobile phone, which will entail a violation of the person's right to secrecy of correspondence, provided for in Part 2 of Art. 23 of the Constitution of the Russian Federation.*

However*, the appellate court agreed with the arguments of the first instance court about the absence of grounds for judicial authorization of the telephone inspection.*

The court established that the search in the suspect's home in order to find mobile phones and other means of communication was carried out in accordance with the requirements of the Code of Criminal Procedure of the Russian Federation, i.e. based on a court decision.

Justifying the decision, the court indicated that in accordance with Art. 29 of the Code of Criminal Procedure of the Russian Federation, a court decision is necessary to control and record telephone and other conversations, to obtain information about connections between subscribers and (or) subscriber devices.

The appellate court agreed with the findings of the district court that, within the meaning of the law, **obtaining a court decision is necessary** in the course of operational-search or investigative measures **to retrieve informa-**

tion held by a telecom operator in order to ensure the legality of its appearance from the relevant body carrying out criminal prosecution. At the same time, the court noted *that the criminal procedural legislation does not provide for the receipt by the body producing ORM or preliminary investigation of a court decision to conduct an inspection, for example, protocols of telephone connections between subscribers, provided on the basis of a court decision.*

According to the court of appeal, the court reasonably refused to allow the investigator to inspect the mobile phones seized during the search of the home, since this is not provided for by the criminal procedure legislation. In such circumstances, in the opinion of the court of appeal, there were no grounds for satisfying the petition filed by the investigator, in the opinion of the court of appeal, and the arguments of the appeal submission about a possible violation of the person's right to privacy of correspondence, provided for in Part 2 of Art. 23 of the Constitution of the Russian Federation, are not based on the norms of the criminal procedure law, and therefore are not subject to satisfaction [8].

So, despite the ambiguity of the issue raised, it should be concluded that in situations where the cell phone of a participant in criminal proceedings is seized and is from the investigator, it is not required to receive a court decision for its examination and familiarization with the digital content.

Indicative in this vein is the Definition of the Constitutional Court of the Russian Federation dated 25.01.2018 No. 189-O "On the refusal to accept for consideration the complaint of citizen Dmitry Alexandrovich Prozorovsky on violation of his constitutional rights by Articles 176, 177 and 195 of the Criminal Procedure Code Russian Federation". In this decision, the Constitutional Court emphasized that the conduct of an examination and examination in order to obtain information relevant to a criminal case in the electronic memory of subscriber devices seized during investigative actions in the manner prescribed by law does not imply the issuance of a special court decision on this [9].

And finally, **fourthly**, the issues of introducing digital technologies into expert activities.

Information technologies occupy a special place among forensic examinations today. The consequence of this was, on the one hand, a certain transformation of expert research as a cognitive process, on the other, a significant expansion of its capabilities, as well as an increase in the scientific validity of the data obtained. At present, there are several directions of computerization of forensic activity.

Thus, the Information Retrieval System (ISS) "Arms" is designed to store and search for information on rifled weapons; The information retrieval system (ISS) "Patron" is designed to store and search information on cartridges for rifled weapons. The generator of expert opinions (GEZ) "Blade" is designed to create an expert opinion on melee weapons; "Arsenal" is a modern powerful computer system that allows automating the entire technological chain of research of bullets, shells and their fragments: from entering information and creating an electronic database, checks and comparative studies to obtaining an expert opinion.

In addition, digital technologies are used in the production of almost all existing forensic examinations: linguistic, video-technical, phonoscopic, computer-technical, etc.

Modern digital technologies in the field of recording audiovisual information have reached such a level of development that prerequisites are created for the use of these technologies for forensic purposes. Digital methods of recording information have largely surpassed analogue means in the quality of recording, reproducing and storing recorded information.

The central issue is the question of the fundamental admissibility of using a computer in the production of forensic research itself and about the conditions under which this becomes possible.

Nowadays, the question is not raised (in those cases when an expert uses a computer as a tool of labor) whether he has learned the mechanism of the "research" activity of a machine. Another thing is important – whether this machine works reliably in a technical sense and whether it gives correct results in relation to the technology of the process being carried out, for example, in relation to the analysis of the quantitative characteristics of the selected features.

The assertions that the expert cannot explain either the nature of the operation of the computer or the principles of forming the "conclusions" of the machine are also untenable. The fact is that any computer operates according to clear and unambiguous algorithms, the fundamental structure of which can be understood by any subject specialist. If you do not talk about the rarest failures, the computer does only what it is prescribed by a person.

Summing up, it can be noted that expert systems not only do not imply the displacement of a person from any intellectual spheres of activity, but, on the contrary, are guided by the fact that the professional knowledge of a specialist plays a significant role in expert systems. This role is to make the knowledge of one or more experts the property of any specialist in the field, regardless of space-time constraints. It is also important that the higher the degree of automation of the expert research, the less the degree of creative participation of the expert, but on the other hand, with the help of automation, the expert spends less time on work and is more accurate in his assessments.

Bibliographic list

1. Resolution of the Plenum of the Supreme Court of the Russian Federation of June 1, 2017 No. 19 "On the practice of consideration by the courts of petitions for the production of investigative actions related to the restriction of the constitutional rights of citizens (article 165 of the Criminal Procedure Code of the Russian Federation)" // Rossiyskaya Gazeta, 2017, June.

2. Butenko O.S. Criminalistic and procedural aspects of the examination of mobile phones in the framework of the preliminary investigation // Lex Russica. 2016. No. 4 (113) April. P. 49–60.

3. Bertovsky L.V. Investigation of economic crimes: a scientific and practical guide. Moscow: Prospect, 2016. 05 p.; Ostrovsky S. Typical violations revealed during the supervision of the investigation of criminal cases of thefts committed using mobile communications // Legality. 2017. No. 2 (988). P. 23–26.

4. The cassation ruling of the Judicial Collegium for Criminal Cases of the Omsk Regional Court dated May 24, 2012 in case No. 22K-2225/2012 (Extract) // www. consultant.ru

5. Appeal ruling of the Judicial Collegium for Criminal Cases of the Yamal-Nenets Autonomous Okrug Court dated January 20, 2014 in case No. 22–49 / 2014 (Extract) // www.consultant.ru

6. Federal Law No. 126-FZ of July 7, 2003 “On Communications” (Article 53, Part 3, Article 63) // www.consultant.ru; Federal Law of 27.07.2006 No. 149-FZ “On Information, Information Technologies and Information Protection” (Article 16) // www.consultant.ru

7. The cassation ruling of the Judicial Collegium for Criminal Cases of the Supreme Court of the Russian Federation dated 30.09.2014 in case No. 55-014-6 // www.consultant.ru

8. The appeal decision of the Primorsky Regional Court dated 02.02.2015 in case No. 22–455 / 15 // www.consultant.ru

9. Determination of the Constitutional Court of the Russian Federation dated 25.01.2018 No. 189-O "On the refusal to accept for consideration the complaint of the citizen Dmitry Alexandrovich Prozorovsky on violation of his constitutional rights by Articles 176, 177 and 195 of the Criminal Procedure Code of the Russian Federation" // www. consultant.ru

For citation: Bastrykin A.I. Lecture: “Digital technologies of modern forensics” // Legal thought. 2020. No. 3 (119). P. 174–186. DOI: 10.47905/MATGIP.2020.119.3.012