АКТУАЛЬНЫЕ ВОПРОСЫ ГОСУДАРСТВЕННОГО РЕГУЛИРОВАНИЯ ПРИМЕНЕНИЯ ТЕХНИЧЕСКИХ СРЕДСТВ В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ

Сильнов М.А.
Университет прокуратуры Российской Федерации, г. Москва
email: silnov@yandex.ru

Аннотация. В статье рассматриваются вопросы совершенствования нормативного регулирования применения технических средств в уголовно-процессуальном доказывании с позиций использования программных и технических средств защиты информации.

Ключевые слова: уголовный процесс; достоверность доказательств; следственные действия; защита информации; видео-конференц-связь.

Технический прогресс ворвался во все сферы человеческой деятельности и серьезно изменил их привычное содержание. Эра цифровизации вторглась и в весьма закрытую, консервативную область государственной компетенции - сферу борьбы с преступностью. Ведь многие приемы и методы, используемые сегодня при раскрытии преступлений, насчитывают более сотни лет [1, с. 1-12].

Но наступление технической революции неумолимо. Уже прочно вошли в повседневную жизнь основанные на использовании средств вычислительной техники криминалистические учеты: автоматизированная баллистическая идентификационная система (АБИС) «Арсенал» автоматизированная дактилоскопическая информационная система (АДИС) «Папилон» [2, с. 250 - 254]. Осваиваются, еще вчера казавшиеся научной фантастикой, методы идентификации по признакам внешности, использующие технологию распознавания лиц[1]. С 2018г. запущена единая электронная система биометрических персональных данных россиян, позволяющая государственным органам, банкам и иным организациям в предусмотренных законом случаях проводить удаленную идентификацию физических лиц, на основе использования их биометрических персональных данных[2].

Активно обсуждаются практиками и представителями научного сообщества возможности использования в уголовно-процессуальной деятельности электронных уголовных дел [3, с. 95-101], принципы и алгоритмы автоматизации процесса квалификации преступлений [4, с. 5-10], другие направления применения систем искусственного интеллекта [5, с. 3-12].

Вызовы времени стремительны и не оставляют законодателю и правоприменителю для ответа на них пауз «на раскачку». О некоторых проблемах, требующих скорейшего нормативного урегулирования, в сфере уголовно-процессуального доказывания и пойдет речь в настоящей статье.

Известно, что как в ходе следственных действий (ч. 5 ст. 166 УПК РФ), так и в процессе оперативно-розыскных мероприятий (Ст. 6 Федерального закона «Об оперативно-розыскной деятельности» от 12.08.1995 N 144-ФЗ) могут использоваться разнообразные технические средства фиксации их хода и результатов. Как правило, это различная видео-, фото-, и аудио-аппаратура.

---

[1] С помощью алгоритмов удаленной идентификации граждане уже сегодня могут получать дистанционно банковские услуги, подтвердив свою личность с помощью биометрических персональных данных (голоса и изображения лица). См.: Приказ Минкомсвязи России от 25 июня 2018 г. № 321.

[2] Федеральный закон от 31 декабря 2017 г. № 482-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации»

Последние годы мы наблюдаем тенденцию усиления роли Правительства в регулировании уголовно-процессуальных правоотношений, в том числе, в вопросах хранения, учета и передачи вещественных доказательств[1]. Однако нормативный регламент использования технических средств при обнаружении следов преступления, по сути тех же вещественных доказательств, и их фиксации при производстве следственных действий сегодня отсутствует. Следователи часто руководствуются морально устаревшими научно-практическими рекомендациями прошлых лет. В то же время применительно к закреплению некоторых результатов оперативно-розыскной деятельности, - он существует. Так, ст.6 Федерального закона «Об оперативно-розыскной деятельности» гласит, что Перечень видов специальных технических средств, предназначенных для негласного получения информации в процессе осуществления оперативно-розыскной деятельности, устанавливается Правительством Российской Федерации[2].

Указанная проблема представляется весьма актуальной. Ведь отсутствие регламента по использованию специальных, защищенных от постороннего вмешательства технических средств при обнаружении, фиксации и изъятии следов преступления, побуждает следователей и дознавателей практически повсеместно использовать в таком качестве обычную бытовую фото-, видео- и аудио- технику, приобретенную в общедоступной торговой сети. Такой порядок вещей представляется неприемлемым.

Еще в 90-е нами была обозначена проблема защиты криминалистической информации от фальсификации в том числе путем компьютерной корректировки протоколов следственных действий, фото- и видео- доказательств [6, с. 103-104]. И как свидетельствует судебная практика, тема подделки материалов уголовных дел остается весьма злободневной по сей день[3].

Технические способы решения задачи защиты криминалистической информации существуют. Сегодня они активно используются в предпринимательской деятельности. Однако применительно к обеспечению тайны следствия, достоверности фото-, видео- и звуко- записи, других материалов следствия они не задействованы, хотя совершенно очевидна необходимость создания, производства и внедрения подобных средств в практику органов предварительного расследования на основе госзаказа.

Тут важно понимать, что отдельные защищающие коммерческую тайну технологии, при должном проявлении государственной воли могут быть

---

[1] Постановление Правительства РФ от 08.05.2015 N 449 «Об условиях хранения, учета и передачи вещественных доказательств по уголовным делам»; Постановление Правительства РФ от 23.09.2019 N 1238 «О распоряжении имуществом, обращенным в собственность государства»; Постановление Правительства РФ от 08.05.2015 N 449 «Об условиях хранения, учета и передачи вещественных доказательств по уголовным делам» и др.

[2] См.: Постановление Правительства РФ от 01.07.1996 N 770 «Об утверждении Положения о лицензировании деятельности физических и юридических лиц, не уполномоченных на осуществление оперативно-розыскной деятельности, связанной с разработкой, производством, реализацией, приобретением в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации, и Перечня видов специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации в процессе осуществления оперативно-розыскной деятельности».

[3] Приговор Троицкого городского суда Челябинской области от 19 марта 2015 г. по делу № 1-359/2014 -в отношении Тухватулиной Н.А. по ч. 1 ст. 303 УК РФ; Приговор Кировского районного суда города Красноярска по делу № 1-386/2017 в отношении Гайнатулиной Е.А. по ч. 3 ст. 303 УК РФ; Приговор Кировского районного суда г. Томска суда по делу № 1-67/2017 в отношении Костоусовой Н.В по ч. 3 ст. 303 УК РФ и др.

реализованы и как средство защиты тайны следствия и как способ обеспечения достоверности доказательств.

Так, например, научно-инжиниринговый центр технических средств охраны (НИЦ ТСО), входящий в структуру «Ростеха», разработал решение по защите сетевых камер фотовидеофиксации, соответствующее требованиям федерального закона №187-ФЗ «О безопасности критической инфраструктуры РФ». Оно обеспечивает максимальную степень защиты информации, передаваемой с камер видеонаблюдения. Специальная линейка кибербезопасных камер исключает несанкционированный доступ к информационным системам видеонаблюдения, функционирующим согласно реестру объектов критической информационной инфраструктуры (КИИ). В камеру встраивается плата киберзащиты со специальным программным обеспечением, благодаря которому весь входящий и исходящий трафик передается зашифрованным. Как отмечают разработчики, широкое использование незащищенных систем видеонаблюдения в различных областях применения, в том числе в системах обеспечения безопасности, делает более опасными последствия взломов, утечек информации или ее незаконного использования, например, для сокрытия событий, подмены документов фотовидеофиксации и т.д.[1]

С учетом изложенного, считаем полезной практику расширения сферы государственного регулирования в области уголовно-процессуальных отношений за счет принятия правительственных постановлений по обеспечению деятельности, связанной с расследованием преступлений. В этой связи логичным и своевременным шагом стало бы принятие комплексных решений, направленных на защиту информации, составляющей тайну следствия и обеспечивающих достоверность добываемых с помощью технических средств доказательств. Тем более, что положения ч.5 ст.166 УПК никак не менее значимы чем ст.6 Федерального закона «Об оперативно-розыскной деятельности».

Появление системы видео-конференц-связи судов общей юрисдикции для проведения апелляционных, кассационных и надзорных судебных процессов было вызвано необходимостью оптимизации сложных и ресурсоемких уголовно-правовых процедур судебного производства. Россия — пионер в освоении новых технологий. 18 ноября 1999 года в Челябинском областном суде впервые в мировой практике состоялся процесс с использованием технологии видео-конференц-связи.

Сегодня в национальной судебной системе существует возможность повсеместного использования средств видео-конференц-связи при рассмотрении любых уголовных дел не только по первой инстанции, но и тех, слушание которых проходит по правилам апелляционного, кассационного и надзорного производства в условиях удаленного участия подсудимого. Применение средств видео-конференц-связи (далее – ВКС) стало возможным и в судах первой инстанции при производстве отдельных процессуальных действий [7, с. 56-59].

Проведение процессуальных действий с использованием средств видео-конференц-связи осуществляется на основании статей 35, 240, 241, 278.1, 293, 389.12, 389.13, 399, 401.13 УПК РФ.

Технические комплексы ВКС судебной системы выполнены для решения процессуальных действий в залах судебного заседания и учреждениях Федеральной службы исполнения наказаний России, в состав которых входят: устройства отображения информации, кодеки видео-конференц-связи, сервера многоточечной связи, микрофонные системы и микширования звука, преобразователи сигналов, конфиденциальные линии связи общения адвокатов с осужденными и лицами,

[1] Разработано решение по криптозащите IP-камер фотовидеофиксации. Сайт Информационного агентства «Индустрия Безопасности». [Электронный ресурс] 20.09.20 https://www.securitymedia.ru/news_one_11409.html (дата обращения: 19.11.2020)

содержащимися под стражей. Используемая техника имеет достаточный технический и программный уровень защиты информации.

Сейчас в судебной системе уже оборудовано более восьми тысяч точек ВКС, по которым ежедневно проходит более полторы тысячи судебных заседаний, а за 20 лет уже проведено несколько миллионов дистанционных судебных заседаний.

Вместе с тем, как показывает практика, другие правоохранительные органы вовлеченные в орбиту уголовного судопроизводства (Прокуратура, МВД, и др.), оборудуют свои территориальные органы другой техникой, что создаёт проблемы межведомственной коммуникации и взаимодействия, необходимость которых очевидно вытекает не только из осуществления прокурором уголовно-процессуальных функций надзора, обвинения и уголовного преследования (ст. 15, 37 УПК РФ), но и такого направления как координации деятельности правоохранительных органов по борьбе с преступностью функции (Ст.8 Федерального закона от 17.01.1992 N 2202-1 "О прокуратуре Российской Федерации"). Поэтому было бы логичным урегулировать основы применения ВКС на уровне Правительства Российской Федерации на основе 20-ти летнего успешного опыта эксплуатации технических средств в Верховном Суде Российской Федерации, с учётом всех унификаций в средствах вычислительной техники и каналах связи.

В системе средств процессуального доказывания как бы особняком стоят следственные действия: «Контроль и запись переговоров» - ст.186 УПК, «Получение информации о соединениях между абонентами и (или) абонентскими устройствами» - ст. 186-1 УПК. Данные процессуальные действия никак не подпадают под традиционное определение следственных, поскольку они не выполняются следователем (дознавателем) и не характеризуются его познавательной активностью [8, с.45-67]. Роль следователя при этом сводится лишь к вынесению постановлений о производстве этих действий и приобщению к делу их результатов. Ответственные лица и организации, технический порядок реализации указанных средств доказывания, варианты защиты информации в законе не предусмотрены, что часто не позволяет выявить отличий данных средств процессуального доказывания от схожих оперативно-розыскных мероприятий: «Просушивание телефонных переговоров» (ч. 1 п. 10 ст. 6 Федерального закона «Об оперативно-розыскной деятельности») и «снятие информации с технических каналов связи» (ч. 1 п. 11 ст. 6 Федерального закона «Об оперативно-розыскной деятельности»), что на практике приводит к сложностям при выборе надлежащих средств процессуального доказывания и способов обеспечения достоверности их результатов.

Очевидно, что помимо более детальной регламентации в УПК, существует необходимость издания нормативного акта правительственного уровня, устанавливающего круг министерств и ведомств, должностных лиц, технических средств и порядок их использования при производстве указанных следственных действий.

Указанными вопросами не исчерпывается круг сложнейших задач и проблем уголовно-процессуальной деятельности, которые цифровая эпоха ставит на повестку дня. Но так или иначе ключ к их решению находится в расширении сферы государственного регулирования в уголовном судопроизводстве, в том числе, на уровне федерального правительства.

Библиографический список

1. Торвальд Ю. Сто лет криминалистики // Пути развития криминалистики. - М.: Прогресс, 1974. - 439 с.

2. Кочерга А.А. Актуальность и проблемы использования автоматизированных систем в работе с криминалистическими учетами // Общество и право. 2011. – № 2. – С. 250 - 254.

3. Качалова О.В., Цветков Ю.А. Электронное уголовное дело – инструмент модернизации уголовного судопроизводства // Российское правосудие. 2015. – № 2. – С. 95-101.
4. Аликперов Х.Д. Электронная технология определения меры наказания («Электронные весы правосудия») / Предисл. докт. юрид. наук, проф. А.И. Коробеева. // СПб.: Издательство «Юридический центр», 2020. 170 с.
5. Девятков В.В. Системы искусственного интеллекта / Гл. ред. И.Б.Фёдоров. — М.: Изд-во МГТУ им. Н. Э. Баумана, 2001. 352 с.
6. Сильнов М.А. К вопросу о допустимости использования цифровых технологий в доказывании при расследовании преступлений // Вестник Российского университета дружбы народов. Серия юридические науки.- М., 1998. – № 3-4. – С. 103-104.
7. Сильнов М.А., Герман А.С. Практика применения видеоконференц-связи в уголовном процессе // Уголовный процесс. 2012. – № 9. – С. 56 - 59.
8. Шейфер С.А. Следственные действия // Система и процессуальная форма. – М., 1981. 127 с.

TOPICAL ISSUES OF STATE REGULATION OF THE USE OF TECHNICAL MEANS IN CRIMINAL PROCEEDINGS

Silnov M.A.
University of the Prosecutor's Office of the Russian Federation, Moscow,
email: silnov@yandex.ru

Abstract. The article discusses the issues of improving the normative regulation of the use of technical means in criminal procedural proving from the standpoint of using software and technical means of protecting information.

Keywords: criminal process; reliability of evidence; investigative actions; protection of information; video conferencing.