УДК 343.13

Юрий Александрович АНДРИЕНКО,
старший следователь по особо важным делам
следственной части Главного следственного управления
ГУ МВД России по Алтайскому краю (г. Барнаул)
andrienko-mvd@mail.ru

ОТДЕЛЬНЫЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И РАБОТЫ С ЭЛЕКТРОННЫМИ НОСИТЕЛЯМИ ИНФОРМАЦИИ В ДОКАЗЫВАНИИ ПО УГОЛОВНЫМ ДЕЛАМ

PARTICULAR ASPECTS OF USING INFORMATION TECHNOLOGIES AND WORKING WITH ELECTRONIC DATA STORAGE DEVICES IN PROVING CRIMINAL CASES

В статье рассматриваются вопросы, связанные с влиянием информационных технологий на доказывание по уголовным делам, нормативным регулированием и практическими аспектами работы следователя с электронными носителями информации, порядка их изъятия, получения и осмотра содержащихся в них данных, обнаружения и использования в доказывании электронных сообщений.

The article considers the most current issues pertaining to the influence of information technologies on proving criminal cases, regulation control and practical aspects of the investigator's work with electronic data storage devices, the procedure of their seizure, receiving and examination of the stored data, discovery and using electronic messages in proving.

Ключевые слова: *предварительное расследование, следователь, доказывание, следственные действия, доказательства, информационные технологии, электронные носители информации, электронные сообщения.*

Keywords: *preliminary investigation, investigator, proving, investigative actions, evidence, information technologies, electronic data storage devices, electronic messages.*

УПК РФ предусматривает различные способы и средства обеспечения следователем быстроты и полноты исследования обстоятельств преступления. Среди них и возможности использования оперативно-розыскного и криминалистического обеспечения производства по уголовному делу, и средства контроля и надзора за деятельностью следователя. Важнейшая роль в обеспечении быстроты и полноты предварительного расследования принадлежит процессу доказывания, заключающемуся в собирании, оценке и проверке доказательств.

Как известно, состояние преступности является своеобразным отражением, индикатором процессов, происходящих в обществе. Стремительное внедрение в последние 10-15 лет продуктов цифровых технологий без преувеличения во все сферы нашей повседневной жизни не замедлило сказаться как на способах совершения преступлений, так и на методах доказывания при расследовании уголовных дел.

В настоящее время широкое распространение получили преступления в сфере незаконного оборота наркотиков, экономики, противоправные деяния экстремистской и террористической направленности и другие преступления, совершаемые с помощью различных электронных носителей (компьютеры, ноутбуки, смартфоны и т.д.), а также с использованием информационно-коммуникационных сетей (включая сеть Интернет). Кроме того, все чаще именно цифровые носители информации, использующиеся фигурантами уголовных дел, несут в себе важную

информацию в виде различных сообщений, фотографий, аудио- и видеозаписей, способную пролить свет на обстоятельства совершенного преступления.

Вышеперечисленные обстоятельства делают электронные носители информации важнейшими вещественными доказательствами, значение которых для уголовного дела невозможно переоценить. Их оперативное изъятие, своевременный и тщательный осмотр, произведенные в соответствии с требованиями закона, могут помочь не только установить обстоятельства совершенного преступления, но и даже пресечь новые преступления.

Так, в марте 2017 г. сотрудниками УНК ГУ МВД России по Алтайскому краю была задержана преступная группа в составе граждан З., Г. и В., которые совместно с неустановленными лицами – организаторами и другими сотрудниками интернет-магазина осуществляли незаконный сбыт синтетических наркотических средств путем формирования тайников с «закладками» в малозаметных местах г. Барнаула (дворах, подъездах многоэтажных домов, промышленных зонах и т.д.). В ходе личных досмотров граждан З., Г. и В. были обнаружены наркотические средства, расфасованные в виде «закладок» для последующего сбыта. Кроме того, в изъятых у З. и В. смартфонах были обнаружены фотографии «закладок», сформированных в подъездах многоэтажных домов непосредственно перед задержанием. Данные «закладки» с наркотическими средствами были в кратчайшие сроки изъяты сотрудниками правоохранительных органов, что позволило не допустить их поступление к наркопотребителям (Судебные и нормативные акты РФ (СудАкт). URL: https://sudact.ru/regular/doc/SSQVtOm1rzNu).

Указанные обстоятельства заставляют правоприменителей и ученых переосмысливать значение и роль электронных носителей информации в уголовном судопроизводстве. Не случайно в последнее время развернулась широкая дискуссия именно по вопросам внедрения цифровых технологий в уголовное судопроизводство, данной проблематике посвящается много статей, монографических исследований.

Вместе с тем приходится констатировать, что отечественное уголовно-процессуальное законодательство не успевает отвечать всем вызовам, которые бросает ему развитие информационных технологий. В то время как практические и научные работники уже ввели в свой обиход такие термины, как «цифровая информация» [2, с. 203–210], «электронные доказательства» [6, с. 120–124], а некоторые исследователи даже говорят о необходимости введения электронных уголовных дел [3, с. 587–595], законодатель в этом плане остается консерватором.

Было бы несправедливо говорить о полном бездействии законодателя в рассматриваемой области, так как несколькими последними изменениями в УПК РФ введены положения, регулирующие порядок изъятия электронных носителей информации и их возврата законным владельцам, осмотра и выемки электронных сообщений, использования электронных документов в уголовном судопроизводстве и т.д.

Вместе с тем нормы, вводимые в УПК РФ с целью регулирования вопросов, касающихся работы с электронными носителями информации, носят довольно противоречивый характер, что порождает ряд спорных моментов и на настоящий момент неразрешенных проблем. Рассмотрим наиболее насущные из них.

Как уже было указано выше, важнейшую роль при расследовании уголовного дела играет своевременное и правильное изъятие электронных носителей информации. Как правило, такое изъятие происходит при производстве обыска или выемки. Федеральным законом от 28 июля 2012 года № 143-ФЗ в статьи УПК РФ, касающиеся производства обыска (ст. 182) и выемки (ст. 183), внесены изменения, в соответствии с которыми изъятие электронных носителей информации в ходе указанных следственных действий должно производиться с участием специалиста. Представляется, что по замыслу законодателя это должно обеспечить сохранность изымаемого носителя информации, предотвратить возможную потерю хранящихся на указанном носителе данных, позволить лицу, у которого производится изъятие носителя

информации, получить копию нужной ему информации.

Указанные нормы об обязательном участии специалиста создали значительные сложности в правоприменительной практике. Так, зачастую по уголовным делам о сбытах наркотических средств обыски в жилище лиц, причастных к совершению преступлений, производятся в условиях, не терпящих отлагательств. Целью таких мероприятий является не только изъятие наркотических средств, но и отыскание средств совершения преступлений, в том числе компьютерной техники. В подобных случаях привлечение специалиста является весьма затруднительным, особенно если обыск производится в ночное время.

Как правило, в подобных ситуациях обнаруживаемая компьютерная техника при отсутствии специалиста изымается де-юре незаконно и в дальнейшем, при обнаружении в ней представляющих интерес данных, признается вещественным доказательством по уголовному делу. Исходя из анализа сложившейся судебной практики, в настоящее время судом и сторонами процесса в большинстве случаев не ставится вопрос о недопустимости изъятых подобным способом вещественных доказательств.

В то же время имеют место противоположные ситуации. Так, по приговору Индустриального районного суда г. Барнаула Алтайского края от 23 декабря 2013 года гражданка Г., обвинявшаяся следственными органами в приготовлении к сбыту наркотического средства в крупном размере (ч. 1 ст. 30, п. «г» ч. 4 ст. 228.1 УК РФ), была признана виновной лишь в незаконном приобретении и хранении указанного наркотика без цели сбыта (ч. 2 ст. 228 УК РФ). Причиной переквалификации действий гражданки Г. с более тяжкого преступления на менее тяжкое послужило признание недопустимым доказательством распечатки переписки указанного лица с сотрудником интернет-магазина, касающейся работы Г. «закладчиком» наркотических средств. Суд, мотивируя указанное решение, акцентировал внимание на том, что в деле отсутствовали сведения об участии специалиста при изъятии указанной переписки (URL: https://rospravosudie.com/court-industrialnyj-rajonnyj-sud-g-barnaula-altajskij-kraj-s/act-459202135).

Не менее дискуссионными являются положения ст. 182 и ст. 183 УПК РФ, предусматривающие копирование информации, содержащейся на изымаемых электронных носителях, которое может быть осуществлено в ходе следственного действия специалистом по ходатайству законного владельца указанных носителей или обладателя содержащейся на них информации. Как показывает практика, на месте производства обыска или выемки довольно проблематично сразу изучить всю информацию в электронном носителе и решить, может ли ее копирование воспрепятствовать расследованию преступления. Поспешное решение следователя о предоставлении копии информации зачастую в дальнейшем может помешать установлению обстоятельств совершения преступления.

Так, в практике ГСУ ГУ МВД России по Алтайскому краю все чаще встречаются случаи, когда работники интернет-магазинов по продаже наркотиков в целях конспирации и во избежание постороннего доступа к аккаунтам в интернет-мессенджерах и другой важной информации устанавливают на используемых в преступной деятельности технические средства (компьютеры, смартфоны) многоуровневые системы защиты, шифрования и сокрытия информации («TrueCrypt», «VPN» и т.д.). Пароли для доступа к таким сокрытым данным могут храниться в виде наименования либо текстового содержимого каких-либо маловажных файлов, таких как рисунки или текстовые документы. Предоставление владельцу технического средства копии этой, на первый взгляд, не представляющей интерес информации дает тому возможность как ограничить доступ следователя к искомым данным посредством другого устройства, так и уничтожить ценную для следствия информацию.

К вышесказанному следует добавить, что общий порядок копирования информации с изъятых электронных носителей для предоставления их законному владельцу подробно регламентирован ч. 2.1 ст. 82 УПК РФ и, по нашему мнению, в дополнительной конкрети-

зации не нуждается. В данном случае следует согласиться с мнением В.В. Кальницкого, говорящего об избыточной процессуализации порядка производства обыска и выемки после введения рассматриваемых изменений. [4, с. 32-38]

Говоря об установленном законодателем обязательном участии специалиста в каждом без исключения случае изъятия электронного носителя информации, также необходимо отметить следующее. Как показывает практика, в подавляющем большинстве случаев непосредственно изъятие электронных носителей не требует наличия у следователя и других участвующих в следственном действии сотрудников правоохранительных органов специальных познаний в технико-компьютерной области. Как правило, общие криминалистические знания и навыки работы с электронными носителями на уровне среднестатистического пользователя оказываются достаточными, поскольку, как уже указывалось, цифровые технологии давно стали неотъемлемой частью нашей жизни, а некоторые сферы деятельности человека уже невозможно представить без них. Возникающие сложности при изъятии электронных носителей информации, например вероятность удаления информации в результате неправильного отключения техники от сети, являются частными случаями, и поэтому неправильно распространять их на общий порядок производства обыска и выемки.

Анализируя рассмотренные выше ситуации, полагаем, что при регулировании изъятия электронных носителей информации в ходе обыска и выемки было бы целесообразным руководствоваться общими правилами привлечения специалиста для участия в следственных действиях, установленными ст. 168 УПК РФ. Для этого необходимо внести изменения в ч. 9.1 ст. 182 УПК РФ и ч. 3.1 ст. 183 УПК РФ об оставлении за следователем права привлечения специалиста для изъятия электронных носителей информации. Кроме того, было бы разумным предусмотреть срок для предоставления копии информации с изъятых электронных носителей их законному владельцу или обладателю указанной информации.

В 2016 г. большой резонанс в российском обществе вызвало принятие так называемого пакета законов «Яровой-Озерова» (Федерального закона от 6 июля 2016 г. №374-ФЗ, Федерального закона от 6 июля 2016 г. №375-ФЗ) по установлению дополнительных мер противодействия терроризму и обеспечения общественной безопасности.

Наиболее значительные обсуждения вызвали изменения в Федеральный закон от 27 июля 2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации», введенные вышеназванным ФЗ от 6 июля 2016 года №374-ФЗ, в соответствии с которыми организаторы распространения информации в сети Интернет (в том числе «VKontakte», «WhatsApp», «Telegram», «Viber» и т.д.) обязаны хранить на территории РФ:

– информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков, видео- или иных электронных сообщений пользователей сети Интернет и информацию об этих пользователях в течение одного года с момента окончания осуществления таких действий;

– текстовые сообщения пользователей сети Интернет, голосовую информацию, изображения, звуки, видео-, иные электронные сообщения пользователей сети Интернет до шести месяцев с момента окончания их приема, передачи, доставки и (или) обработки.

Кроме того, указанными изменениями на организаторов распространения информации в сети Интернет была возложена обязанность предоставлять вышеуказанную информацию уполномоченным государственным органам, осуществляющим оперативно-разыскную деятельность или обеспечение безопасности РФ в случаях, установленных федеральными законами.

На первый взгляд, вышеперечисленные изменения, носящие без преувеличения революционный характер, призваны существенно облегчить как раскрытие преступлений и выявление лиц, их совершивших, так и процесс доказывания по уголовному делу. В то же время на практике применение вышеуказанных норм в досудебном производстве по

уголовному делу может вызвать ряд затруднений.

В частности, вызывает недоумение перечень субъектов, уполномоченных запрашивать сведения у организаторов распространения информации в сети Интернет, который ограничивается уполномоченными государственными органами, осуществляющими оперативно-разыскную деятельность или обеспечение безопасности РФ. Как уже отмечалось исследователями, из данного положения следует, что организаторы распространения информации в сети Интернет не обязаны предоставлять электронные сообщения органам, осуществляющим предварительное расследование. [7, с. 59-64].

Принятием пакета законов «Яровой-Озерова» были также внесены изменения и в УПК РФ. Так, вышеупомянутым Федеральным законом от 6 июля 2016 г. №375-ФЗ в ст. 185 УПК РФ, регулирующую порядок наложения ареста на почтово-телеграфные отправления, их осмотр и выемку, была введена часть 7. В соответствии с указанной нормой при наличии достаточных оснований полагать, что сведения, имеющие значение для уголовного дела, могут содержаться в электронных сообщениях или иных передаваемых по сетям электросвязи сообщениях, следователем по решению суда могут быть проведены их осмотр и выемка.

Введение указанной новеллы вызвало неоднозначный отклик как у практических работников, так и ученых-процессуалистов. И больше всего вопросов вызывает не столько содержание данной нормы, сколько ее включение законодателем в ст. 185 УПК РФ. В этом смысле следует согласиться с Б.Т. Безлепкиным, по мнению которого актуальность и практическую значимость ч. 7 ст. 185 УПК РФ для раскрытия и расследования преступлений невозможно переоценить. Но в ст. 185 УПК, посвященной наложению ареста на почтово-телеграфные отправления, их осмотру и выемке в учреждениях связи, она «чужая». Задержание, наложение ареста, осмотр и выемка электронных и иных передаваемых по сетям электросвязи сообщений индивидуально-определенных отправителей и (или) получателей таких сообщений на основании заранее представленного следователем судебного решения в учреждениях связи не предусмотрено УПК РФ, не осуществляется на практике и технически невозможно [1, с. 162].

Другим немаловажным вопросом, до сегодняшнего дня не урегулированным уголовно-процессуальным законом, является исследование электронных носителей информации с их подключением к сети Интернет. В частности, такая необходимость возникает в случаях, когда ценная для следствия информация хранится не в самой памяти телефона, а в облачном хранилище данных, или «облаке». Это могут быть и переписка в интернет-мессенджерах, и сведения о посещенных местах (например, из приложения «Google Maps» или других аналогичных программ), и даже медиафайлы (фотографии, видеозаписи). Доступ к информации из «облака» с помощью изъятого электронного носителя возможен только при его подключении к сети Интернет. Однако в этом случае изучение информации уже выходит за пределы изъятого объекта (ноутбука, телефона и т.д.).

Рассматриваемый аспект работы с электронными носителями информации затрагивает целый комплекс вопросов процессуального характера, связанных и с выбором подходящего следственного действия, и с обеспечением прав лиц, чьи интересы могут быть затронуты проведением следственных действий. Проанализируем обозначенные вопросы в контексте их возникновения на практике.

Как уже отмечалось исследователями [5, с. 142–146] и подтверждено практическими примерами, при изъятии электронного носителя и возникновении необходимости его исследования с подключением к сети Интернет наиболее вероятны два варианта развития событий.

В первом случае, лицо, чей электронный носитель изъят, дает согласие на ознакомление следователя с информацией из принадлежащего ему технического средства и сообщает все необходимые сведения (логины, пароли) для осуществления доступа к представляющим интерес данным.

При наличии указанной выше ситуации в ГСУ ГУ МВД России по Алтайскому краю применяется практика производства следственного эксперимента с участием владельца электронного носителя информации. В ходе данного следственного действия участвующему лицу предоставляется принадлежащее ему техническое средство, подключенное к сети Интернет, и предлагается воспроизвести и продемонстрировать определенные действия, например, которые лицо выполняло при работе в интернет-магазине, сбывавшем наркотические средства. В ходе данного следственного действия следователь может установить и зафиксировать значительное количество важной информации: последовательность действий подозреваемого при совершении преступления, многоуровневые способы и методы конспирации, сокрытия информации, содержание переписки и других файлов, касающихся обстоятельств уголовного дела. При проведении следственного эксперимента необходимо обеспечить обширное применение технических средств для фиксации его хода и результатов посредством фото-, видеосъемки, производства скриншотов с экрана электронного носителя.

Исследование электронного носителя путем следственного эксперимента в подобных случаях обосновано тем, что по своей природе именно данное следственное действие наиболее соответствует описанному выше способу получения и исследования информации, когда участвующему в следственном действии лицу предоставлена активная роль в ее демонстрации. Вместе с тем представляется, что исследование информации с помощью изъятого электронного носителя, подключенного к сети Интернет, допустимо и в ходе его осмотра.

В другом случае лицо, которому принадлежит изъятый электронный носитель, отказывается предоставлять данные, необходимые для доступа к представляющей интерес информации и ознакомления с ней, и не желает принимать участие в следственных действиях по получению и исследованию указанной информации с подключением к сети Интернет.

Наиболее разумным представляется вариант регулирования подобных ситуаций, при котором следственные действия по исследованию электронных носителей информации с их подключением к сети Интернет будут производиться в соответствии с требованиями ст. 165 УПК РФ, то есть на основании судебного решения, а в случаях, не терпящих отлагательства, без такого, но с последующим уведомлением суда о произведенном следственном действии. Введение соответствующих изменений позволило бы также исключить нарушения права владельца изъятого электронного носителя информации на тайну переписки и иных сообщений.

С учетом изложенного можно сделать вывод, что для устранения разночтений в вопросах получения и осмотра электронных сообщений и другой информации, передаваемой посредством информационно-телекоммуникационных сетей, а также хранящейся в изъятых электронных носителях, целесообразно нормы, регулирующие данную область, выделить в отдельную статью в главе 25 УПК РФ. Это также позволит сформировать единую практику работы следователя с электронными носителями и использования информационно-телекоммуникационных сетей в ходе следственных действий.

Подводя итог вышесказанному, следует сказать, что в настоящее время в отечественном уголовном судопроизводстве существует немало проблем, касающихся нормативного регулирования работы следователя с электронными носителями, порядка их изъятия, получения и осмотра содержащейся в них информации. В условиях стремительного развития информационных технологий, их широкого использования при совершении преступлений законодателю необходимо адекватно и своевременно реагировать на это путем внесения соответствующих поправок в нормы УПК. Наличие у следователя отвечающих требованиям времени процессуальных инструментов позволит эффективно осуществлять доказывание по уголовным делам и тем самым обеспечивать качественное предварительное расследование.

Библиографический список

1. Безлепкин, Б.Т. Уголовный процесс в вопросах и ответах : учебное пособие / Б.Т. Безлепкин. – 9-е изд., перераб. и доп. – М. : Проспект, 2018. – 304 с.

2. Васюков, В.Ф. Некоторые проблемы получения и использования цифровой информации при расследовании уголовных дел / В.Ф. Васюков, Е.А. Семенов // Известия ТулГУ. Экономические и юридические науки. – 2016. – № 3 –2. – С. 203–210.

3. Зуев, С.В. Информационные технологии в решении уголовно-процессуальных проблем / С.В. Зуев, Е.В. Никитин // Всероссийский криминологический журнал. – 2017. – № 3. – С. 587–595.

4. Кальницкий, В.В. Вопросы правовой регламентации следственных действий на современном этапе / В.В. Кальницкий // Законы России: опыт, анализ, практика. – 2015. – № 2. – С. 32–38.

5. Карлов, А.Л. Использование в доказывании по уголовным делам сведений, составляющих тайну связи, расположенных в сети Интернет / А.Л. Карлов // Вестник Сибирского юридического института ФСКН России. – 2015. – № 2 (19). – С. 142–146.

6. Оконенко, Р.И. Электронные доказательства как новое направление совершенствования российского уголовно-процессуального права / Р.И. Оконенко // Актуальные проблемы российского права. – 2015. – № 3. – С. 120–124.

7. Супрун, С.В. О противоречивом характере новеллы в законодательном регулировании следственного действия «Наложение ареста на почтово-телеграфные отправления» / С.В. Супрун, В.С. Черкасов // Вестник ОмЮА. – 2017. – № 1. – С. 59–64.