Министерство внутренних дел Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ КАЗЕННОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СИБИРСКИЙ ЮРИДИЧЕСКИЙ ИНСТИТУТ
МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ»
(СибЮИ МВД России)

УДК 343.1, 343.12, 343.13
Рег. № 01221551
Инв. № 02220658

УТВЕРЖДАЮ
Начальник
СибЮИ МВД России
доктор юридических наук,
профессор
генерал-майор полиции
Д.В. Ким
«___» _____ 2022 г.

ОТЧЕТ
О НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ РАБОТЕ

ПРАВОВЫЕ АСПЕКТЫ ПОЛУЧЕНИЯ И ИСПОЛЬЗОВАНИЯ ИНТЕРНЕТ-ПЕРЕПИСКИ В ДОКАЗЫВАНИИ ПО УГОЛОВНЫМ ДЕЛАМ О ПРЕСТУПЛЕНИЯХ В СФЕРЕ НЕЗАКОННОГО ОБОРОТА НАРКОТИКОВ

(заключительный)

Шифр работы, присвоенный организацией: 27

Руководитель НИР,
старший преподаватель
кафедры уголовного процесса
подполковник полиции А.Л. Карлов

Красноярск 2022

СПИСОК ИСПОЛНИТЕЛЕЙ

Руководитель НИР,
старший преподаватель
кафедры уголовного процесса
подполковник полиции — А.Л. Карлов
(ведение, разделы 1,2,3,4, заключение)

Исполнители:

Следователь отдела по РОПД в сфере НОН
СЧ по РОПД ГСУ ГУ МВД России
по Красноярскому краю
капитан юстиции — Т. А. Вельямидова
(сбор и предоставление эмпирических материалов)

Нормоконтроль — А.Н. Михайлов

РЕФЕРАТ

Отчет 40 с., 17 источн.

ДОКАЗАТЕЛЬСТВА, ИНТЕРНЕТ-ПЕРЕПИСКА, НАРКОТИКИ, НЕЗАКОННЫЙ ОБОРОТ, СЛЕДСТВЕННЫЕ ДЕЙСТВИЯ, ТАЙНА СВЯЗИ

Объект исследования – общественные отношения, складывающиеся между лицом, ведущим расследование по уголовному делу и иными участниками уголовного судопроизводства, в процессе получения и дальнейшего использования переписки между абонентами в сети Интернет.

Цель исследования – разработать практические рекомендации, направленные на правильное применение закона в процессе получения и использования интернет-переписки как доказательства по уголовному делу.

Методология проведенного исследования: в качестве основных использовались методы сравнительно-правового анализа, эмпирический, а также методы обработки информации – анализ, синтез, прогноз.

По результатам исследования подготовлены методические рекомендации, позволяющие определить порядок действий следователя (дознавателя), позволяющий обеспечить доказательственное значение интернет-переписки при расследовании уголовного дела.

Итоговая научная продукция может быть использована в практической, а также образовательной деятельности.

Научная новизна и практическая ценность полученных выводов связаны, прежде всего, с отсутствием буквально выраженной позиции законодателя по многим аспектам использования в доказывании интернет-переписки, а также с отличающимися подходами в следственно-судебной практике.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность работы связана с распространенностью фактов использования в доказывании по уголовным делам о преступлениях в сфере незаконного оборота наркотиков сведений об интернет-переписке, а также с тем, что однозначных позиций по многим сопутствующим вопросам до настоящего времени не сформировано. В научной литературе встречаются лишь фрагментарные материалы по предмету исследования. Основная часть публикаций освещает лишь криминалистические вопросы, связанные с тактикой и методикой получения интернет-переписки, при этом не акцентируется внимание не правовых (уголовно-процессуальных) положениях в соотношении со складывающейся следственной и судебной практикой. Такое положение дел влечет неправильное представление о правовом статусе интернет-переписки и режиме доступа к таким данным.

Особенностью представленной работы является то, что материал изложен сугубо в уголовно-процессуальном ключе с позиций законности и обеспечения допустимости доказательств, а также преимущественно на основе эмпирических материалов о преступлениях в сфере незаконного оборота наркотиков.

Перечень исследованных вопросов определен исходя из порядка действий следователя (дознавателя) с учетом вариативности той информации, которая поступает ему процессе расследования преступлений.

ОСНОВНАЯ ЧАСТЬ

1 Общая характеристика работы

Основание для проведения исследования: инициатива кафедры уголовного процесса, пункт 27 Плана научной деятельности Сибирского юридического института МВД России на 2022 год.

Вид научного результата: методические рекомендации.

Срок завершения НИР: сентябрь 2022 года.

Учитывая теоретическое и практическое значение, исходя из обозначенных проблем и поставленной цели исследования в ходе проведенной научно-исследовательской работы решались следующие задачи:

- изучение и обобщение теоретических аспектов по вопросам выбора надлежащего следственного действия, направленного на получение и фиксацию интернет-переписки по преступлениям в сфере незаконного оборота наркотиков;

- определение надлежащего порядка действия следователя (дознавателя) при документировании интернет-переписки, расположенной на электронных носителях информации;

- определение надлежащего порядка действия следователя (дознавателя) при документировании интернет-переписки, расположенной на удаленных серверах сети Интернет (в том числе части необходимости получения судебного решения);

- разработка соответствующего закону алгоритма действий по получению интернет-переписки в ходе расследования уголовного дела о преступлении в сфере незаконного оборота наркотиков.

В работе исследована совокупность норм уголовно-процессуального права, а также нормативные акты, регламентирующие право на тайну переписки, телефонных и иных переговоров, обобщены правовые позиции

Конституционного Суда РФ и Верховного Суда РФ по исследуемым вопросам.

Базовая часть работы основана на теоретических и эмпирических источниках: примерах судебной практики, аналитических обзорах, результатах проведенного интервьюирования. Изучена практика расследования 16 уголовных дел, находившихся в производстве ГСУ ГУ МВД Росси по Красноярскому краю.

Значимость исследования определяется выполнением научной задачи, посредством интерпретации автором имеющихся положений, а также выработке новых теоретических подходов, касающихся вопросов получения и использования в доказывании интернет-переписки. Практическая значимость заключается в детальной проработке отдельных этапов деятельности следователя (дознавателя), а также процессуальных решений, сопровождающих получение интернет-переписки. Следование выработанному алгоритму позволит исключить нарушение законности и, как следствие, признание полученных доказательств недопустимыми.

2 Сведения об использовании результатов научных исследований, проводимых иными организациями системы МВД России

В целях сбора и анализа информации по теме исследования изучены размещенные в Банке данных системы научно-технической информации МВД России научные исследования, проведенные иными организациями МВД России. Результаты показали, что проблемы использования интернет-переписки в доказывании по уголовным делам о преступлениях в сфере незаконного оборота наркотиков предметно практически не исследовались.

Так, в 2009 г. по результатам научного исследования, проведенного авторами Академии экономической безопасности МВД России под руководством доктора юридических наук, профессора Ю.Е. Ширяева, подготовлена научно-исследовательская работа на тему «Конституционное право на тайну сообщений и механизм его реализации в Российской Федерации». Следует отметить, что авторами проведено комплексное исследование актуальных теоретических и практических проблем, возникающих, с одной стороны, в связи с закреплением в Конституции РФ права граждан на тайну переписки, телефонных переговоров, телеграфных и иных сообщений как составного элемента института неприкосновенности частной жизни, а с другой стороны – в связи с бурным развитием научно-технического прогресса, появлением новых способов связи и средств межличностного общения, со стремительным ростом информационной инфраструктуры, с тенденцией к увеличению открытости общества, повышением интенсивности информационного обмена, широким использованием передовых информационных технологий. Вместе с тем, в работе не содержится предметных правил и алгоритмов, учитывающих специфику уголовного судопроизводства.

Методические рекомендации по теме «Особенности расследования преступлений в сфере незаконного оборота наркотиков», подготовленное коллективом сотрудников Уфимского юридического института МВД России

в 2019 году, содержат проработку порядка производства следственных действий по рассматриваемой категории дел, авторы указывают на необходимость изъятия переписки в ходе обыска (стр. 33), однако при этом не затрагиваются вопросы правовых оснований и порядка такого изъятия, соотношение с тайной связи. В этом же учебном заведении в 2019 году были подготовлены методические рекомендации по теме «Особенности осмотра компьютерной техники и электронных документов» под руководством кандидата юридических наук, доцента А.Ю. Самойлова. В данной работе авторы задаются вопросами о выборе следственного действия для изъятия сведений, хранящихся на удаленных серверах сети «Интернет», при этом предлагают для их изъятия использовать обыск или выемку. Оценить позицию авторов не представилось возможным, поскольку каких-либо доводов и аргументов, в обоснование своей позиции они не приводят.

Об отнесении к тайне связи отдельных сведений, которые могут быть получены от оператора связи, говорит в своей работе А.В. Тарнтынский (методические рекомендации по теме «Особенности расследования преступлений, связанных со сбытом наркотических средств, совершённых с использованием современных систем связи», подготовленные следственным управлением УМВД России по Ханты-Мансийскому автономному округу – Югре), он разграничивает материалы, которые могут быть получены без судебного решения от тех, которые требуют обязательного обращения в суд. Данные сведения представляют определенный интерес для настоящего исследования, как и аналитический обзор «Организация и тактика осмотра и изъятия электронных носителей информации», подготовленный авторским коллективом Академии управления МВД России под руководством доктора юридических наук, доцента Ю.В. Гаврилина.

Таким образом, обзорный анализ обнаруженных источников дает основание полагать, что в большинстве своем научно-исследовательские работы близкой тематики работы носят криминалистический характер, не

учитывают специфику уголовно-процессуальных отношений, что дополнительно подтверждает актуальность проведенного исследования.

3 Выявленные проблемы, требующие научного решения, и результаты их анализа

3.1 Обоснование проблемы выбора надлежащего следственного действия для получения интернет-переписки по делам о преступлениях в сфере незаконного оборота наркотиков

В современных условиях информационного общества все более распространенным становится использование компьютерной техники, специального программного обеспечения и глобальной сети Интернет в качестве орудий и средств совершения различных правонарушений. Использование указанных средств формирует новые способы совершения преступлений в сфере незаконного оборота наркотиков, таких как «бесконтактный сбыт», контрабанда, совершенная путем заказа наркотика через сеть Интернет и др.

Анализ судебной и следственной практики показывает, что информационно-компьютерные средства используются злоумышленниками на всех этапах преступной деятельности (при подготовке к совершению преступлений; при их непосредственном совершении и дальнейших действиях, направленных на сокрытие следов преступлений или распоряжение полученными денежными средствами).

Изучение уголовных дел, расследуемых в ГСУ ГУ МВД России по Красноярскому краю подтверждает, что в большинстве случаев использование компьютерной техники и сети Интернет при совершении преступлений сводится к обмену различными сведениями между абонентами, причем наибольшее значение приобретает обнаружение и процессуальная фиксация интернет-переписки[1], которая зачастую позволяет подтвердить (доказать) место, время, способ совершения преступления, факт достижения

[1] Под интернет-перепиской в данной работе следует понимать обмен текстовыми сообщениями, а также файлами различного содержания между пользователями, посредством сети Интернет.

сговора, а также отдельные обстоятельства, свидетельствующие о наличии умысла на совершение преступления.

Подобные примеры встречаются и в других регионах нашей страны, так в приговоре Волжского городского суда (Волгоградская область) от 7 мая 2015 г. по делу № 1-358/2015, указывается, что сбытчик наркотиков скинул одному из своих соучастников гиперссылку на интернет сайт под названием «bit coin» и реквизиты, после чего посредством данной платежной системы тот перевел интернет- продавцу денежные средства в размере 800 долларов[1]. В приговоре Советского районного суда г. Омска от 19 мая 2017 г. по делу № 1-232/2017 также указывается, что злоумышленник, получив сообщение с адресом, на который необходимо отправить денежные средства, через электронный терминал на Bitcoin - кошелек магазина перечислил денежные средства в сумме 8200 рублей, получив сообщение о нескольких местам нахождения закладок[2].

Несмотря на большое доказательственное значение интернет-переписки, достаточно часто следователь, получив доступ к о переписке, сталкивается с проблемами её надлежащего процессуального закрепления и дальнейшего использовании в доказывании, в том числе с проблемой выбора следственного действия.

Начать нужно с того, что интересующая следователя переписка может храниться в сети Интернет (на удаленных серверах) либо на электронных носителях пользователя, причем на данных носителях она может находиться как в явном виде (текстовые файлы, архивы программы и т.д.), так и в зашифрованном (log-файлов, системных файлов, данных реестра и т.д.), причем в каждом из указанных случаев, процессуальная форма фиксации сведений должна отличаться.

---

[1] Официальный сайт Волжского городского суда. URL: https://vol--vol.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=15607125&delo_id=1540006&new=0&text_number=1.

[2] Официальный сайт Советского районного суда г. Омска. URL: https://sovetsky--oms.sudrf.ru/modules.php?name=sud_delo&name_op=case&_id=12933699&_deloId=1540006&_caseType=0&_new=0&_doc=1&srv_num=1.

В ситуации нахождения переписки на электронных носителях, значительных трудностей при выборе следственного действия не возникает, и в большинстве случаев следователи абсолютно оправданно проводят осмотр предметов (самого электронного носителя: телефона, ноутбука, USB-накопителя и др.), либо судебную экспертизу, если для извлечения информации с такого носителя требуются специальные познания. Однако стоит учитывать, что на сегодняшний день законом предусмотрены специальные правила изъятия таких носителей при производстве следственных действий, в том числе по преступлениям в сфере незаконного оборота наркотиков.

Правовая регламентация порядка изъятия электронных носителей информации при проведении следственных действий впервые была произведена в 2012 году. Статьи 182 и 183 УПК РФ были дополнены отдельными частями (9.1 и 3.1), предусматривающими специальные правила изъятия электронных носителей информации, в том числе обязательное участие специалиста при таком изъятии. Федеральным законом от 27.12.2018 № 533-ФЗ «О внесении изменений в статьи 76.1 и 145.1 Уголовного кодекса Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации» указанные положения закона были исключены, вместе с тем УПК РФ был дополнен статьей 164.1, которая в значительной степени дублирует ранее действовавшие правила изъятия электронных носителей информации, однако данные правила распространили свое действие не только на обыск и выемку (как было ранее), но и на любые другие следственные действия.

Согласно п. 3.1.9 ГОСТ 2.051-2013 «Единая система конструкторской документации. Электронные документы. Общие положения» электронный носитель – это «материальный носитель, используемый для записи, хранения и воспроизведения информации, обрабатываемой с помощью средств вычислительной техники». К электронным носителям информации относят довольно обширный перечень объектов: внутренний накопитель на жестком

магнитном диске («жесткий диск», «винчестер», «винт», Hard Disk Drive – HDD); оптический диск («лазерный диск», «компакт-диск», CD, DVD, диск Blu-Ray, HD-DVD); карта памяти («флэш-карта»); USB флеш-накопитель («флешка»); гибкий магнитный диск («дискета», Floppy Disk Drive – FDD) и многие другие, вплоть до интегральной микросхемы памяти (интегральная схема, чип, микрочип), которая может выполнять различные функции, в том числе выступать в качестве модулей и схем памяти и реализовывать функции миникомпьютера (следовательно, содержать информацию, имеющую значение для уголовного дела)[1]. Помимо указанных к электронным носителям информации безусловно необходимо относить мобильные телефоны, ноутбуки, системные блоки компьютера, поскольку данные устройства могут хранить в себе электронную информацию.

Статья 164.1 УПК РФ содержит неоднозначное по содержанию и достаточно категоричное по форме правило, согласно которому при производстве по преступлениям в сфере экономической деятельности изъятие электронных носителей информации не допускается. Для рассматриваемой категории преступлений это правило становится актуальным при вменении дополнительного состава легализации средств, добытых от незаконного оборота наркотиков (ст.174, 174.1 УК РФ).

На наш взгляд, формулировка, запрещающая изымать электронные носители информации при расследовании указанных преступлений, не учитывает, что далеко не все носители, которые потенциально могут быть изъяты, связаны с предпринимательской деятельностью. Заложенный в ч. 1 ст. 164.1 УПК РФ запрет необоснованно ограничивает субъекта доказывания в собирании доказательств, в связи с чем должен толковаться не буквально, а с учетом ч. 4.1 ст. 164 УПК РФ, в которой говорится о недопустимости необоснованного применения мер, могущих привести к приостановлению

[1] Судницын А.Б. Отдельные процессуальные и организационные особенности изъятия и хранения электронных носителей информации при производстве по уголовным делам // Вестник Сибирского юридического института ФСКН России. 2016. № 1 (22). С.12.

законной деятельности юридических лиц или индивидуальных предпринимателей.

Вместе с тем законодатель предусматривает исключения, допускающие изъятие электронных носителей в том числе при расследовании указанных выше преступлений. К ним относятся случаи, когда:

1) вынесено постановление о назначении судебной экспертизы в отношении электронных носителей информации;

2) изъятие электронных носителей информации производится на основании судебного решения;

3) на электронных носителях содержится информация, полномочиями на хранение и использование которой владелец электронного носителя информации не обладает, либо которая может быть использована для совершения новых преступлений, либо копирование которой, по заявлению специалиста, может повлечь за собой ее утрату или изменение.

Толкование и тем более применение данных положений вызывают существенные затруднения. Так, не ясно, какие электронные носители законодатель имеет в виду, говоря о назначении судебной экспертизы. Если те, которые подлежат изъятию, то каким образом в отношении них уже может быть назначена экспертиза? Если другие электронные носители – то как они были изъяты при наличии общего запрета?

Второе исключение не менее сложно для понимания. Какое судебное решение имеет в виду законодатель? Если следовать буквальному смыслу, то это не любое решение суда (например, о производстве обыска в жилище), а такое, которое является основанием для изъятия электронных носителей. Представляется, что речь идет, в частности, о носителях, содержащих охраняемую законом тайну, доступ к которой может быть получен не иначе, как на основании судебного решения.

Последнее исключение состоит из трех самостоятельных исходных ситуаций. Первая заключается в том, что лицо, у которого предполагается изъятие носителя, не обладает полномочиями на хранение и использование

информации на таком носителе. С практической точки зрения достаточно сложно судить о полномочиях лица в отношении какой-либо информации. Полагаем, что здесь можно говорить о случаях, когда сам носитель находится у человека на незаконных основаниях (например, предмет хищения), исходя из этого мы имеем возможность сделать вывод об отсутствии полномочий и в отношении информации на изымаемом носителе. Также законодатель позволяет изъять электронный носитель, когда информация на нем может быть использована для совершения новых преступлений. Вне всякого сомнения, к такому выводу можно прийти лишь после ознакомления с содержанием информации. По нашему мнению, к такой информации можно отнести различные вредоносные программы, пароли доступа и логины электронных профилей, посредством которых могут быть совершены преступления, различного рода электронные базы данных и др. Наиболее понятной и применимой можно считать ситуацию, при которой по заявлению специалиста копирование при производстве следственного действия может повлечь за собой утрату или изменение информации на носителе. Речь идет о случаях, когда следователь, руководствуясь запретом на изъятие электронных носителей, рассматривает возможность копирования важной для доказывания информации без изъятия самого носителя. Если в такой ситуации участвующий в следственном действии специалист заявит о вероятности утраты или изменения информации, запрет на изъятие электронного носителя снимается.

Дополнительно стоит сказать, что по аналогии с п. 7 постановления Пленума Верховного Суда Российской Федерации «О практике применения судами законодательства о мерах пресечения в виде заключения под стражу, домашнего ареста и залога», можно утверждать, что если лицо подозревается или обвиняется в совершении не только преступления, подпадающего под запрет изъятия электронных носителей, но и предусмотренного иной статьей Особенной части УК РФ (в частности в сфере незаконного оборота

наркотиков), электронные носители могут быть изъяты без каких-либо ограничений.

При положительном решении вопроса о возможности изъятия электронных носителей должны быть учтены правила их изъятия, которые мы предлагаем последовательно рассмотреть.

1. Обязательное участие специалиста при изъятии электронных носителей информации**.**

Часть 2 ст. 164.1 УПК РФ гласит: «Электронные носители информации изымаются в ходе производства следственных действий с участием специалиста…». Данная формулировка по содержанию аналогична ранее действующей и, по мнению большинства авторов, обязывает следователя привлекать специалиста при изъятии электронных носителей[1]. Такой подход мы полностью поддерживаем и полагаем, что непривлечение специалиста является нарушением порядка и с учетом п. 3 ч. 2 ст. 75 УПК РФ ставит вопрос о допустимости полученного доказательства. Следует подчеркнуть, что на отсутствие специалиста защитники и представители обращают самое пристальное внимание, требуя признать незаконным производство следственного действия (см., напр.: апелляционные определения Московского городского суда от 30.09.2013 № 10-9507, от 25.11.2013 № 10-12096 // СПС КонсультантПлюс).

Вместе с тем в научной литературе можно встретить немало примеров, когда суды, рассматривая изъятие электронного носителя без участия специалиста, оставляют в силе полученные доказательства по причине признания допущенного нарушения несущественным[2].

---

[1] Зуев С.В. Осмотр и изъятие электронных носителей информации при проведении следственных действий и оперативно-розыскных мероприятий // Законность. 2018. № 4. С.58; Козловский П.В., Седельников П.В. Участие специалиста в изъятии электронных носителей // Научный вестник Омской академии МВД России. 2014. № 1(52). С.18.

[2] Зуев С.В., Черкасов В.С. Новые правила изъятия электронных носителей и копирования информации (статья 1641 УПК РФ): преимущества и недостатки новеллы // Сибирское юридическое обозрение. 2019. № 2. С.195.

В данном случае решения судов в полной мере соответствуют толкованию, данному Пленумом Верховного Суда Российской Федерации в постановлении от 19.12.2017 № 51 «О практике применения законодательства при рассмотрении уголовных дел в суде первой инстанции (общий порядок судопроизводства)», который указал, что доказательства признаются недопустимыми, в частности, если были допущены существенные нарушения установленного уголовно-процессуальным законодательством порядка их собирания и закрепления.

Говоря о допустимости доказательств, можно привести мнение М.А. Барановой и В.Л. Григоряна[1], которые определяют существенность нарушения в зависимости от того, насколько они:

- ограничивают права заинтересованных участников процесса;

- противоречат требованиям уголовно-процессуальной формы и другим процессуально значимым факторам;

- блокируют возможность полноценной реализации принципов уголовного судопроизводства.

Соответственно, возникает вопрос: как определить существенность отсутствия специалиста в том или ином случае? Когда изъятие электронного носителя без его участия не будет являться существенным нарушением порядка проведения следственного действия?

Подробный анализ необходимости привлечения специалиста при изъятии электронных носителей произвели Ф.В. Васюков, А.В. Булыжкин, которые обобщили взгляды авторов по данной проблеме и выделили три основных подхода[2]. Первый сводится к решению вопроса об участии специалиста в зависимости от потребности уполномоченных лиц в

[1] Баранова М.А., Григорян В.Л. Признание доказательств недопустимыми в судебных решениях по уголовным делам: поиск критериев // Юридическая наука и правоохранительная практика. 2016. № 1 (35). С.122.

[2] Васюков В.Ф. Изъятие электронных носителей информации при расследовании преступлений: нерешенные проблемы правового регулирования и правоприменения / В.Ф. Васюков, А.В. Булыжкин // Российский следователь. 2016. № 6. С.5.

специальных познаниях, второй – в зависимости от типа электронного носителя информации (если это технически простой носитель, следователь может изъять его самостоятельно). Третий подход говорит о необходимости учитывать способ изъятия информации, то есть в случае, если в ходе следственного действия в целях получения информации происходит копирование с электронных устройств, обнаруженных при обыске, участие специалиста обязательно. Стоит отметить, что последний из приведенных подходов противоречит действующему закону, так как порядок действий в указанном случае регламентирован ч. 3 ст. 164.1 УПК РФ и обязательного участия специалиста не предусматривает.

Полагаем, что приведённые мнения в большей мере учитывают криминалистические подходы к проблеме, предполагают анализ вопросов целесообразности, технических особенностей получения доказательств, при этом не принимают во внимание правовые (уголовно-процессуальные) аспекты, связанные с необходимостью обеспечить права участников процесса, и в первую очередь право на копирование информации с изымаемых электронных носителей. Именно наличие данного права, на наш взгляд, делает обязательным участие специалиста. Во-первых, потому что изменения в части обязательного участия специалиста были внесены в закон одновременно с закреплением права на копирование информации; во-вторых, само по себе копирование, согласно положениям УПК РФ, может быть осуществлено только специалистом; в-третьих, одним из оснований для отказа в копировании является «заявление специалиста» о возможной утрате или изменении информации, содержащейся на изымаемом электронном носителе.

Вне зависимости от технической сложности изымаемого носителя, потребности в использовании специальных знаний и других особенностей отсутствие специалиста при изъятии электронных носителей лишает его законного владельца или обладателя потенциальной возможности реализовать право на копирование. Исходя из этого именно объективная

вероятность привлечения специалиста для разрешения ходатайства о копировании информации с изымаемых электронных носителей или к самой процедуре копирования должна учитываться как критерий существенности участия специалиста. При этом техническая сложность изъятия или самого электронного носителя определяет лишь общее правило, согласно которому специалист может быть привлечен к участию в следственных действиях по усмотрению следователя (дознавателя).

Обозначенный подход позволяет утверждать, что для преступлений в сфере незаконного оборота наркотиков не будет являться существенным нарушением отсутствие специалиста в следующих практических ситуациях:

- изъятие у приобретателя или сбытчика наркотиков технических устройств, которые находились у них в пользовании и были добровольно представлены ими следователю (в такой ситуации данные лица имели возможность скопировать информацию до изъятия);

- изъятие носителей, содержащих сведения о переписке у представителей оператора связи (у оператора связи остаются копии передаваемых сведений);

- изъятие у представителя банка или иных организаций носителей, содержащих видеозапись или фотоснимки с камер видеонаблюдения (подтверждающих оплату наркотика);

- изъятие электронных носителей, содержащих сведения, не представляющие интерес с точки зрения их копирования (пустой (новый) электронный носитель, телевизоры со встроенным жёстким диском, автомобили с бортовым компьютером и др.);

- изъятие электронных носителей, содержащих сведения, полномочиями на хранение и использование которых владелец электронного носителя информации не обладает, либо которая может быть использована для совершения новых преступлений (изначально предполагается основание для отказа в копировании, не связанное с участием специалиста).

Приведенная логика рассуждений позволяет также предложить критерий для оценки уровня специальных знаний привлекаемого специалиста: их должно быть достаточно для производства безопасного копирования с одного электронного носителя на другой, а также для оценки потенциальных рисков утраты или изменения информации в результате такого копирования.

Таким образом, вопреки распространенному мнению, даже очень простое с технической стороны изъятие электронного носителя, предполагающее необходимость копирования информации для её обладателя, при отсутствии специалиста должно повлечь недопустимость полученных доказательств. Напротив, произведенное без специалиста технически сложное изъятие, потенциально не вызывающее необходимости копирования, не должно признаваться существенным нарушением порядка производства следственного действия.

В подтверждение сказанного предлагаем обратиться к ч. 3 ст. 164.1 УПК РФ, из содержания которой следует, что в случае, когда в ходе следственного действия осуществляется копирование без изъятия электронного носителя информации, оно осуществляется следователем самостоятельно. То есть, несмотря на вероятную сложность такого копирования, вопрос о предоставлении копии владельцу или обладателю здесь не возникает (сам электронный носитель остается в их распоряжении), в связи с чем участие специалиста не обязательно.

2. Предоставление законному владельцу изымаемых электронных носителей информации или обладателю содержащейся на них информации права ходатайствовать об изготовлении копий с изымаемых электронных носителей информации и получить такие копии.

Право заявлять ходатайства является общим правом участников уголовного процесса, а также иных лиц, права и законные интересы которых затронуты в ходе досудебного производства (ч. 1 ст. 119 УПК РФ), и первый вопрос, который возникает в связи с этим: обязан ли следователь

(дознаватель) отдельно разъяснить право на копирование информации с изымаемых электронных носителей? Полагаем, что на этот вопрос необходимо ответить положительно, так как ч. 1 ст. 11 УПК РФ прямо указывает на необходимость разъяснять участникам уголовного судопроизводства их права, обязанности и ответственность, а также обеспечивать возможность осуществления этих прав.

Далее нужно обратить внимание на субъекта, наделенного таким правом. Согласно ч. 2 ст. 164.1 УПК РФ к таковым относятся законный владелец изымаемых электронных носителей информации или обладатель содержащейся на них информации[1]. Полагаем, что лицом, заявляющим такое ходатайство, могут быть также и представители (законные представители, защитник, адвокат).

Получив ходатайство о выдаче копии, в первую очередь необходимо внести его в протокол следственного действия, после чего в соответствии со ст. 121 УПК РФ следователь обязан принять решение, при этом правило о фиксации хода и результатов копирования в протоколе следственного действия указывает на то, что поступившее ходатайство должно быть разрешено до окончания следственного действия.

Законом предусмотрены основания для отказа в копировании, причем они отсылают нас к одной из групп случаев, допускающих изъятие электронных носителей по преступлениям экономической направленности, а именно:

- на электронных носителях информации содержится информация, полномочиями на хранение и использование которой владелец электронного носителя информации не обладает;

[1] Согласно п.5 ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» обладатель информации это лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам // СПС КонсультантПлюс.

- информация может быть использована для совершения новых преступлений;

- копирование информации, по заявлению специалиста, может повлечь ее утрату или изменение.

Первые два случая уже были предметом нашего внимания и дополнительных пояснений не требуют, в отличие от третьего. Как было указано выше, в контексте возможности изъятия электронного носителя по отдельным экономическим преступлениям специалист оценивает риск утраты или изменения информации при её копировании с первоисточника (электронного носителя) на электронные носители, подготовленные следователем (дознавателем). А при оценке наличия оснований для отказа в копировании та же норма трактуется по-другому, специалисту необходимо оценить риски копирования информации опять же с первоисточника, но уже на электронные носители, представленные лицом, заявившим ходатайство о копировании. С учетом этого обстоятельства при использовании для копирования стороннего электронного носителя вероятность утраты или изменения исходной информации существенно повышается. Стоит отметить, что относительную безопасность копирования может обеспечить порядок, при котором информация сначала копируется с изымаемого носителя на электронный носитель следователя (дознавателя), а затем уже с него – на носитель, представленный законным владельцем или обладателем.

В любом случае при отказе в удовлетворении ходатайства о копировании в протоколе делается соответствующе отметка (а в случае, если имеет место заявление специалиста – оно также заносится в протокол), после чего с целью обеспечить выполнение требований ч. 4 ст. 7 УПК РФ, а также права на обжалование принятого решения (ч. 1 ст. 19 УПК РФ) после окончания следственного действия в разумные сроки необходимо вынести постановление об отказе в удовлетворении ходатайства с доведением его до сведения заявителя (ст. 122 УПК РФ).

В случае, если ходатайство о копировании информации с изъятых электронных носителей будет заявлено после окончания следственного действия, оно подлежит рассмотрению в порядке ч. 2.1 ст. 82 УПК РФ (копирование с электронных носителей, признанных вещественными доказательствами).

3. Специальные правила, регламентирующие порядок копирования информации с изымаемого электронного носителя информации при производстве следственного действия.

При отсутствии оснований для отказа в копировании специалистом по решению следователя (дознавателя) производится копирование информации, с детальным отражением процедуры в протоколе следственного действия. Как было указано выше, копирование производится на электронный носитель, представленный законным владельцем или обладателем информации, однако в условиях проведения обыска могут быть изъяты все находящиеся в помещении и при лице электронные носители. Полагаем, что в такой ситуации следователь также вправе отказать в удовлетворении ходатайства о копировании, при этом признаем, что это мнение не бесспорно.

Особое внимание необходимо обратить на то, что изготовление копии информации, содержащейся на изымаемых электронных носителях, осуществляется в присутствии понятых. Интересно отметить, что относительно вопроса об обязательном участии понятых в законе имеется технический недочет. Так, ч. 1 ст. 170 УПК РФ, перечисляя случаи, когда понятые обязательны, упоминает ч. 3.1 ст. 183 УПК РФ (в которой ранее речь шла об изъятии электронных носителей информации). Вместе с тем, как было указано выше, эта норма утратила силу, а ст. 164.1 УПК РФ говорит об обязательном участии понятых при копировании информации с изымаемых носителей. Соответственно, в случае если ходатайство о копировании не заявлялось или в его удовлетворении было отказано, следственное действие может быть произведено без участия понятых (за исключением обыска и личного обыска, при проведении которых участие понятых обязательно по

общему правилу). Так, выемка электронного носителя допустима с применением технических средств фиксации, однако в случае удовлетворения ходатайства о копировании информации с такого носителя в обязательном порядке должны быть привлечены понятые.

Таким образом, в части изъятия интернет-переписки, содержащейся на электронных носителях информации, вынуждены с сожалением констатировать, что положения закона не исключают проблем, которые правоприменитель вынужден разрешать самостоятельно с учетом позиции надзирающего прокурора и складывающейся судебной практики.

Также существенные затруднения возникают в случаях, когда переписка хранится на удаленных серверах сети Интернет.

Анализ материалов следственной и судебной практики позволяет выделить несколько вариантов проводимых следственных действии. Первый заключается в том, что следователь получает судебное решение о наложении ареста на почтово-телеграфные отправления (ст. 185 УПК РФ), их осмотр и выемку в учреждениях связи, после чего производит выемку переписки у оператора связи (на электронном носителе либо в виде распечатанного текста) и её осмотр. Нам такой вариант представляется не приемлемым, поскольку, во-первых, данное следственное действие направлено на ознакомление с бандеролями, посылками, другими почтово-телеграфными отправлениями либо телеграммами или радиограммами, то есть с корреспонденцией, предусмотренной Федеральным законом «О почтовой связи» № 176-ФЗ от 17.07.1999 г., соответственно интернет-переписка вне зависимости от места её хранения к предмету регулирования ст. 185 УПК РФ не относится. Во-вторых, данное следственное действие подразумевает «задержание» отправления до получения адресатом, тогда как в большинстве случаев следствие интересует уже полученная адресатом интернет-переписка за предшествующий период.

Стоит отметить, что изменениями от 06.07.2016 года (Федеральный закон №375-ФЗ) рассматриваемая статья была дополнена частью 7

следующего содержания «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», однако в силу приведенных доводов, полагаем, что включение электронных сообщений в предмет регулирования ст. 185 УПК РФ является не корректным и не позволяет сделать правильный выбор следственного действия в рассматриваемом случае, что отмечается многими авторами[1].

Достаточно распространены случаи получения интернет-переписки в ходе выемки предметов и документов, содержащих охраняемую федеральным законом тайну, которая производится непосредственно у представителя оператора связи, на основании полученного следователем судебного решения. С учетом положений ст. 13 и п.7 ч.2 ст. 29 УПК РФ данный подход можно признать в полной мере законным и обоснованным, однако с учетом далекого расположения организаций, владеющих серверами крупных социальных сетей и других коммуникационных сервисов (г. Москва, г. Санкт-Петербург), производство таких выемок для следователей Красноярского края становится достаточно затратным как по времени, так и по средствам реализации, а в случае нахождения сервера за пределами Российской Федерации (электронные почтовые ящики вида @gmail.com, @google.com, @hotmail.com, социальная сеть facebook) – практически невозможным.

Одним из вариантов дистанционной фиксации интернет-переписки является её осмотр путем введения адреса и пароля с последующей

[1] 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 Омской юридической академии 2017 Том 14 №1 С.59-64; Карпов О.В. Проблемы регламентации порядка изъятия информации из социальных сетей в российском уголовном процессе // Политика, государство и право. 2016. № 6 [Электронный ресурс]. URL: http://politika.snauka.ru/2016/06/3923 (дата обращения: 20.12.2017).

фиксацией в протоколе текста переписки. Говоря об осмотре, как о следственном действии необходимо отметить, что ст. 176 УПК РФ предусматривает два наиболее подходящих к нашей ситуации варианта – это осмотр предметов и осмотр документов. Автору встречались примеры осмотра страницы сети Интернет посредством такого следственного действия, как «осмотр предметов», в протоколе которого следователь указывал, что объектом осмотра является компьютер, однако нужно понимать, что компьютер в данном случае выступает лишь используемым техническим средством, и сам осмотр не направлен на установление его свойств, поэтому осмотр предметов в рассматриваемом случае не приемлем.

За неимением ничего более подходящего, мы предлагаем использовать в подобных случаях осмотр документа (электронного), поскольку любой интернет-сайт, в том числе содержащий какую-либо переписку, может быть отнесен к электронному документу. Данная позиция косвенно подтверждается положениями Федерального закона «Об информации, информационных технологиях и защите информации» №149-ФЗ от 27.07.2006 г.[1] Авторы неоднократно принимали участие в составлении протоколов осмотра электронного документа, например, с фиксацией содержания созданного мошенниками интернет-сайта, рекламирующего услуги регистрации по месту жительства, выдачу разрешений на работу и т.д., этим же следственным действием был оформлен осмотр содержания профиля одного из преступников в социальной сети «ВКонтакте» (в показаниях он категорически отрицал факт знакомства с соучастником, однако последний довольно долго состоял у него в друзьях).

[1] Согласно указанному закону под электронным документом необходимо понимать: «документированную информацию, представленную в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин...». В свою очередь под документированной информацией понимается «зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель. Требуемыми реквизитами на наш взгляд вполне может выступать всегда оригинальный электронный адрес любой интернет-страницы.

Не редки случаи, когда интернет-переписка фиксируется в ходе проверки показаний на месте. Опуская некоторое терминологическое несоответствие (местом, где будут проверяться показания, по сути будет выступать интернет-пространство), полагаем такой вариант также приемлемым, однако с учетом целей и характера данного следственного действия считаем, что его производство целесообразно в ситуации, когда показания лица о переписке носят фрагментарный характер, точное содержание и местоположение этой переписки точно указать он не может, следовательно сопутствующей целью ознакомления с перепиской является получение новых сведений или уточнение данных им показаний.

Встречаются случаи процессуального закрепления интернет-переписки при проведении следственного эксперимента, в ходе которого лицо, чья переписка представляет интерес, самостоятельно заходит на соответствующий ресурс сети Интернет и, открывая входящие и исходящие сообщения, позволяет следователю зафиксировать в протоколе их содержание. Стоит отметить, что данный подход не лишен логики, поскольку результат совершаемых действий заранее не известен (страница сети Интернет может быть удалена, изменена и т.д.). А цели в общем соответствуют заявленным в ст. 181 УПК РФ (проверяется возможность восприятия каких-либо фактов, совершения определенных действий, наступления какого-либо события, а также выявляются последовательность происшедшего события и механизм образования следов), однако в контексте нашего исследования, можно утверждать, что следственный эксперимент должен проводиться для проверки навыков лица, в случаях, когда возникает сомнение в его возможности осуществить определенные операции в сети Интернет. Дополнительным аргументом может служить тот факт, что открытие профиля социальной сети или электронной почты на сегодняшний день нельзя отнести к действиям, имеющим сложную познавательную структуру, что является одним из критериев отграничения следственного

эксперимента от осмотра[1]. То есть непосредственно для фиксации содержания интернет-переписки на наш взгляд данное следственное действие не подходит.

3.2 Обоснование проблемы определения необходимости получения судебного решения для получения интернет-переписки

Определившись с правилами изъятия интернет-переписки, а также с выбором следственного действия, необходимо отдельно рассмотреть проблему, связанную с ограничением тайны связи[2], которая сопутствует рассматриваемым следственным действиям. Для этого, в первую очередь нужно ответить на два вопроса: 1) относятся ли сведения о переписке, сохранившиеся на техническом устройстве коммуникации к какому-либо виду охраняемой законом тайны? 2) если относятся - то к какому из видов тайны.

На первый вопрос, несомненно, следует ответить положительно, так как по содержанию личная переписка отражает частные стороны жизни, при этом механизм передачи рассматриваемых сообщений подразумевает осознание определенной конфиденциальности по отношению к третьим лицам. Разрешение второго вопроса сложнее, поскольку статья 23 Конституции Российской Федерации содержит две части, в первой из которых говорится о тайне частной жизни, личной, семейной тайне, а во второй – о тайне переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений.

Таким образом законодатель разделяет эти виды тайн, указывая, что, что доступ к сведениям о частной жизни, личной и семейной тайне не требует получения судебного решение (в соответствии с ч.3 ст. 55

---

[1] Шейфер С.А. Следственные действия. Основания, процессуальный порядок и доказательственное значение., 2004. С.145

[2] К тайне связи в соответствии с ч.1 ст.63 ФЗ от 07.07.2003 № 126-ФЗ «О связи» относится тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и сетям почтовой связи.

Конституции РФ ограничение прав допускается федеральным законом, в том числе Уголовно-процессуальным кодексом РФ), а ограничение тайны связи, напротив, в обязательном порядке требует решение суда.

Приведем пример судебной практики: из определения Омского областного суда от 24 мая 2012 года следует, что адвокат в интересах подзащитного обратился в суд с жалобой на действия следователя, который без судебного решения осмотрел СМС-сообщения, телефонные соединения, контакты и т.д. Суд, разрешая данную жалобу, признал в действиях следователя нарушение ч.1 ст. 13 УПК РФ и ч. 2 ст. 23 Конституции Российской Федерации. Суд указал, что информация о факте и содержании переписки, хранящаяся в мобильном телефоне относятся к тайне переписки, так как «имеет двусторонний характер и содержит мысли не только потерпевшего, но и других лиц, пусть и имеющих отношение к делу, но вообще никак не уведомленных о том, что их личная переписка будет достоянием органов предварительного следствия…при осмотре мобильного телефона следователем подвергались тщательному описанию все соединения между абонентами, вплоть до указания времени соединений, номеров телефонов и имен лиц, которые этими телефонами пользуются. Между тем статья 186.1 УПК РФ предусматривает необходимость судебного разрешения на получение информации о соединениях между абонентами». Используя приведенные доводы, суд признал действия следователя незаконными.

На наш взгляд, в данном случае суд необоснованно отнес сведения, хранящиеся в памяти мобильного телефона к тайне связи. Ведь если следовать этой логике, то у следователей возникает обязанность получать судебное решение при ознакомлении с содержанием любой переписки, сохранившейся в памяти компьютера, планшета и т.д.

В качестве единственного критерия отнесения данных сведений к тайне связи суд принял содержание переписки, но в таком случае по аналогии необходимо получать судебное решение на осмотр полученного ранее по почте и изъятого в ходе расследования письма, либо распечаток интернет-

переписки. Ошибочность применённого судьей подхода подтверждается другими примерами судебной практики[1].

Первым критерием отграничения данных видов тайн действительно выступает их форма и содержание, поскольку сведения служебного характера, как и другие, не отражающие частные стороны жизни человека, к рассматриваемым видам тайн не относятся, однако в связи с тем, что без ознакомления с перепиской мы не можем определить ее характер, следователю следует исходить из того, в чьем распоряжении она находится. Переписка, которая ведется с использованием служебных аккаунтов (представленных работодателем), может располагаться на серверах разных операторов (работодатель самостоятельно решает, какой из сервисов для этого использовать, но наиболее распространенными являются такие почтовые сервисы, как Mail.ru, Gmail, Yahoo messenger, Яндекс.Почта и др.), при этом работодатель имеет право на получение и использование данной переписки в полном объеме, поскольку эти данные не относятся к тайне связи[2]. Однако ограничиваться этим было бы неправильным.

Следующим обязательным критерием выступает нахождение интересующей следствие переписки в ведении оператора связи. Для подтверждения состоятельности данного критерия нужно обратиться к разъяснениям Конституционного Суда Российской Федерации, так как на уровне федеральных законов вопрос разграничения тайны связи от иных видов тайны не урегулирован. Тарасов Н.А. обратился с жалобой в Конституционный Суд РФ, посчитав, что положения УПК РФ, позволяющие без вынесения судебного решения осматривать содержание электронной памяти изъятых мобильных телефонов противоречат Конституции РФ. В своем определении от 8 апреля 2010 года № 433-О-О Конституционный суд

[1] Апелляционное постановление Приморского краевого суда от 02.02.2015 года по делу № 22-455/15 URL: https://rospravosudie.com/court-primorskij-kraevoj-sud-primorskij-kraj-s/act-469764857/ (дата обращения: 20.12.2017).

[2] Постановление ЕСПЧ от 12.01.2016 по делу «Барбулеску (Bărbulescu) против Румынии» (жалоба № 61496/08) URL: http://hudoc.echr.coe.int/rus?i=001-159906 (дата обращения: 20.12.2017).

указал, что получение судебного решение на ограничение тайны связи необходимо только при истребовании информации, находящейся в ведении операторов связи. Кроме того, в определении от 2 октября 2003 года №345-О Конституционный Суд РФ, толкуя ч.2 ст. 23 Конституции отмечает, что «право каждого на тайну телефонных переговоров в своем конституционно-правовом смысле предполагает комплекс действий по защите информации, получаемой по каналам телефонной связи, независимо от времени поступления, степени полноты и содержания сведений, фиксируемых на отдельных этапах её осуществления».

Кроме того, тайна связи, включающая в себя тайну переписки, телефонных и иных переговоров регламентирована положениями Федерального закона от 07.07.2003 № 126-ФЗ «О связи». Часть 2 ст. 63 указанного федерального закона говорит о том, что обязанность по соблюдению тайны связи возлагается на операторов связи, то есть никто кроме оператора связи не имеет возможности обеспечить сохранность соответствующих сведений.

Однако окончательно данный вопрос был разрешен в решении Конституционного Суда РФ от 25 января 2018 г. N 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 решении суд констатирует, что проведение осмотра и экспертизы (как и других следственных действий) 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.

Таким образом интернет-переписка, как и любые другие данные будут защищаться тайной связи с момента их отправления до момента получения адресатом. Любые сообщения, еще не отправленные, либо уже полученные и

сохранившиеся на каких-либо устройствах пользователей могут быть отнесены к иным видам тайны (личная, частной жизни, семейная и т.д.), и соответственно получение судебного решения для ознакомления с ними не требуется.

В связи с изложенным, можно констатировать, что интернет-переписка, сохранившаяся на электронных носителях пользователя ни при каких обстоятельствах не может быть отнесена к тайне связи и процессуальное ознакомление с ними получения судебного решения не требует (независимо от выбранного следственного действия), в случае же выхода в ходе осмотра телефона или другого устройства в сеть Интернет и просмотра переписки (например, в социальных сетях, электронной почты) определяющим становится следующий критерий - наличие или отсутствие согласия абонента.

При наличии такого согласия, выраженного в форме заявления или отметки в протоколе, получать судебное решение необходимости нет, при отсутствии – решение суда обязательно. Решение вопроса о допустимости ознакомления с интернет-перепиской при наличии согласия лица зависит от признания права на тайну связи в полной мере неотчуждаемым (как право на неприкосновенность жилища при производстве обыска в жилище), либо допускающим ограничение с согласия правообладателя (как в случае производства осмотра жилища). В то же время, ч. 2 ст. 17 Конституции РФ предусматривает, что основные права и свободы (в том числе право на тайну связи) не отчуждаемы и принадлежат человеку от рождения, однако это право является субъективным, что означает возможность человека самостоятельно выбирать вид и меру своего поведения[1], а также свободу поведения и поступков в границах, установленных нормой права[2]. Исходя из такой трактовки, любой человек может самостоятельно распоряжаться своим

[1] Невирко Д.Д. Права и свободы человека и гражданина: проблемы соотношения, взаимодействия и иерархии : монография. Красноярск, 2006 С. 22.

[2] Строгович М.С. Проблемы советского социалистического государства в современный период. Некоторые теоретические вопросы. М., 1967. С. 170.

правом; соответственно, в ситуации, когда ознакомление с интернет-перепиской осуществляется с согласия пользователя, ограничение его права на тайну связи не происходит, а значит, судебного санкционирования такие действия не требуют. При наличии такого согласия, исходя из удостоверительного характера доказывания, оно должно быть оформлено письменно и с участием защитника (для подозреваемого, обвиняемого).

Дополнительным аргументом может служить тот факт, что положения ч.2 ст. 186 УПК РФ указывают на возможность производства контроля и записи телефонных переговоров участников при наличии угроз на основании письменного заявления (без получения судебного решения), что косвенно подтверждает возможность правообладателя частично распоряжаться своим правом на тайну связи. При рассмотренном подходе решение суда может потребоваться только при отсутствии согласия правообладателя.

Предлагаемая позиция может вызвать вопрос: требуется ли помимо согласия получателя, выяснять позицию отправителя того или иного сообщения? Полагаем, что ответ на этот вопрос должен быть отрицательным, поскольку, во-первых, направляя кому-либо письмо (сообщение) лицо передает получателю право законно распорядиться этими сведениями (законность выдачи сведений следователю не вызывает сомнения), а во-вторых, сохранность этих сведений и интересы отправителя будут обеспечены за счет положений ст. 161 УПК РФ – недопустимость разглашения данных предварительного расследования.

С учетом специфики заявленной темы, мы намеренно не касаемся средств оперативно-розыскной деятельности, которые также очень активно используются в данной сфере, но при их применении следует помнить, что Конституционный Суд РФ в рамках возбужденного уголовного дела запрещает подмену оперативно-розыскными мероприятиями процессуальных

действий, для осуществления которых уголовно-процессуальным законом установлена специальная процедура[1].

В итоге, приведенные доводы, позволяют предложить следующий обобщенный алгоритм определения процессуального порядка получения и фиксации интернет-переписки: 1) выбор надлежащего следственного действия (по приведённым критериям); 2) определение порядка изъятия (получения) сведений, имеющих доказательственное значение 3) определение необходимости получения судебного решения (критерии также были приведены).

[1] Определение Конституционного Суда РФ от 25.02.2010 № 261-О-О // СПС КонсультантПлюс.

4 Оценка результатов исследования

В рамках предмета исследования автором всесторонне изучены проблемы, связанные с получением и использованием в доказывании интернет-переписки.

Поставленные перед исследованием задачи решены в полном объеме, дополнительные исследования могут касаться лишь вопросов использования в доказывании сведений из облачных хранилищ данных. Выводы, сделанные автором достоверны, основываются на методологии и доктринальных положениях науки уголовного процесса. Основные положения базируются на результатах анализа действующего законодательства, а также правоприменительной практики.

Полученные по итогам исследования результаты составили основу научной продукции в виде методических рекомендаций. Представленные материалы могут быть использованы в практической деятельности следственных подразделений, учебном процессе, а также для дальнейшего научного анализа и проведения диссертационного исследования.

ЗАКЛЮЧЕНИЕ

Комплексный анализ проблем, связанных с получением и использованием в доказывании интернет-переписки по делам о преступлениях в сфере незаконного оборота наркотиков, позволил выработать и сформулировать ряд подходов и предложении, нашедших отражение в подготовленных методических рекомендациях. Следование данным рекомендациям позволит минимизировать негативные последствия нарушений закона при собирании и проверке доказательств.

В работе рассмотрены вопросы:

- о проблеме выбора надлежащего следственного действия для получения интернет-переписки;

- о порядке получения интернет-переписки, расположенной на электронных носителях информации;

- о проблеме определения необходимости получения судебного решения для получения интернет-переписки;

- о порядке действий и особенностях принятия отдельных решений, связанных с получением интернет-переписки в различных исходных ситуациях;

Имеются основания полагать, что материалы указанной работы будут с интересом восприняты как практиками, так и обучающимися, что повысит их готовность к предстоящему выполнению своих профессиональных обязанностей.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

Международные нормативные правовые акты[1]

Нормативные акты:

1. Конституция Российской Федерации: принята всенародным голосованием 12.12.1993.

2. Уголовный кодекс Российской Федерации: Федеральный закон от 13.06.1996 № 63-ФЗ.

3. Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон от 18.12.2001 № 174-ФЗ.

4. Федеральный закон от 17.04.2017 № 73-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации» // «Российская газета», № 83. 19.04.2017.

5. Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» // СПС КонсультантПлюс.

6. Об утверждении перечня наркотических средств, психотропных веществ и их прекурсоров, подлежащих контролю в Российской Федерации: постановление Правительства Российской Федерации от 30.06.1998 № 681 (ред. от 18.01.2017) // Собрание законодательства РФ. – 1998. – № 27. – Ст. 3198.

7. Об утверждении значительного, крупного и особо крупного размеров наркотических средств и психотропных веществ, а также значительного, крупного и особо крупного размеров для растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества, для целей статей 228, 228.1, 229 и 229.1 Уголовного кодекса Российской Федерации : постановление Правительства Российской Федерации от 1

[1] Для поиска документов, входящих в раздел «Международные нормативные правовые акты», использована СПС КонсультантПлюс.

октября 2012 г. № 1002 (ред. от 18.01.2017) // Собрание законодательства РФ. – 2012. – № 41. – Ст. 5624.

Учебники и учебные пособия:

8. Долгиева М.М. Операции с криптовалютами : актуальные проблемы теории и практики применения уголовного законодательства / М.М. Долгиева // Актуальные проблемы российского права. – 2019. – № 4. – С. 128-139.

9. Дремлюга Р.И. Незаконный оборот наркотиков и крипторынки : угрозы и вызовы правоохранителю / Р.И. Дремлюга // Наркоконтроль. – 2018. – № 2. – С. 33-38.

10. Енаева Л. К. Уголовный процесс6 учебное пособие. 2-е изд. М.: ФОРУМ: ИНФРА-М, 2007.

11. Жарова А.И. Риски информационной безопасности правового регулирования криптовалюты в России // Информационное право. – 2018. – № 4. – С. 11-16;

12. Карпов О.В. Проблемы регламентации порядка изъятия информации из социальных сетей в российском уголовном процессе // Политика, государство и право. 2016. № 6 [Электронный ресурс]. URL: http://politika.snauka.ru/2016/06/3923 (дата обращения: 20.12.2017).

13. Леонов А.И. Некоторые проблемы расследования преступлений, связанных с легализацией денежных средств, приобретенных в результате незаконного сбыта наркотических средств / А.И. Леонов, А.В. Беденко, Ю.О. Волокитина // Вестник Воронежского института МВД России. – 2020 – №1. – С. 248-254.

14. Невирко Д.Д. Права и свободы человека и гражданина: проблемы соотношения, взаимодействия и иерархии : монография. Красноярск, 2006 С. 22.

15. Строгович М.С. Проблемы советского социалистического государства в современный период. Некоторые теоретические вопросы. М.,

1967. С. 170.

16. 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 Омской юридической академии 2017 Том 14 №1 С.59-64;

17. Шейфер С.А. Следственные действия. Основания, процессуальный порядок и доказательственное значение, 2004. С.145.