

Список литературы

1. Апостолова Н. Н. Искусственный интеллект в судопроизводстве // Северо-Кавказский юридический вестник. 2019. № 3. С. 135–141.
2. Буряков П. Н. Искусственный интеллект и «предсказуемое правосудие»: зарубежный опыт // Lex russica. 2019. № 11. С. 79–87.
3. Колоколов Н. А. Компьютер вместо судьи – арифметика вместо души // Уголовное судопроизводство. 2019. № 3. С. 3–7.
4. Попова И. П. Автоматизация уголовного процесса: зло или благо для общества? // Мировой судья. 2019. № 11. С. 3–14.
5. Сушина Т. Е, Собенин А. А. Перспективы и риски использования искусственного интеллекта в уголовном судопроизводстве // Российский следователь. 2020. № 6. С. 15–21.
6. Черниговская Т. М. Цифровизация и человечность // Global Woman Media. 2020. URL: <http://eawfpress.ru/presstsentr/news/glav/nauka/tatyana-chernigovskaya-tsifrovizatsiya-i-chelovechnost/> (дата обращения: 17.09.2022).
7. Kehl D., Kessler S. Algorithms in the criminal justice system: Assessing the use of risk assessments in sentencing. URL: <http://nrs.harvard.edu/urn-3:HUL.InstRepos:33746041> (дата обращения: 17.09.2022).
8. Polloni C. Police prédictive: la tentation de ‘dire quel sera le crime de demain’. 2015. URL: [https://www.nouvelobs.com/rue89/rue89-police-justice/20150527.RUE 9213/police-predictive-la-tentation-de-dire-quel-sera-le-crime-de-demain.html](https://www.nouvelobs.com/rue89/rue89-police-justice/20150527.RUE%209213/police-predictive-la-tentation-de-dire-quel-sera-le-crime-de-demain.html)
9. Щелконогова Е. В. Цифровые технологии и уголовное право: вопросы взаимодействия // Вестник Югорского государственного университета. 2021. Вып. 1 (60). С. 105–110.

Н. В. Бушная,

кандидат юридических наук, заведующий кафедрой
общегуманитарных и юридических дисциплин,

Ставропольский филиал

Московского педагогического государственного университета

В. В. Кудинов,

кандидат педагогических наук, доцент,

Ставропольский филиал

Московского педагогического государственного университета

РИТОРИКА ЗАКОНОДАТЕЛЯ В ВОПРОСЕ ИЗЪЯТИЯ ЭЛЕКТРОННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ И КОПИРОВАНИЯ С НИХ ИНФОРМАЦИИ ПРИ ПРОИЗВОДСТВЕ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ

Аннотация. Электронные носители информации, их изъятие и копирование с них сведений, имеющих непосредственное значение для расследования преступлений, являются лакмусом современных тенденций цифровизации, масштабного

использования IT-технологий в различных сферах, в том числе лицами, совершающими общественно опасные деяния с использованием указанных технологий. В статье анализируется взгляд законодателя в вопросе механизма приобщения электронных носителей информации, имеющей непосредственное отношение к расследованию преступления, результаты восприятия нововведений правоприменительной практикой, нуждаемость положений закона в совершенствовании.

Ключевые слова: информационное общество, электронный носитель информации, изъятие электронных носителей информации, копирование информации, цифровизация, доказательственное значение, использование специальных знаний, участие специалиста

THE RHETORIC OF THE LEGISLATOR ON THE ISSUE OF THE SEIZURE OF ELECTRONIC MEDIA AND COPYING INFORMATION FROM THEM DURING INVESTIGATIVE ACTIONS

Abstract. Electronic media, their seizure and copying of information directly relevant to the investigation of crimes from them are a litmus of modern trends in digitalization, large-scale use of IT technologies in various fields, including by persons committing socially dangerous acts using these technologies. The article analyzes the legislator's view on the issue of the mechanism of introducing electronic media directly related to the investigation of a crime, the results of the perception of innovations by law enforcement practice, the need for improvement of the provisions of the law.

Keywords: Information society, Electronic media, Seizure of electronic media, Copying of information, Digitalization, Evidentiary value, Use of special knowledge, Participation of a specialist

Информационное общество, цифровизация, информационные технологии – символы современного мирового и российского поступательного развития в сторону технического прогресса, направленного на взаимодействие общества и государства посредством технологий беспроводной передачи информации, искусственного интеллекта, возможности использования электронных платежных систем. Современные технологии буквально проникли в каждую сферу жизни общества, взаимодействия населения с органами власти, оказывая важное, а порой, решающее воздействие при принятии тех или иных решений в повседневной жизни и профессиональных областях [1. Р. 2517]. Правовая сфера в этом вопросе не является исключением. Одной из тенденций цифровизации юридической деятельности является появление смарт-контракта, основанного на технологии блочных цепей (блокчейн), использование информационных технологий в различных видах судопроизводства, в том числе уголовно-процессуального.

Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы определяет основные ориентиры в механизме формирования общества знаний, возврата от так называемого клипового мышления к научному, образовательному уровню восприятия окружающего мира [12].

Отдельные из принципов указанного нормативного акта коррелируются со смысловым наполнением, сутью уголовного судопроизводства и выражаются

в обеспечении требований законности и разумности при проведении всех действий, связанных с получением информации о физических и юридических субъектах; гарантированности со стороны государства защищенности интересов российских граждан в информационной сфере.

Обеспечение национальных интересов, стратегических национальных ориентиров в развитии информационного общества корреспондируют международно-правовым актам, в частности, Окинавской хартии Глобального информационного общества, ставящей ИТ-технологии определяющим фактором формирования и развития общества двадцать первого века [10].

Цифровизация всех сфер жизнедеятельности общества и государства, необходимость использования цифровых ресурсов в праве, рост киберпреступности, сохранение важной для расследования преступлений информации на электронных носителях вынуждают законодателя на ответную реакцию в виде новелл, регламентирующих информационно-цифровую составляющую уголовного судопроизводства. Неизменным остается постулат о необходимости создания действенной системы гарантий прав участников уголовного судопроизводства по всевозможным вопросам, связанным с ИТ-технологиями.

Федеральный закон от 27.12.2018 № 533-ФЗ [5] видоизменил механизм нормативного регулирования в вопросах появления и использования в производстве по уголовным делам сведений, полученных с электронных носителей, добавив в ст. 164 УПК РФ ч. 4.1, а также введя новую норму 164.1. При этом из ст. 182 и 183 УПК РФ, регламентирующих, соответственно, производство обыска и выемки, были исключены части, содержавшие нормативные руководства по изъятию электронных средств и копированию с них информации.

Ключевым при анализе и толковании новелльных установлений является термин «электронный носитель информации». И здесь возникают определенные трудности ввиду отсутствия в уголовно-процессуальном законе легального определения, значимого именно для понимания такого объекта как составного компонента системы доказательств. Безосновательно было бы утверждать, что российское законодательство и система национальных стандартов не содержат каких-либо терминов, имеющих отношение к рассматриваемому вопросу. Например, УК РФ дает понятие компьютерной информации, Национальный стандарт РФ ГОСТ Р 7.0.8–2013 «Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения» [11] так же, как и Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [7], обращаются к категории «электронный документ». Однако интересующий нас термин содержит только ГОСТ 2.051–2013 «Единая система конструкторской документации (ЕСКД). Электронные документы. Общие положения (с Поправкой)» [3], представляя его как материальный носитель, используемый для записи, хранения и воспроизведения информации, обрабатываемой с помощью средств вычислительной техники. Такая дефиниция перечисляет общие свойства без относительно и применительно к сфере уголовного судопроизводства, уделяющей особое внимание вопросам допустимости доказательств. Такая правовая неопределенность, в конечном итоге, может сказываться на результатах расследования и формировании доказательственной базы при расследовании преступлений.

Законодателю следует сосредоточить внимание на данном вопросе, что позволит исключить в правоприменительной практике возникновение ситуаций, нивелирующих результаты доказательственной деятельности следователей, дознавателей. Здесь следует согласиться с одной из точек зрения, делающей акцент на ключевое в содержании разрабатываемого понятия, а именно, на значимость получаемой информации для формирования доказательственной базы, а не на технические характеристики [4. С. 40].

Указанные выше нововведения сделали акцент на деяниях, затрагивающих предпринимательство. Предпринимательская деятельность является важным компонентом реализуемой национальной политики в силу значимости возлагаемых функции. Стратегия развития малого и среднего предпринимательства в Российской Федерации на период до 2030 г. [9] определяет функционал предпринимательства, имеющего целеназначением развитие интеллектуальной экономики, улучшение ее отраслевой структуры, обеспечение высоких показателей занятости населения.

Придавая особую значимость сфере предпринимательства, законодатель закрепляет гарантии защищенности от неправомерных действий должностных лиц в рамках уголовно-процессуальной деятельности, в частности, ч. 4.1. ст. 164 УПК РФ, закрепляет правило, запрещающее изъятие электронных средств без достаточных на то оснований. В следующей статье законодатель не забывает упомянуть об исключительных обстоятельствах. Речь идет о постановлении о назначении судебной экспертизы в отношении указанных объектов либо вынесенном судебном решении, предполагающим производство анализируемого процессуального действия.

Конструктивно непросто видится третье исключение в силу концентрации сразу нескольких исключаяющих возможности изъятия указанных носителей информации: их владелец не уполномочен на хранение и использование информации либо имеется альтернатива для ее использования в преступных целях или возможны утрата, изменение имеющейся на носителе информации, если будут проведены действия по ее копированию. В последнем утверждении вывод делает не сам следователь, а специалист. С данным суждением следует согласиться, поскольку действительно работа с техническими средствами, электронными носителями информации не проста, а требует специальных знаний, в противном случае, неумение или незнание технически верных действий может привести к утрате доказательственной базы. Правильный подход законодателя к регламентации правил, требований по вовлечению в сферу уголовно-процессуальной деятельности информации с электронных носителей, могущей быть преобразованной в доказательства, напрямую обуславливает качество расследования, решение задач уголовного судопроизводства.

Анализ перечисленных исключений свидетельствует о сложности восприятия для толкования и, самое главное, апробации правоприменителем анализируемых положений. Несомненно, появление таких положений неоднозначно было воспринято учеными-процессуалистами и представителями правоприменительной практики. Например, если речь идет о владельце электронного информационного средства, который не имеет соответствующих полномочий по ее хранению и использованию, то необязательно, с нашей точки зрения, что данные средства находятся у него в силу совершения им противоправных действий. Противоположной точки зрения

придерживается В. Ф. Васюков [2. С. 11], высказывающий именно этот аргумент как ключевой для данного исключения.

Предусмотренный п. 1 ч. 1 ст. 164.1 УПК РФ запрет на изъятие носителей информации электронного формата вызывает сомнение в возможности априори возникновения подобной ситуации.

Проведение любой экспертизы предполагает наличие объектов исследования, а не обратную последовательность, когда следователь выносит постановление, а потом ищет то, что будет исследоваться. Аналогично и в случае электронных доказательств: первично – изъятие носителя информации, вторично – вынесение постановления о назначении экспертизы, т. е. последнее может появиться в рамках уголовного дела уже тогда, когда проведено соответствующее следственное действие и изъят носитель информации, который в дальнейшем может выступать объектом экспертного исследования.

Второе исключение, предусмотренное п. 2 ч. 1 той же нормы уголовно-процессуального закона, вызывает неоднозначное толкование, что напрямую сказывается на формировании правоприменительной практики, демонстрирующей разноплановый подход к восприятию данной нормы. В каких случаях должно быть вынесено судебное решение, на основании которого может быть проведено процессуальное действие, сводящееся к изъятию электронных носителей информации? Решение суда носит «персонифицированный» характер относительно непосредственно носителя информации или касается следственного действия, которое предполагается производить с разрешения суда? Эти и многие другие вопросы, возникающие в уголовно-процессуальной деятельности правоохранительных органов, нередко либо создают препятствия для эффективного производства расследования, либо впоследствии приводят к признанию полученной информации недопустимой. В этом вопросе интересной видится пояснение Конституционного Суда РФ об отсутствии необходимости вынесения отдельного специального судебного решения для производства экспертизы, если изъятие абонентских устройств производилось в соответствии со всеми процессуальными требованиями. Если участники процесса не согласны с какими-то решениями или действиями должностных лиц, они могут их обжаловать в общем порядке, предусмотренном ст. 125 уголовно-процессуального закона [8].

Еще один вопрос, требующий внимания: распространяются ли установленные запреты на доследственную проверку сообщения о преступлении либо приобретают юридическую силу уже в рамках возбужденного уголовного дела? Согласно Постановления Пленума Верховного Суда Российской Федерации от 15 ноября 2016 г. № 48 [6], рассматривая поступившие жалобы на постановление о возбуждении уголовного дела, судом реализуется функция контроля, заключающаяся в проверке законности и обоснованности процессуальных действий, проведенных в ходе проверки сообщения о преступлении, обратив внимание на выполнение всех требований закона по изъятию электронных носителей информации. Такая рекомендация позволяет сделать вывод о возможности производства таких процессуальных действий до начала деятельности в рамках возбужденного уголовного дела и, следовательно, юридической силе установленных запретов на самом первоначальном этапе уголовно-процессуальной деятельности.

Риторика законодателя в отношении электронных носителей информации предполагает две составляющие: изъятие этих самых носителей и копирование с них информации. Изъятие, в свою очередь, требует соблюдение следующих условий: производство обусловленного обстоятельствами уголовного дела следственного действия и участие специалиста. Относительно последнего возникает вопрос: так ли необходимо привлечение сведущего лица в каждом случае проведения указанного процессуального действия? Возможно то, что данная норма является чрезмерной, не требующей привлечения специальных знаний и умений в каждом случае возникновения такой потребности. Считаем, что законодателю следует дополнить уточнением анализируемую норму о привлечении специалиста, когда по мнению следователя этого требует сама ситуация, что будет согласовываться с положениями закона о самостоятельности следователя как лица, ведущего расследование преступления.

Копирование информации представлено в двух вариациях: при изъятии электронного носителя и без такового. В последнем случае следователю предоставлено право самостоятельного копирования информации в ходе следственного действия. Данный случай, на наш взгляд, требует дифференцированного подхода в зависимости от сложности устройства электронного средства, содержащего необходимую информацию, с учетом обязательного исключения, уверенности, что данное действие не несет вреда расследованию. Отталкиваясь от данных факторов, должен решаться вопрос о привлечении лица, сведущего в этом вопросе, что согласуется с п. 3 ч. 1 ст. 164.1 УПК РФ, указывающей на необходимость получения мнения специалиста о запрете изъятия, поскольку это может привести к утрате или изменению интересующих следствие сведений.

Копирование информации, производимое при изъятии электронного носителя, не коррелируется с нормами ч. 2 ст. 82 УПК РФ и содержит противоречия. Указанное положение закона обращает внимание на производство действий по копированию информации локационно, а именно в помещении органа предварительного расследования или в здании суда, тогда как в ч. 2 ст. 164.1 такое уточнение отсутствует. Аналогичное рассогласование встречается и при толковании случаев запрета копирования информации: ч. 2 ст. 164.1 содержит отсылку к п. 3 ч. 1 этой же нормы, тогда как ч. 2.1 ст. 82 УПК РФ указывает на дополнительный запрет копирования сведений, если это будет препятствовать расследованию преступления. Объединяя все перечисленные случаи, получаем расширенную версию запретов копирования информации. Какая норма подлежит применению в данных обстоятельствах: общая или специальная либо следователь должен учитывать все исключения, перечисленные законодателем? Ответ на этот вопрос остается открытым.

Внимание законодателя должен привлечь вопрос о формировании соответствующей нормы с точки зрения конструктивного подхода. Семантика ст. 164.1 УПК РФ была бы более звучной при перестроении ее частей. На наш взгляд, по смыслу содержательной части правильней видится следование от общего к частному: первично описание порядка изъятия электронных носителей информации и копирования с них информации, а затем переход к тем запретам и ограничениям, которые в нынешней редакции содержатся в ч. 1 указанной нормы. При таком изменении ч. 2 и 3 станут, соответственно, 1 и 2, а ч. 1 будет завершать нормативную конструкцию.

Таким образом, пристальный анализ действий законодателя по внедрению регламентации относительно электронных носителей информации свидетельствует о необходимости доработки, модернизации, корректировки действующих положений, приведения ряда статей УПК РФ в соответствие друг с другом для исключения неоднозначной апробации в правоприменительной практике и, напротив, формирования ее единообразия.

Список литературы

1. Васюков В. Ф. Особенности изъятия электронных носителей информации при производстве следственных действий: новеллы законодательства и проблемы правоприменения // Криминалистика: вчера, сегодня, завтра. 2019. № 2. С. 8–14.
2. ГОСТ 2.051–2013 «Единая система конструкторской документации. Электронные документы. Общие положения (Введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 22 ноября 2013 г. № 1628-ст). URL: <https://docs.cntd.ru/document/1200106864?ysclid=l6ukykj7gg126409827>
3. Григорьев В. Н., Максимов О. А. Понятие электронных носителей информации в уголовном судопроизводстве // Вестник Уфимского юридического института МВД России. 2019. № 2 (84). С. 33–44.
4. О внесении изменений в статьи 76.1 и 145.1 Уголовного кодекса Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон от 27 декабря 2018 № 533-ФЗ // Российская газета. 29 декабря 2018. № 295.
5. О практике применения судами законодательства, регламентирующего особенности уголовной ответственности за преступления в сфере предпринимательской и иной экономической деятельности: Постановление Пленума Верховного Суда РФ от 15 ноября 2016 г. № 48 // Российская газета. 24 ноября 2016. № 266.
6. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. № 149-ФЗ // Российская газета. 29 июля 2006. № 165.
7. Об отказе в принятии к рассмотрению жалобы гражданина Прозоровского Д. А. на нарушение его конституционных прав статьями 176, 177 и 195 УПК РФ: Определение Конституционного суда РФ от 25.01.2018 № 189-О. URL: <https://www.ksrf.ru> (дата обращения: 11.08.2022).
8. Об утверждении Стратегии развития малого и среднего предпринимательства в Российской Федерации на период до 2030 года (вместе с «Планом мероприятий («дорожной картой») по реализации Стратегии развития малого и среднего предпринимательства в Российской Федерации на период до 2030 года»): Распоряжение Правительства РФ от 02.06.2016 № 1083-р (ред. от 30.03.2018) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_199462/ (дата обращения: 11.08.2022).
9. Окинавская хартия Глобального информационного общества // Дипломатический вестник. 2000. № 8.
10. Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения: национальный стандарт

РФ ГОСТ Р 7.0.8–2013 (утв. приказом Федерального агентства по техническому регулированию и метрологии от 17 октября 2013 г. № 1185-ст). URL: <https://docs.cntd.ru/document/1200108447?ysclid=l6ukecn684210777985> (дата обращения: 11.08.2022).

11. Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы: Указ Президента РФ от 9 мая 2017 г. № 203 // Собрание законодательства Российской Федерации. 2017. № 20. Ст. 2901.

12. Balashova A. Action Plan For Using Digital Evidences When Investigating Drug Marketing Via The Internet, Instant Messengers And Crypto markets / A. Balashova, V. Vasyukov, O. Efremova, G. Gasparyan // Jour of Adv Research in Dynamical & Control Systems. 2019. Vol. 11. Spesial Issue-08. Pp. 2517–2524.

Ю. В. Быстрова,

доктор юридических наук, доцент,

Орловский государственный университет имени И. С. Тургенева

Е. Е. Быстрова,

студент Банковского колледжа

Среднерусский институт управления, филиал Российской академии народного хозяйства и государственной службы при Президенте РФ

В. С. Изотова,

магистр,

Орловский государственный университет имени И. С. Тургенева

ТАКТИКА ПРОИЗВОДСТВА ВЕРБАЛЬНЫХ И НЕВЕРБАЛЬНЫХ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ ПРИ РАССЛЕДОВАНИИ КИБЕРПРЕСТУПЛЕНИЙ

Аннотация. В статье рассматриваются актуальные проблемы, возникающие при расследовании киберпреступлений. Исследована система средств, с помощью которых совершаются данные виды преступных деяний: электронная почта, файловые архивы, видеоблоги, носители информации (персональные компьютеры, ноутбуки, оптические диски, умные часы, смарт-браслеты, смартфоны и т. д.). Предложено оптимальное сочетание вербальных и невербальных методов, способствующих быстрому раскрытию и расследованию рассматриваемых деяний.

Ключевые слова: компьютерные преступления, киберпреступления, компьютерные средства, компьютерные технологии, вербальные и невербальные следственные действия

TACTICS OF VERBAL AND NON-VERBAL INVESTIGATIVE ACTIONS IN THE INVESTIGATION OF CYBERCRIMES

Abstract. The article discusses the current problems arising in the investigation of cybercrimes. The system of means by which these types of criminal acts are committed is investigated: e-mail, file archives, video blogs, information carriers (personal computers, laptops, optical disks, smart watches, smart bracelets, smartphones, etc.), an optimal combination of verbal and non-verbal methods that contribute to the rapid disclosure and investigation of the acts in question is proposed.