УДК 343.14
ББК Х410.204
DOI: 10.14529/law170105

ЭЛЕКТРОННАЯ ИНФОРМАЦИЯ И ЕЕ НОСИТЕЛИ В УГОЛОВНО-ПРОЦЕССУАЛЬНОМ ДОКАЗЫВАНИИ: РАЗВИТИЕ ПРАВОВОГО РЕГУЛИРОВАНИЯ

С. В. Зуев
Южно-Уральский государственный университет, г. Челябинск

Автор рассматривает развитие российского уголовно-процессуального института по использованию электронной информации и ее носителей в доказывании по уголовным делам. Утверждается, что данный институт берет свое начало с 2010 года, с момента принятия Федерального закона № 143-ФЗ, которым в УПК РФ была внесена ст. 186.1 «Получение информации о соединениях между абонентами и (или) абонентскими устройствами». С этого момента организации, осуществляющие услуги связи, стали предоставлять электронную информацию на различных материальных носителях. Автор обосновывает перспективу развития копирования электронной информации и многие другие вопросы обращения с электронной информацией и ее носителями. Обращается внимание на то, что уголовное судопроизводство должно развиваться с учетом современных информационных телекоммуникационных отношений в обществе.

Ключевые слова: доказывание, уголовный процесс, электронная информация, электронные носители информации.

Анализ действующего российского уголовно-процессуального законодательства позволяет сделать вывод о том, что уголовный процесс медленно, но меняется с учетом развития информационных телекоммуникационных отношений в обществе. Представляется, что история регламентирования вопросов использования электронной информации и ее носителей в уголовно-процессуальном доказывании берет свое начало с принятия Федерального закона от 1 июля 2010 г. № 143-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации». Этим законом в УПК РФ была внесена ст. 186.1. «Получение информации о соединениях между абонентами и (или) абонентскими устройствами». С этого момента организации, осуществляющие услуги связи, при обращении к ним следователя (или дознавателя) в судебном порядке, стали предоставлять соответствующую информацию на различных материальных носителях информации. На практике эти данные в большинстве случаев предоставляются на оптических дисках – CD, DBD, Blu-ray, HVD либо флеш-накопителях [1, с. 69]. Последние стали рассматриваться как доказательства. При этом интересующая органы расследования электронная информация предоставляется в опечатанном виде с сопроводительным письмом, в котором указываются период, за который она предоставлена, и номера абонентов и (или) абонентских устройств.

Эффективность этого следственного действия не вызывает сомнений. В настоящее время использование биллинговой информации позволяет раскрывать различные преступления, в том числе убийства, совершенные в условиях неочевидности [4, с. 8].

28 июля 2012 г. был принят Федеральный закон № 143-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации», который внес ряд процессуально значимых положений в УПК РФ относительно правовой природы электронных носителей информации и определил некоторый порядок обращения с ними. Так, в п. 5 ч. 2 ст. 82 УПК РФ порядок обращения с электронными носителями информации представлен наряду с другими разновидностями вещественных доказательств. Кроме того, в данной статье закреплено, что они хранятся в опечатанном виде в условиях, исключающих возможность ознакомления посторонних лиц с содержащейся на них информацией и обеспечивающих их сохранность и сохранность указанной информации, законному владельцу возвращаются после осмотра и производства других

необходимых следственных действий, если это вообще возможно без ущерба для доказывания по уголовному делу.

Вместе с тем, изъятые в ходе досудебного производства, но не признанные вещественными доказательствами предметы, включая электронные носители информации, и документы подлежали возврату лицам, у которых они были изъяты (ч. 4 ст. 81 УПК РФ).

Тем же законом ч. 2.1 ст. 81 УПК РФ дополнилась новым содержанием, суть которого заключается в том, что после производства неотложных следственных действий в случае изъятия электронных носителей информации и невозможности их возврата законному владельцу содержащаяся на этих носителях информация по ходатайству их законного владельца может быть скопирована.

Следует признать, что копирование электронной информации при производстве по уголовным делам, как правовой институт, пока недостаточно развит в уголовно-процессуальном праве. При этом в настоящее время такое одноименное действие в уголовном процессе осуществляется с участием законного владельца изъятых электронных носителей информации и (или) его представителя и специалиста в присутствии понятых в подразделении органа предварительного расследования или в суде на другие электронные носители информации, предоставленные законным владельцем изъятых электронных носителей информации. При копировании информации должны обеспечиваться условия, исключающие возможность ее утраты или изменения. По всей видимости, на это должны обращать внимание специалист и следователь. Последний может в любой момент приостановить дальнейшее копирование информации. По закону не допускается копирование информации, если это может воспрепятствовать расследованию преступления. Электронные носители информации, содержащие скопированную информацию, передаются законному владельцу изъятых электронных носителей информации. Об осуществлении копирования информации и о передаче электронных носителей информации, содержащих скопированную информацию, законному владельцу изъятых электронных носителей информации составляется протокол в соответствии с требованиями ст. 166 УПК РФ.

Тем же законом № 144-ФЗ от 28 июля 2012 г. было изменено содержание ч. 8 ст. 166 УПК РФ. Согласно ее новой редакции к протоколу должны прилагаться электронные носители информации, которая была получена или скопирована с других электронных носителей информации в ходе производства того или иного следственного действия.

Кроме того, ст. 182 УПК РФ была дополнена частью 9.1. С этого момента закон стал требовать, чтобы при производстве обыска электронные носители информации изымались с участием специалиста. По ходатайству законного владельца изымаемых электронных носителей информации специалистом, участвующим в обыске, в присутствии понятых с изымаемых электронных носителей информации осуществляется копирование информации.

В той же ст. 182 УПК РФ было закреплено, что копирование информации осуществляется на другие электронные носители информации. Такие носители информации предоставляются законным владельцем изымаемых электронных носителей. При производстве обыска не допускается копирование информации, если это может воспрепятствовать расследованию преступления либо, по заявлению специалиста, повлечь за собой утрату или изменение информации. Электронные носители информации, содержащие скопированную информацию, передаются законному владельцу изымаемых электронных носителей информации. Об осуществлении копирования информации и о передаче электронных носителей информации, содержащих скопированную информацию, законному владельцу изымаемых электронных носителей информации в протоколе делается запись.

Аналогичным образом была дополнена ч. 3.1 ст. 183 УПК РФ относительно выемки электронных носителей информации.

Изъятие электронных носителей и копирование электронной информации – это два дополняющих, а в некоторых случаях и конкурирующих между собой познавательных приема по обращению с электронными средствами уголовно-процессуального доказывания. Преимущества того или иного действия зависят от решаемых задач, условий и сложности процесса.

В перспективе копирование электронной информации вполне может рассматриваться в качестве самостоятельного следственного действия. Такое предположение основано на различиях в фактической природе обыска,

выемки, осмотра, с одной стороны, и копирования электронной информации, с другой. В. А. Семенцов, соглашаясь в целом с такой идеей, отметил: «В практике расследования возникает необходимость электронного копирования информации, и этот новый познавательный прием соответствует требованиям закона, морали и социальным закономерностям общественного развития. Необходимо только включить электронное копирование в систему процессуальных действий, предназначенных для собирания доказательств» [3, с. 36].

29 ноября 2012 г. был принят Федеральный закон № 207-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации», в котором в новой редакции была представлена ч. 2.1 ст. 82 УПК РФ. Формулировка «может быть скопирована» была заменена на «копируется», что выглядит более категорично. Кроме того, участвующим и заинтересованным лицом при копировании электронной информации, наряду с владельцем изъятых электронных носителей информации, в статье был указан обладатель содержащейся на них информации. Подобной корреляции подверглись ч. 9.1 ст. 182 и ч. 3.1 ст. 183 УПК РФ.

Тем же законом внесено положение в ст. 15 Федерального закона «Об оперативно-розыскной деятельности», согласно которому в случае, если при проведении гласных оперативно-розыскных мероприятий невозможно изготовить копии документов и (или) скопировать информацию с электронных носителей информации или передать их одновременно с изъятием документов и (или) электронных носителей информации, указанное должностное лицо передает заверенные копии документов и (или) электронные носители информации, содержащие копии изъятой информации, лицу, у которого были изъяты эти документы, и (или) законному владельцу изъятых электронных носителей информации или обладателю содержащейся на них информации в течение пяти дней после изъятия, о чем делается запись в протоколе.

Спорным как в уголовном процессе, так и в сфере оперативно-розыскной деятельности, является вопрос об обязательном участии специалиста во всех безоговорочно действиях (мероприятиях), связанных с изъятием электронных носителей информации. В литературе высказываются разные мнения, практика вырабатывает различные подходы. Суть их заключается в необходимости дифференцированного подхода, который следовало бы закрепить в законе. И с этим можно согласиться. Эффективность, целесообразность и минимизация ущерба для участников – вот основные критерии, которыми должны руководствоваться следователь, дознаватель, а также сотрудник оперативного подразделения.

При этом надо отметить, что в большинстве случаев, как правило, применяется изъятие электронных носителей информации, что вряд ли совпадает с интересами их владельца. Например, изъятию на длительный срок подлежит сам видеорегистратор или его карта памяти.

Так, неизвестный заманил малолетнего ребенка О. в автомобиль и увез в неизвестном направлении. Органы расследования располагали только информацией о промежутке времени совершенного преступления и участке местности. Следователь обратился через СМИ к владельцам автомобилей, оборудованных видеорегистраторами, которые проезжали по дороге в момент похищения ребенка с просьбой предоставить видеозапись. Несколько водителей откликнулись и предоставили видеорегистраторы своих автомашин. В ходе осмотра записей, их сопоставления и анализа был установлен автомобиль преступника, а девочка найдена. Аналогичный прием применялся при расследовании изнасилования и убийства двух студенток в Подмосковье. Видеорегистратор автомобиля одного из водителей зафиксировал автомашину, в которую садились погибшие. В результате удалось установить преступника и раскрыть особо тяжкое преступление [2, с. 6].

Другой пример. По данным МВД России, в феврале 2016 года в станице Ленинградской Краснодарского края сотрудники уголовного розыска совместно с авиационным отрядом специального назначения и при силовой поддержке СОБР «Беркут» ГУ МВД России по Краснодарскому краю с помощью беспилотника задержали подозреваемых в совершении серии краж (https://мвд.рф/news/item/7149953/).

В данном случае в доказывании по уголовному делу необходимо использовать электронную видеозапись. При этом согласно действующему законодательству электронные носители информации признаются вещест-

венными доказательствами. Однако закон не предусматривает порядок их возврата владельцу или собственнику. Последние могут получить лишь копию информации. Согласно ч. 3.1 ст. 183 УПК РФ по ходатайству законного владельца изымаемых электронных носителей информации или обладателя содержащейся на них информации специалистом, участвующим в выемке, в присутствии понятых с изымаемых электронных носителей информации осуществляется копирование информации на другие электронные носители информации, предоставленные законным владельцем изымаемых электронных носителей информации или обладателем содержащейся на них информации.

В последнем рассмотренном примере в качестве электронного носителя, по всей видимости, выступает ноутбук. Но его изъятие в определенной степени препятствует нормальной работе указанных спецслужб. И это не единственный случай. На практике изъятие электронных носителей все чаще создает трудности хозяйствующих субъектов и физических лиц (см. решение Арбитражного суда города Санкт-Петербурга и Ленинградской области по делу № А56-640/2013 // URL: http: //base.garant.ru/41122724/).

Федеральным законом от 3 июля 2016 г. № 323-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации по вопросам совершенствования оснований и порядка освобождения от уголовной ответственности» было установлено, что электронные носители информации, изъятые в ходе досудебного производства по уголовным делам о преступлениях, предусмотренных ст. 159 ч. 5–7, 159.1–159.3, 159.5, 159.6, 160 и 165 УК РФ, если эти преступления совершены в сфере предпринимательской деятельности, а также ст. 171–174.1, 176–178, 176–178, 180–183, 185–185.4 и 190–199.2 УК РФ, признаются вещественными доказательствами и приобщаются к материалам уголовного дела, о чем выносится соответствующее постановление. При этом изъятые в ходе досудебного производства, но не признанные вещественными доказательствами электронные носители информации, возвращаются лицам, у которых они были изъяты, не позднее чем через пять суток по истечении сроков, указанных в части второй настоящей статьи.

Другим Федеральным законом от 6 июля 2016 г. № 375-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» ст. 185 УПК РФ дополнена частью 7, согласно которой 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.

С последним нововведением проблем меньше не стало, так как закон не дает четких предписаний, как действовать следователю. Но однозначно для получения необходимой информации следователь, находясь в организации связи, должен привлечь в качестве специалиста оператора этой организации [1, с. 71].

Подвоя итог, следует заметить, что вопросы правового регулирования применения электронно-технических средств в доказывании по уголовным делам требуют большего внимания со стороны законодателя.

Литература

1. Васюков, В. Ф. Осмотр, выемка электронных сообщений и получение компьютерной информации / В. Ф. Васюков // Уголовный процесс. – 2016. – № 10. – С. 68–71.

2. Дмитриев, Е. Г. О некоторых особенностях использования информации систем видеонаблюдения в ходе расследования преступлений / Е. Г. Дмитриева, А. В. Котенков // Российский следователь. – 2013. – № 1. – С. 5–9.

3. Семенцов, В. А. Следственные действия в досудебном производстве (общие положения теории и практики): монография / В. А. Семенцов. – Екатеринбург: Изд-во «Уральская государственная юридическая академия», 2006. – 298 с.

4. Тарабан, Н. А. Информация о телефонных соединениях как доказательство в уголовном судопроизводстве и источник криминалистически значимой информации при раскрытии преступлений против личности / Н. А. Тарабан // Российский следователь. – 2014. – № 17. – С. 5–9.

Зуев Сергей Васильевич – доктор юридических наук, заведующий кафедрой правоохранительной деятельности и национальной безопасности, Южно-Уральский государственный университет, г. Челябинск. E-mail: zuevsergej@inbox.ru.

Статья поступила в редакцию 30 ноября 2016 г.

DOI: 10.14529/law170105

DIGITAL INFORMATION AND ITS CARRIERS IN CRIMINAL PROCEDURE PROVING: DEVELOPMENT OF LEGAL REGULATION

S. V. Zuev
South Ural State University, Chelyabinsk, Russian Federation

The author considers the development of the Russian Criminal Procedure Institution of using digital information and its carriers in criminal case proving. It is stated that the institution dates back to 2010 since the adoption of the Federal Law № 143-FZ, which introduced Clause 186.1 "Obtaining information about connections between subscribers and (or) subscriber units" into the RF Criminal Procedure Code. Since then, the organization providing communication services have been providing submitting information in a variety of physical media. The author proves the prospects for the development of electronic information backup and many other issues of dealing with digital information and its carriers. Attention is drawn to the fact that criminal proceedings should be developed on account of the modern information and communication relations in society.

Keywords: proof, criminal proceedings, digital information, electronic carriers of information.

References

1. Vasyukov V. F. [Inspection, seizure of electronic communications and obtaining computer information]. *Ugolovnyy protsess [Criminal process],* 2016, no. 10, pp. 68–71. (in Russ.)

2. Dmitriev E. G., Kotenkov V.A. [Some features of the use of information systems of video surveillance in the investigation of crimes]. *Rossiyskiy sledovatel' [Russian investigator]*. 2013, no. 1, pp. 5–9. (in Russ.)

3. Sementsov V. A. *Sledstvennye deystviya v dosudebnom proizvodstve (obshchie polozheniya teorii i praktiki)* [Investigative actions in pre-trial proceedings (general theory and practice)]. Ekaterinburg, 2006, 298 p.

4. Taraban N. A. [Information about the phone connection as a proof-tion in criminal proceedings and the source of considerable forensically-mine of information in solving crimes against the person]. *Rossiyskiy sledovatel' [Russian investigator]*. 2014, no. 17, pp. 5–9. (in Russ.)

Zuev Sergey Vasilievich – Doctor of Sciences (Law), Head of the Department of Law Enforcement and National Security, South Ural State University, Chelyabinsk, Russian Federation. E-mail: zuevsergej@inbox.ru.

Received 30 November 2016.

ОБРАЗЕЦ ЦИТИРОВАНИЯ

Зуев, С. В. Электронная информация и ее носители в уголовно-процессуальном доказывании: развитие правового регулирования / С. В. Зуев // Вестник ЮУрГУ. Серия «Право». – 2017. – Т. 17, № 1. – С. 31–35. DOI: 10.14529/law170105.

FOR CITATION

Zuev S. V. Digital information and its carriers in criminal procedure proving: development of legal regulation. *Bulletin of the South Ural State University. Ser. Law*, 2017, vol. 17, no. 1, pp. 31–35. (in Russ.) DOI: 10.14529/law170105.