УДК 343.140.02

Карташов Игорь Игоревич
кандидат юридических наук,
доцент кафедры уголовно-процессуального права;
Российский государственный университет правосудия
(Центральный филиал)
iik_vrn@mail.ru
Igor I. Kartashov
candidate of law;
associate professor of the chair of the criminal procedure right
of Central Branch of the Russian State University of Justice
iik_vrn@mail.ru

Цифровые данные в доказывании по уголовным делам: некоторые проблемы получения

Digital evidence in criminal cases: some problems of obtaining

Аннотация. *Статья посвящена процессуальным проблемам получения цифровых данных, хранящихся и циркулирующих в информационных телекоммуникационных системах, в ходе производства следственных действий и их последующего использования в доказывании по уголовным делам. В частности, проводится анализ возможности получения данных из облачных хранилищ посредством удаленного доступа. С учетом особенностей цифровой информации, информационных телекоммуникационных сетей и современных средств коммуникации, автором отмечается необходимость совершенствования уголовно-процессуального закона, а также предлагаются конкретные шаги в указанном направлении.*

Ключевые слова: *уголовное судопроизводство, цифровые данные, доказательства, информационные телекоммуникационные системы, облачные технологии*

Abstract. *The article is devoted to procedural problems of obtaining digital information stored and circulating in the information telecommunication systems, in the course of investigative actions and their subsequent use in proving criminal cases. In particular, the analysis of possibility of obtaining data from cloud storage through remote access. Given the peculiarities of digital information, information telecommunication networks and modern means of communication, the author notes the necessity of improvement of criminal procedural law, and proposes concrete steps in that direction.*

Key words: *criminal procedure, digital data, evidence, information telecommunication systems, cloud computing*

Тенденция развития информационных телекоммуникационных средств и систем указывает на формирование глобальной информационной структуры, включающей в себя не только компьютерные сети как таковые, но и телевидение, радиовещание, телефонию, с одновременным увеличением видов оконечных устройств [6, с. 46].

Возможности инфотелекоммуникационных систем не остались без внимания со стороны современного криминалитета, что привело к появлению новых способов совершения преступлений. Вместе с тем информационные телекоммуникационные системы стали не только инструментом совершения преступлений, но и той средой, где эти преступления совершаются. Указанные обстоятельства требуют от правоприменителя адекватной реакции, направленной на выявление, раскрытие и расследование совершенных преступлений. Однако, в отличие от представителей криминалитета, правоприменитель связан в своих действиях нормами права их регламентирующих. Особенно актуально это в процессе осуществления доказывания по уголовному делу, поскольку нарушение закона влечет за собой признание полученных доказательств недопустимыми (ст. 75 УПК РФ).

Следует отметить, что законодатель во многом не успевает или не хочет успевать за развитием инфотелекоммуникационных технологий, особенно в сфере совершенствования уголовно-процессуального законодательства. В настоящее время уголовно-процессуальный закон не закрепляет такого вида доказательств как «электронные» или «цифровые» [2, 3], используя термин «электронный носитель информации» (п. 5 ч.2 ст. 82 УПК РФ). Полагаем, что такая подмена понятий не допустима хотя бы по той причине, что значение для доказывания имеет непосредственно информация, содержащаяся на носителе, а не сам носитель как объект материального мира.

Еще большую проблему, на наш взгляд, порождает отсутствие в уголовно-процессуальном законе указания на процедуру получения электронных данных в некоторых случаях. Традиционно принято считать, что получить электронную информацию в рамках расследования уголовного дела можно посредством производства таких следственных действий как осмотр, обыск и выемка [5, с. 108].

Отметим, что следователь не всегда имеет дело непосредственно с физическим «электронным носителем информации» в том понимании, которое содержится в УПК РФ. Особенностью функционирования информационных телекоммуникационных сетей является то обстоятельство, что получить информацию, имеющую значение для уголовного дела, можно и не имея физического доступа к конкретному физическому носителю и даже не зная его точного пространственного местоположения. В частности, речь идет об использовании «облачных хранилищ», когда данные хранятся и обрабатываются в так называемом «облаке», которое представляет собой, с точки зрения клиента, один большой виртуальный сервер. Физически же такие серверы могут

располагаться удалённо друг от друга географически, вплоть до расположения на разных континентах.

Для получения информации из таких источников некоторыми авторами предлагается проводить «обыск посредством удаленного доступа» [1, с.75]. На наш взгляд, предлагаемый «выход» имеет ряд существенных недостатков. Во-первых, в отличие от обыска в классическом его понимании, в данном случае не происходит изъятия обнаруженной информации, а осуществляется лишь ее копирование. Кроме того, технология «удаленного обыска» предполагает использование специальных программно-аппаратных средств не только для обнаружения и закрепления (копирования) информации, но и для получения доступа к ней (обход или взлом паролей), что приводит к модификации исходных данных. Указанное обстоятельство ставит под сомнение возможность дальнейшего использования такой информации в качестве доказательств.

Во-вторых, как уже нами отмечалось, информация может храниться на физическом носителе, располагающемся за границами Российской Федерации. Между тем, в соответствии со ст. 2 УПК РФ действие уголовно-процессуального закона ограничивается территорией РФ, исключение составляют лишь случаи, предусмотренные ст. 12 УК РФ. В связи с чем возникает резонный вопрос: на сколько законно получение в процессе расследования информации, хранящейся на носителе, расположенном за пределами государства, посредством использования удаленного доступа? Полагаем, что при буквальном толковании закона мы придем к отрицательному ответу, поскольку юрисдикция российских органов расследования не распространяется на территорию иностранных государств. Выходом из сложившейся ситуации может отчасти послужить присоединение России к Конвенции о преступности в сфере компьютерной информации ETS №185, которая закрепила, что «в случае, когда компетентные органы производят обыск или получают аналогичный доступ к определенной компьютерной системе или ее части … и имеют основания полагать, что искомые данные хранятся в другой компьютерной системе или ее части …, и когда такие данные на законном основании могут быть получены из первой системы или с ее помощью, такие органы имели возможность оперативно распространить производимый обыск или иной аналогичный доступ на другую систему» (ч. 2 ст. 19) [4], а также введение в УПК РФ соответствующей нормы, регламентирующей производство указанных следственных действий.

Существенное значение для доказывания зачастую имеет не только информация, хранящаяся на тех или иных серверах, но и передающаяся по информационно-телекоммуникационным сетям в режиме on-line, в частности, сообщения электронной почты, переписка в разного рода мессенджерах, IP-телефония, общение в сетевых форумах и т.д. Однако, имеющиеся в УПК РФ нормы ст.ст. 185, 186, 186.1 УПК РФ не дают органам предварительного расследования получить соответствующую информацию посредством проведения следственных действий. В связи с

чем, в научной литературе можно встретить предложения о введении в УПК РФ такого следственного действия, как наложение ареста на электронно-почтовую корреспонденцию [7, с. 14]. В целом поддерживая указанный подход, полагаем, что данное следственное действие не должно ограничиваться лишь электронно-почтовой корреспонденцией, а распространяться на получение всех видов электронной информации, циркулирующей в инфотелекоммуникационных системах, содержащей сведения, имеющие значение для уголовного дела.

Получение электронной информации сопряжено с определенными трудностями и в случаях, когда следователь имеет непосредственный доступ к носителю такой информации. Следует констатировать, что стала привычной практика изъятия в ходе производства следственных действий различных средств коммуникации (смартфонов, планшетных компьютеров и т.п.) с последующим направлением их для проведения компьютерно-технической экспертизы. Отметим, что современные программно-аппаратные средства с успехом обходят установленные на средствах коммуникации пароли, и открывают доступ ко всей хранящейся на них информации. Если технический аспект таких действий не вызывает вопросов, то правовой порождает множество. Главный из них: не является ли такой порядок получения информации нарушением конституционных прав и интересов гражданина, поскольку осуществляется в отсутствии разрешения суда? Нам могут возразить, что для производства экспертизы его и не требуется. Это, безусловно, так. Но вместе с тем, не следует забывать, что ее производство связано с доступом к информации, тайна которой гарантируется Конституцией РФ (ст. 23).

С одной стороны законодатель признает производство такого следственного действия, как получение информации о соединениях между абонентами и (или) абонентскими устройствами, ограничивающим конституционные права граждан (ст. 186.1 УПК РФ). При том, что в ходе его производства органы расследования получают лишь информацию о дате, времени и продолжительности соединения, тогда как содержание разговора или текстового сообщения остается недоступной.

С другой стороны в ходе производства компьютерно-технической экспертизы открывается доступ не только к информации о соединениях владельца устройства, но и содержание SMS-переписки, голосовым сообщениям, не говоря о фото- и видеозаписях, геопозиционировании и т.д. Однако, никакого судебного разрешения в данном случае не требуется.

Такой подход представляется нам нелогичным и непоследовательным. В связи с чем полагаем, что в случае, когда телекоммуникационное средство или его носитель информации изымается в ходе производства следственного действия, производимого без судебного решения, то для производства последующих следственных действий, направленных на получение информации в нем содержащейся необходимо соответствующее разрешение суда.

Решение обозначенных нами проблем требует комплексного подхода к вопросам правовой регламентации получения, закрепления и проверки «цифровых доказательств» в уголовном судопроизводстве, с учетом специфики информационных телекоммуникационных систем.

Литература:

1. Иванов А.Н. Удаленное исследование компьютерной информации: уголовно-процессуальные и криминалистические проблемы // Известия Саратовского университета. Сер. Экономика. Управление. Право. 2009. № 2. С. 74 – 77.

2. Иванов Н.А. Цифровые доказательства: понятие и классификация // Криминалистика в системе правоприменения: Материалы конф. М., 2008. С. 130 – 134.

3. Карташов И.И. «Цифровые доказательства» в уголовном процессе // Центральный научный вестник. 2016. Т. 1. № S15. С. 23-25.

4. Конвенция о преступности в сфере компьютерной информации ETS №185 (Будапешт, 23 ноября 2001 г.) // СПС «Гарант» (дата обращения 30.11.2017).

5. Мещеряков В.А., Трухачев В.В. Формирование доказательств на основе электронной цифровой информации // Вестник Воронежского института МВД России. 2012. №2. С. 108 – 110.

6. Осипенко А.Л. Сетевая компьютерная преступность: теория и практика борьбы: монография / А.Л. Осипенко. – Омск: Омская академия МВД России, 2009. 480с.

7. Усов А.И. Концептуальные основы судебно-компьютерно-технической экспертизы: автореф. Дис. ... д-ра юрид. наук. – М., 2002. 41с.

Literature:

1. Ivanov A.N. Remote research of computer information: criminal procedure and criminalistic problems//News of the Saratov university. It is gray. Economy. Management. Right. 2009. No. 2. Page 74 – 77.

2. Ivanov N.A. Digital proofs: a concept and classification//Criminalistics in the system of law enforcement: Materials конф. M, 2008. Page 130 – 134.

3. Kartashov I.I. "Digital proofs" in criminal trial//the Central scientific bulletin. 2016. T. 1. No. S15. Page 23-25.

4. The convention on crime in the sphere of computer information of ETS No. 185 (Budapest, on November 23, 2001)//Union of Right Forces "Guarantor" (date of the address 11/30/2017).

5. Meshcheryakov V. A., Trukhachev V.V. Formation of proofs on the basis of electronic digital information//Messenger of the Voronezh institute of the Ministry of Internal Affairs of the Russian Federation. 2012. No. 2. Page 108 – 110.

6. Osipenko A.L. Network computer crime: theory and practice of fight: monograph / A.L. Osipenko. – Omsk: Omsk Russian Interior Ministry Academy, 2009. 480 pages.

7. Usov A.I. Conceptual bases of judicial computer technical expertize: автореф. Yew. ... Dr.s юрид. sciences. – M, 2002. 41 pages.