Научная статья
УДК 343.85
DOI 10.33184/vest-law-bsu-2024.22.9

Романова Галина Валерьевна
Казанский институт (филиал) Всероссийского государственного университета юстиции (РПА Минюста России), Казань, Россия,
GGG341@yandex.ru, https://orcid.org/0000-0002-7247-5983

ЗНАЧЕНИЕ ЭЛЕКТРОННЫХ ДОКАЗАТЕЛЬСТВ В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ

Аннотация. В настоящее время сформировалась информационная сфера, обеспечиваемая функционированием системы объектов цифровой инфраструктуры. Элементы данной системы, представляющие собой информационные процессы и средства их осуществления с присущими им функциональными возможностями информационных преобразований, связанные с поиском, анализом, хранением и упорядочением информации, могут быть использованы и в качестве технико-криминалистических средств, что предопределяет важность поиска и исследования способов и приемов их интеграции в процессе решения криминалистических задач. Однако внедрение передовых технологий в сферу уголовного судопроизводства, как и их применение, само по себе не способно повысить его качество, но позволяет обратить внимание на детали. Существует значительное количество исследований в области разработки технико-криминалистических средств обнаружения и фиксации цифровых (электронных, виртуальных, компьютерных) следов преступной деятельности, однако большинство из них посвящены вопросам разработки и применения специальных технико-криминалистических средств в судебно-экспертной деятельности. Современные высокотехнологичные разработки, специальные программы должны быть использованы на первоначальных этапах расследования. Грамотно процессуально оформленное обнаружение, фиксация, изъятие и сохранение цифровой информации в значительной мере будет способствовать изобличению всех участников преступного события, их розыску и задержанию, поиску похищенного и в целом обеспечению надежной доказательственной базы для органов предварительного расследования. В статье раскрывается значение электронных доказательств в российском законодательстве и практике его применения.

Ключевые слова: уголовный процесс, досудебное производство, электронное доказательство, уголовное судопроизводство, информация, интернет-ресурсы, преступление, доказывание, интернет-доказательство, оценка доказательств

Для цитирования: Романова Г.В. Значение электронных доказательств в уголовном судопроизводстве / Г.В. Романова. – DOI 10.33184/vest-law-bsu-2024.22.9 // Вестник Института права Башкирского государственного университета. – 2024. – № 2. – С. 84–93.

Original article

Romanova Galina Valeryevna
Kazan Institute (Branch) of All-Russian State University of Justice
(RLA of the Ministry of Justice of Russia), Kazan, Russia,
GGG341@yandex.ru, https://orcid.org/0000-0002-7247-5983

THE IMPORTANCE OF DIGITAL EVIDENCE IN CRIMINAL PROCEDURE

Abstract. At present, the information sphere provided by the functioning of the digital infrastructure objects system has been formed. Elements of this system, representing information processes and means of their implementation with inherent functionality of information transformations, associated with the search, analysis, storage and arrangement of information, they can also be used as technical and forensic means, which makes it important to find and explore ways and means of integrating them into the forensic process. The introduction and use of advanced technology in the field of criminal procedure does not in itself increase its quality but allows paying attention to details. There is a significant amount of research in the development of technical and forensic means of detection and fixation of digital (electronic, virtual, computer) traces of criminal activity, but most of them are devoted to the development and application of special technical and forensic means in forensic activities. With the development of modern high technology, special programmes should be used in the initial stages of the investigation. The proper detection, fixation, seizure and preservation of digital information will significantly contribute to the identification of all participants in the criminal event, their search and arrest, the search for stolen goods and, in general, provide a reliable evidence base for the preliminary investigation. The article reveals the significance of digital evidence in the Russian legislation and practice of its application.

Keywords: criminal proceeding, pre-trial procedure, digital evidence, criminal procedure, information, Internet resources, crime, evidence, Internet evidence, evaluation of evidence

For citation: Romanova G.V. The Importance of Digital Evidence in Criminal Procedure. *Vestnik Instituta prava Bashkirskogo gosudarstvennogo universiteta = Bulletin of the Institute of Law of the Bashkir State University,* 2024, no. 2, pp. 84–93. (In Russian). DOI 10.33184/vest-law-bsu-2024.22.9.

Фундаментом досудебного судопроизводства, как известно, является доказывание по уголовному делу, содержание которого, согласно уголовно-процессуальному закону, составляет совокупность процедур собирания, проверки и оценки доказательств. Основными способами собрания доказательств выступают следственные действия, являющиеся центральным звеном в системе доказывания, а основной фигурой в сборе доказательственной информации является следователь. Его полномочия по производству следственных действий установлены в ч. 1 ст. 86 УПК РФ и конкретизированы в уголовно-процессуальных нормах, в которых определены основания и порядок производства конкретных следственных действий.

Большинство уголовно-процессуальных норм, в которых установлены основания и порядок производства следственных действий, сконструировано таким образом, что вывод о том, вправе или обязан следователь производить то или иное следственное действие, возможен при наличии определенных условий. Например, информация о том, что фигуранты во время совершения преступления разговаривали по мобильному телефону, инициирует процедуру получения информации о местоположении абонентов, активность которых была проявлена в этом районе. В то же время анализ структуры этих же норм, осуществляемый с учетом процессуальных ситуаций, в которых они используются, говорит о том, что в ряде случаев следователь обязан соблюдать определенный алгоритм, состоящий из последовательно проведенных следственных действий. Наиболее ярким примером служит специфика реализации в доказывании видеофайлов, копирование которых осуществляется при производстве выемки в помещении, где установлен компьютер, записывающий информацию с камер видеонаблюдения.

После проведения выемки электронного носителя информации следователь обязан провести осмотр скопированных видеозаписей. При обнаружении значимой для доказывания информации в ходе просмотра видеофайлов в обязательном порядке назначается судебная экспертиза. В последующем в ходе целого спектра следственных действий имеющаяся информация должна быть использована в качестве доказательственной. Однако в каждой отдельной ситуации применение алгоритма определяется не только

обязанностью проведения конкретного следственного действия, но и правом, которым наделяется следователь. Например, при анализе результатов осмотра места происшествия и сопоставления информации с картографических сервисов следователь может сделать вывод, что при осмотре исследовались не все здания, оборудованные камерами видеонаблюдения, и принять решение о проведении дополнительного осмотра.

Вопрос об уголовно-процессуальной природе электронных доказательств из сети Интернет, как и непосредственно связанный с ним вопрос о сущности цифровых доказательств, является непростым, а в ряде случаев даже спорным. Так, М. Хужин считает интернет-доказательства отдельным видом уголовно-процессуальных доказательств [1]. Н. Меркулов, напротив, придерживается мнения о том, что оснований для такого выделения нет и следует говорить о цифровом носителе информации, а их фиксация не требует специальной уголовно-процессуальной формы [2]. М. Шалумов рассматривает интернет-доказательства как подвид электронных доказательств [3, с. 84].

Таким образом, для одних исследователей и практиков понятия интернет-доказательства и цифровые (электронные) доказательства являются синонимами, для других – отдельными и самостоятельными явлениями, а третьи рассматривают интернет-доказательства как подвид электронных доказательств. При этом каждый автор включает в перечень разновидностей интернет-доказательств разный объем сведений и их источников, что не позволяет установить единое содержание данного понятия.

Между тем решение указанного вопроса имеет важное практическое и теоретическое значение, так как от него зависит, имеется ли необходимость в выделении специфических признаков интернет-доказательств и, соответственно, в разработке методики их сбора, фиксации, использования и оценки в уголовном процессе. Другими словами, наличие у группы доказательств отличительных черт, имеющих процессуальное и материальное значение, обусловливает их выделение в качестве отдельного понятия, полезного для криминалистики и уголовного процесса.

Так, 23 февраля 2022 г. гражданин Е. совершил сделку: продал рублевый код на 900 000 руб. Деньги за продажу поступили на карту Сбербанка, которая была оформлена на девушку Е. После поступления денежных средств карту заблокировали. Оказалось, что поступившая денежная сумма была похищена телефонными мошенниками (схема со звонком из «службы безопасности» крупного банка и просьбой перевести средства на «безопасный счет»). Действия мошенников были заранее продуманы. Жертва мошенников перечислила деньги на счет неизвестного гражданина С., платежную карту которого преступники использовали для похищения денег, а сам граж-

данин С. получал за это определенный процент. Именно со счета гражданина С. денежные средства поступили на карту девушки Е.

Правоохранительные органы раскрыли данную преступную схему и задержали всех участвующих в ней лиц. По версии следствия, Е., С. и мошенники, которые выманили деньги у потерпевшего, действовали в преступном сговоре, о чем свидетельствовала изъятая электронная переписка. За такие действия суд назначил гражданину Е. 2 года условно, а гражданину С. – 2,5 года условно (оба свою вину признали). По мнению суда, молодые люди жили в разных концах России, общались посредством электронных сообщений.

Очевидно, что определяющим признаком интернет-доказательств является их происхождение: для всех в качестве единого источника выступает Интернет. Как нам видится, Интернет представляет собой информационную систему – результат коммуникации и взаимодействия различных устройств, объединенных посредством единого «языка общения» – интернет-протокола.

Если рассматривать Интернет сугубо функционально как способ коммуникации по типу «отправитель – получатель», то он будет выступать источником таких сведений, как электронная переписка, блокчейн-трансакции или базы данных. Эти сведения, как нам представляется, можно отнести к интернет-доказательствам. В то же время следует помнить, что не все базы данных могут иметь отношение к Интернету, некоторые могут существовать автономно.

Такой же подход справедлив и по отношению к электронной почте или блокчейну. Хотя обмен электронными сообщениями или информацией в данном случае осуществляется посредством Интернета, канал связи закрыт от остального информационного пространства. Только отправитель и адресат, а не любой иной пользователь имеют доступ к содержанию электронных сообщений. Интернет здесь выступает не как источник доказательственной информации, а лишь как способ ее передачи между физическими накопителями – серверами. В итоге доказательственная информация хранится на устройствах даже после отключения от Сети: полученные или отправленные сообщения электронной почты записываются на жесткий диск (или сервер-провайдер), а данные о трансакции сохраняются в закрытом электронном кабинете пользователя и на флэш-карте. Иными словами, Интернет в представленных примерах не производит доказательственную информацию, а лишь передает ее между устройствами в Сети. Это влечет за собой ориентированность следствия при поиске указанных доказательств исключительно на физические носители как первичные источники информации.

Единственной обусловленной Интернетом особенностью электронной переписки или иных подобных доказательств является их трансграничная природа, которая порождает сложности в отношении определения места

хранения электронной переписки и заставляет государства более тесно сотрудничать в рамках международной правовой помощи по уголовным делам для исключения риска конфликта юрисдикции правоохранительных органов. С другой стороны, как электронная почта, так и блокчейн, файлообмен или база данных могут быть реализованы и отдельно от Интернета в рамках локальной изолированной подсети, иногда достаточно больших размеров. Такое решение все чаще используется корпорациями (в том числе банками), желающими обезопасить свой внутренний информационный трафик от угроз извне[1].

Если подходить к Интернету как к общему информационному пространству, открытому источнику сведений и цифровой платформе, выходящей за рамки сугубо коммуникационных нужд, интернет-ресурсы обретают собственную, отдельную от физического носителя значимость как источника сведений. В качестве примера приведем случай из следственной практики.

Главным следственным управлением СК России совместно с оперативными службами было выявлено лицо, разместившее на сайте движения «Бессмертный полк» в сети Интернет фотографию лидера Национал-социалистической немецкой рабочей партии Адольфа Гитлера. Как указано в материалах дела, подобные действия преследуют цель одобрения преступлений нацистского режима. Этим лицом оказался житель Воронежа Александр Хорошильцев. По данному факту было возбуждено уголовное дело по признакам преступления, предусмотренного ч. 1 ст. 354.1 УК РФ – реабилитация нацизма, то есть одобрение преступлений, установленных приговором Нюрнбергского военного трибунала, совершенное публично[2]. В отношении Хорошильцева был вынесен обвинительный приговор, он понес заслуженное наказание.

Анализируя данный пример, следует отметить, что в поле зрения следственных органов часто попадают такие сведения, которые не просто передаются посредством Интернета, а генерируются им, то есть образуются в информационном пространстве и адресуются всем пользователям этого пространства. В качестве таковых могут выступать сайты, личные открытые блоги, сайты вакансий и другие ресурсы, которые продуцируются компаниями и (или) пользователями, в том числе совместно, и предназначены для неограниченного круга лиц. Важная особенность таких источников состоит в

---

[1] Так называемые компьютерные сети, изолированные по принципу «воздушного зазора» (air-gapped networks). См. подробнее: Предприятие с изолированной подсетью: что может пойти не так? [Электронный ресурс]. URL: https://www.kaspersky.ru/ blog/cyberthreats-in- isolated-subnet/31002/ (дата обращения: 12.02.2024).

[2] Следственный комитет РФ : сайт [Электронный ресурс]. URL: https://sledcom.ru/ news/item/1489166/ (дата обращения: 12.02.2024).

том, что их привязка к Интернету как общему информационному пространству и виртуальной среде намного сильнее, чем к материально-технической инфраструктуре Сети. Не играет существенной роли то, на каком носителе в итоге хранится текст открытого поста в социальной сети или опубликованная вакансия на сайте-агрегаторе, значение имеет сама информация. Причем такая информация из Интернета может иметь не только ориентирующее, как кажется на первый взгляд, но и материально-правовое значение, то есть напрямую определять уголовную квалификацию совершенного деяния.

К примеру, совершение преступных действий через Интернет является квалифицирующим признаком большого количества составов преступлений, предусмотренных УК РФ: п. «д» ч. 2 ст. 110, п. «д» ч. 3 ст. 110.1, ч. 2 ст. 110.2, ч. 2 ст. 128.1, п. «б» ч. 3 ст. 133, ч. 3 ст. 137, п. «в» ч. 2 ст. 151.2 и др. Соответственно, интернет-доказательства могут свидетельствовать о наличии квалифицирующего признака состава преступления, влиять на его правильную квалификацию следствием и судом.

В процессе формирования доказательств по уголовному делу зачастую имеется не только информация, хранящаяся на серверах, но и передающаяся по информационно-телекоммуникационным сетям в режиме онлайн, в частности сообщения электронной почты, переписка в мессенджерах, социальных сетях и т. п. Например, 5 марта 2020 г. неустановленное лицо распространило через электронную почту интимные фотографии 25-летней жительницы Казани. По данному факту следственными органами СК России по Республике Татарстан возбуждено уголовное дело по ч. 1 ст. 137 УК РФ (нарушение неприкосновенности частной жизни). В процессе расследования было установлено, что фотографии были отправлены на электронную почту молодого человека потерпевшей. В ходе грамотно спланированных следственных действий и оперативно-розыскных мероприятий установлен предполагаемый злоумышленник – 29-летний бывший друг потерпевшей[1].

В другом случае следственными органами СК России по Республике Татарстан было проведено расследование уголовного дела в отношении 31-летнего местного жителя, обвиняемого в совершении преступлений, предусмотренных ч. 1 ст. 135 УК РФ (развратные действия), п. «б» ч. 3 ст. 242 (незаконное изготовление и оборот порнографических материалов), п. «б» ч. 4 ст. 132 УК РФ (насильственные действия сексуального характера в отношении лица, не достигшего четырнадцатилетнего возраста). По версии следствия, в 2020–2021 гг. обвиняемый в одной из социальных сетей познакомился с двумя жителями Казани 2007 и 2009 г. р., после чего вел с ними пе-

[1] Следственное управление Следственного комитета РФ по Республике Татарстан : сайт [Электронный ресурс]. URL: Tatarstan.sledcom.ru (дата обращения: 12.02.2024).

переписку интимного характера, направляя порнографические материалы. Родители одного из детей обнаружили эту переписку и обратились в правоохранительные органы. Судом по ходатайству следователя в отношении 31-летнего мужчины была избрана мера пресечения в виде заключения под стражу.

Полагаем, что нельзя недооценивать общее процессуальное значение интернет-доказательств при расследовании преступлений. Открытые сведения из Интернета могут доказывать:

– связь между преступниками и членами преступных формирований;

– обмен преступным опытом;

– поиск жертвы и орудий преступления;

– поиск соучастников готовящихся преступлений;

– сбыт имущества, добытого преступным путем;

– осуществление расчетно-денежных операций между лицами с целью подготовки и совершения преступлений;

– наличие имущества у подозреваемых и обвиняемых;

– данные, характеризующие фигурантов уголовного дела;

– способ совершения и сокрытия следов преступления.

В отличие от электронной почты и иных закрытых источников открытые данные в Интернете, такие как веб-сайты, форумы, агрегаторы и информационные сервисы, не могут существовать отдельно от Сети, а являются непосредственной частью единого глобального интернет-пространства. Их процессуальная фиксация не требует физического взаимодействия с конкретным материальным носителем, так как информация подобного рода, с одной стороны, доступна для неограниченного круга лиц, а с другой – подвержена постоянным изменениям и модификации.

Трансграничный характер Интернета в отношении таких сведений не усложняет процесс их получения, а упрощает его: если при получении электронной переписки, сохраненной на сервере, находящемся за рубежом, возникает вопрос о границах юрисдикции правоохранительных органов одной страны [4; 5], то в случае с интернет-ресурсами публичный и открытый характер информационных данных обусловливает их использование любым властным субъектом вне зависимости от территориальных границ государств.

Таким образом, в качестве признаков интернет-доказательств можно выделить следующие:

l) неразрывная связь с Интернетом;

2) доступность информации для потенциально неограниченного круга лиц;

3) независимость презентации информации и доступа к ней от физического носителя (хотя сама она записана на физическом носителе и с технологической стороны неотделима от него).

В заключение отметим, что интернет-доказательство представляет собой информацию, имеющую значение для уголовного дела и неразрывно связанную с Интернетом, что обусловливает ее возникновение и предназначение исключительно для презентации и (или) восприятия в публичном цифровом пространстве неограниченным кругом лиц (а не в закрытой сети с ограниченным количеством пользователей).

Список источников

1. Хужин М. Использование интернет-доказательств в уголовном процессе / М. Хужин // Адвокатская газета. – 2020. – № 20.

2. Меркулов Н. От неподготовленности страдают все / Н. Меркулов // Адвокатская газета. – 2020. – № 20.

3. Шалумов М.С. Электронные доказательства в уголовном судопроизводстве / М.С. Шалумов // Уголовный процесс. – 2021. – №12 (204). – С. 80–85.

4. Jahn M. Digitale Beweismittel im deutschen Strafprozess – Ermittlungsverfahren, Hauptverhandlung und Revision / M. Jahn, D. Brodowski // Digitalisierung und Strafverfahren. – 2020. – № 23 (4). – S. 228–238.

5. Chalmers D. European Union law / D. Chalmers, G. Davies, G. Monti. – Cambridge University Press, 2010. – 1000 p.

References

1. Khuzhin M. Use of Internet Evidence in Criminal Proceedings. *Advokatskaya gazeta = Lawyer's Newspaper,* 2020, no. 20. (In Russian).

2. Merkulov N. Everyone Suffers from Unpreparedness. *Advokatskaya gazeta = Lawyer's Newspaper,* 2020, no. 20. (In Russian).

3. Shalumov M.S. Electronic Evidence in Criminal Proceedings. *Ugolovnyj process = Criminal Procedure,* 2021, no. 12 (204, pp. 80–85. (In Russian).

4. Jahn M., Brodowski D. Digitale Beweismittel im deutschen Strafprozess – Ermittlungsverfahren, Hauptverhandlung und Revision. *Digitalisierung und Strafverfahren,* 2020, no. 23 (4), pp. 228–238.

5. Chalmers D., Davies G., Monti G. European Union Law. Cambridge University Press Publ., 2010. 1000 p.

Информация об авторе

Романова Галина Валерьевна *–*
кандидат юридических наук,
доцент кафедры уголовного
процесса и криминалистики

Information about the Author

Romanova Galina Valeryevna *–*
Candidate of Sciences (Law), Associate
Professor of the Chair of Criminal
Procedure and Criminalistics

Статья поступила в редакцию 31.03.2024; одобрена после рецензирования 29.04.2024; принята к публикации 29.04.2024.
The article was submitted 31.03.2024; approved after reviewing 29.04.2024; accepted for publication 29.04.2024.