ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ПРАВОВЫЕ ПРОБЛЕМЫ УКРЕПЛЕНИЯ РОССИЙСКОЙ ГОСУДАРСТВЕННОСТИ

Часть 83

Сборник статей

LEGAL ISSUES OF STRENGTHENING RUSSIAN STATEHOOD

Vol. 83

Collection of papers

Томск
Издательский Дом Томского государственного университета
2019

14. El'kind, P.S. (1963) *Sushchnost' sovetskogo ugolovno-protsessual'nogo prava* [The essence of Soviet criminal procedure law]. Leningrad: Leningrad State University.
15. Alekseev, S.S. (1966) *Mekhanizm pravovogo regulirovaniya v sotsialisticheskom gosudarstve* [The mechanism of legal regulation in a socialist state]. Moscow: Nauka.
16. Gorshenev, V.M. (1985) *Teoriya yuridicheskogo protsessa* [The theory of the legal procedure]. Kharkiv: Vishcha shkola.
17. Lazarev, V.V. (1974) *Probely v prave i puti ikh ustraneniya* [Gaps in law and ways to eliminate them]. Moscow: Yurid. lit. pp. 175–176.
18. Sil'chenko, D.Yu. (2001) *Primenenie analogii v ugolovnom sudoproizvodstve* [The use of analogy in criminal proceedings]. Abstract of Law Cand. Diss. Moscow.
19. Yakubovich, N.A. (1971) *Teoreticheskie osnovy predvaritel'nogo sledstviya* [The theoretical foundations of the preliminary investigation]. Moscow: Yur. lit.
20. Grigor'ev, V.N., Pobedkin, A.V. & Yashin, V.N. (2006) *Ugolovnyy protsess* [The criminal procedure]. Moscow: Izd-vo Eksmo.
21. Mikheenko, M.M. (1984) *Dokazyvanie v sovetskom ugolovnom protsesse* [Proof in the Soviet criminal procedure]. Kyiv: Vishcha shkola.
22. Larin, A.M. (1985) *Ugolovnyy protsess: struktura prava i struktura zakonodatel'stva* [The criminal procedure: structure of right and structure of law]. Moscow: Yurid. lit.
23. Konovalova, V.E. (1997) *Kriminalisticheskaya taktika: teorii i tendentsii* [Forensic tactics: theories and trends]. Kharkiv: Grif.
24. Marfitsin, P.G. (2002) *Usmotrenie sledovatelya (ugolovno-protsessual'nyy aspekt)* [The discretion of the investigator (a criminal procedural aspect)]. Omsk: Omsk Institute of the Ministry of Internal Affairs of the Russian Federation.

DOI: 10.17223/9785946218566/24

И.В. Чаднова, А.В. Извеков

ЦИФРОВЫЕ СЛЕДЫ КАК ДОКАЗАТЕЛЬСТВО В УГОЛОВНОМ ПРОЦЕССЕ

В статье рассматриваются вопросы использования цифровых следов в процессе доказывания, включения результатов получения электронной информации в систему доказательств в уголовном судопроизводстве.
Ключевые слова: цифровые следы, процессуальная форма, доказывание, доказательство, следственные действия.

В настоящее время неуклонно прогрессирует оцифровка повседневной жизни. Создание цифрового мультимедиа любого вида теперь столь же естественно, как и его потребление, доступно любому

человеку и в любое время. Контент и информация создаются и распространяются в цифровом поле все в больших объемах. Это развитие также оказывает влияние на систему уголовного правосудия.

Цифровые данные обладают значительным потенциалом для изменения различных форм коммуникации. Поскольку уголовное судопроизводство, конечно же, не более чем конкретная коммуникационная платформа, прогрессивные изменения также оказывают на него значительное влияние. Не меньшее значение имеют аспект манипулирования цифровыми доказательствами, который тесно связан с безопасностью данных, а также сопряженные с этим вопросы защиты и ценности доказательств. В настоящее время создаются совершенно новые возможности совершения преступлений в цифровом пространстве, которые можно обобщить кратким термином «киберпреступность». Адаптация существующих норм уголовного и уголовно-процессуального права должна в полной мере и своевременно следовать этому развитию. Поэтому важно найти способ включить цифровые средства информации и их особенности в существующую правовую базу, в систему уголовного правосудия и тем самым создать стандарты, отвечающие требованиям уголовного судопроизводства.

Рост цифровой информации неизбежно идет рука об руку с растущей важностью цифровых доказательств. Текстовые документы, а также фото-, видео- и аудиозаписи теперь в основном создаются и хранятся в цифровом виде. Все типы данных хранятся на носителях в компьютерах и мобильных телефонах, на серверах и в облачном хранилище. Общение происходит через интернет, что такие службы, как Вконтакте, Одноклассники или Whatsapp, через форумы и, конечно, по электронной почте. Местоположение и движение мобильных телефонов возможно отследить путем набора номера в радиоячейках. Вся эта информация может иметь отношение к уголовному судопроизводству и поэтому может рассматриваться как доказательство. Следует, однако, отметить, что цифровые доказательства имеют свои особенности, которые следует учитывать при их рассмотрении. Благодаря цифровой форме хранимой информации ее можно относительно легко и разными способами модифицировать. Большинство программ, которые помогают осуществлять подобного рода манипуляции, доступны бесплатно и предлагают возможность последующих изменений, которые были бы не так просты с рукописным документом или проявленными с пленки фотографиями. Как создание файлов,

так и последующие изменения в них обычно оставляют цифровые следы. Утерянные, на первый взгляд, данные могут быть реконструированы и проверены. Восстановление измененного файла в его первоначальный вид должно быть произведено в рамках экспертизы, то же самое относится и к восстановлению уничтоженных данных. Простое форматирование жесткого диска не так критично, нежели сожжение письма или фотопленки. Помимо этого, интернет менее анонимен, чем думает большинство. На сегодняшний день возможно проследить почти всю активность обычного пользователя.

Специфика фиксации цифровых доказательств предполагает необходимость раннего выявления «места совершения цифрового преступления» и использование специальных тактических приемов при его осмотре. Крайне важным является полное сохранение доказательств. Полученные данные должны быть надлежащим образом защищены, при необходимости сделана полная копия соответствующего носителя данных. Таким образом, дальнейшие исследования могут проводиться на основе всей базы данных без необходимости отказа пользователя от использования своего устройства. Этот факт является одним из важнейших обстоятельств для лиц, использующих цифровые устройства в своей работе. Изъятые данные, в свою очередь, должны храниться следственными органами с наименьшим риском потери.

Важность цифровых доказательств в каждом конкретном случае зависит, не в последнюю очередь, от вида преступного деяния. Если это «классическое» преступление, в котором деяние не имеет места в цифровом пространстве, обычно доступны стандартные доказательства, достаточные для реконструкции деяния. Кража может быть раскрыта, например, с помощью показаний свидетелей и обнаружения похищенного имущества. Цифровое доказательство в таком случае является подходящим и необходимым только в качестве дополнительного доказательства. Если преступник обменялся электронным письмом о правонарушении или предложил украденные товары для продажи в интернете, эти аспекты будут важными, но не обязательными при судебном преследовании за совершение правонарушения преступления.

В области «киберпреступлений» цифровые доказательства имеют очевидную значимость. При совершении деяния, которое происходит исключительно в цифровом пространстве, следственным органам остается полагаться исключительно на цифровые данные. Например,

любой, кто вошел без авторизации в корпоративную сеть и получил конфиденциальные данные, не оставляет ощутимых следов. Отслеживание доступа в большинстве случаев будет затруднено мерами анонимизации, которые необходимо обнаружить и обойти. Например, необходимо доказать, кто использовал атакующий компьютер во время совершения преступления. Сделать это можно путем оценки входов в систему.

Помимо массовых преступлений, цифровые доказательства в крупномасштабных экономических и налоговых преступлениях имеют значение, которое трудно переоценить. Это относится, например, к преступности на рынке капитала, где зачастую уже все действия и процессы обрабатываются исключительно в цифровой форме, например, в так называемом высокочастотном трейдинге. Когда речь идет о заявлении по факту манипулирования рынком, подозрительные транзакции часто становятся известными только в результате автоматического анализа в реальном времени, путем определения эффективности конкретных ценных бумаг. При необходимости эти данные также позволяют сделать выводы об отправителях транзакций. То же самое относится, например, к оценкам данных учетной записи.

Для полноценной реализации возможностей использования полученных цифровых следов возникает необходимость в определении места цифровых доказательств в системе доказательств в уголовном судопроизводстве. Сложность заключается в том, что цифровые данные еще не учтены в законодательстве в той мере, в какой это соответствует их практической значимости. В данном отношении уголовный процесс находится в невыгодном положении, поскольку в нем отсутствуют конкретные положения, которые уже нашли свое применение в других отраслях законодательства.

Так, Гражданский процессуальный кодекс Российской Федерации в ст. 178 использует понятие «цифровые данные». Кроме того, приняты следующие стандарты: «ГОСТ OIML R 76-1-2011. Межгосударственный стандарт. Государственная система обеспечения единства измерений. Весы неавтоматического действия. Часть 1. Метрологические и технические требования. Испытания» (Приложение D. Испытание в целях утверждения типа устройств обработки *цифровых данных*, терминалов и цифровых дисплеев как модулей весов, испытуемых отдельно); «ГОСТ Р ИСО 11073-91064-2017. Национальный стандарт Российской Федерации. Информатизация здоровья. Стан-

дартный протокол коммуникаций. Часть 91064. Компьютерная электрокардиография» (Приложение А. Кодирование *алфавитно-цифровых данных* электрокардиограммы в многоязычной среде).

В то же время такие понятия не используются в уголовном процессе. Единственным более-менее соответствующим понятием являются «электронные носители информации», однако они выступают только в качестве передатчика информации.

Использование ст. 85 УПК РФ при рассмотрении возможности отнесения цифровых доказательств к доказательствам, содержащимся в ст. 74 УПК РФ, кажется очевидным, но оно относится к содержимому данных. В то же время перечень доказательств, установленный ст. 74 УПК РФ, приравнивает иные документы к документам или заключениям эксперта и специалиста, т.е. уже воплощенной на бумажном носителе мысли, которая может быть прочитана без предварительной обработки. Но именно этого свойства не хватает цифровым доказательствам.

Помимо этого, стенограммы или механические дубликаты подпадают под концепцию документа – их объединяет то, что они основаны на уже существующих вариантах данных, но не создают их впервые. В отличие от документа, существует возможность получить прямой доступ к цифровому файлу после его создания. С другой стороны, заключения экспертов и специалистов представляются более важными в контексте интерпретации содержания и, прежде всего, достоверности информации.

Очевидные и особые черты цифровых данных, которые с большей вероятностью будут справедливы, – это их классификация как визуального объекта. Соответствующее положение п. 6 ч. 2 ст. 74 УПК РФ де-юре выполняет функцию собирания всех потенциальных доказательств, которые не подпадают под конкретно регламентированные случаи свидетельских, экспертных или документарных доказательств. Но справляется ли оно на практике? В отличие от аналоговых носителей простого воспроизведения на устройстве недостаточно. Скорее, в дополнение к аппаратному обеспечению требуемое программное обеспечение должно присутствовать и работать должным образом. Тем не менее утверждение визуального субъекта представляется уместным, поскольку цифровые данные в конечном счете являются дальнейшим развитием аналоговых данных, таких как фото-, видео-, аудиофайлов и др.

Как правило, доказательства могут достигать своей цели только в том случае, если содержимое файла не является спорным, установлена его подлинность, авторство, а также свобода от манипулирования. В таком случае суду первой инстанции было бы почти невозможно вынести квалифицированное решение на основе своего собственного толкования. Остается только обращаться за консультациями к экспертам. Эксперт, в свою очередь, зависит от соответствующего оборудования – сначала для изъятия, а затем для проверки подлинности, целостности или авторства соответствующего файла. Использование, конечно, также должно быть соответствующим образом задокументировано. Чтобы исключить любые сомнения при оценке цифровых доказательств, суду необходимо проконсультироваться с экспертом в целях констатации подлинности таких доказательств и отсутствия произведенных с ними манипуляций. На практике, однако, такая процедура может потерпеть неудачу из-за связанных с этим мероприятием расходов.

Все доказательства, согласно ч. 1 ст. 17 УПК РФ, должны отвечать принципу свободы оценки доказательств. Если обвинительный приговор будет основан на цифровых источниках информации, суд при их исследовании должен достичь уровня безопасности, достаточного для того, чтобы в подлинности и достоверности таких доказательств не возникало никаких сомнений. Определенный базовый скептицизм в этом вопросе представляется уместным, учитывая, что в соответствии с законодательством для применимых в суде электронных документов требуется квалифицированная подпись в соответствии с ФЗ «Об электронной подписи». Полагаем, что даже сам термин «электронная подпись» некорректен и должен быть изменен на более точный – «цифровая подпись». Если доказательством, подлежащим рассмотрению, является электронное письмо, такая подпись должна обеспечивать, например, отсутствие разумных сомнений в отношении его авторства. Однако наличие квалифицированной цифровой подписи следует ожидать только в наименьшем количестве случаев, это скорее исключение, чем правило. Данная проблема может быть отнесена к большинству цифровых доказательств. В этом контексте следует также упомянуть цифровые водяные знаки или метаданные. Первые, однако, широко не используются на практике, последние не относятся к доказательствам, учитывая возможные манипуляции с ними. В отличие от этого использование программного обеспечения

для анонимизации значительно более широко распространено. В случае успеха подобной деятельности указанный факт приводит к значительному снижению ценности доказательств.

При оценке цифровых доказательств, даже если все этапы получения доказательств были соблюдены и возможность изменения файлов на предварительном расследовании была полностью исключена, не следует пренебрегать возможностью совершения манипуляций с источником информации до его изъятия.

Изложенные аргументы могут привести к выводу о том, что доказательственная ценность цифровых следов является довольно низкой. Однако некоторая доля сомнения в достоверности существует при исследовании любого доказательства. Не вызывает сомнений, например, тот факт, что даже аналоговой картинкой можно манипулировать. Если имеющаяся фотография изменяется, а затем фотографируется заново, то создается новый негатив и, следовательно, новый предполагаемый оригинал. Хотя эта процедура занимает больше времени, чем постобработка или модификация цифровой фотографии, она все же возможна. Как следствие, можно утверждать, что доказательства, имеющие цифровую природу, имеют равное значение с документарным аналогом, что должно быть зафиксировано в уголовно-процессуальном законодательстве. Однако как только возникают сомнения, они должны быть учтены в решении и, если нет дополнительных доказательств, должны привести к последовательному применению принципа In dubio pro reo.

Подводя общий итог, можно говорить о том, что для уголовного процесса существует множество сложных и нерешенных на сегодняшний день проблем в области цифровых данных. Кроме того, ввиду иногда сомнительной безопасности данных и часто трудной для понимания возможности манипулирования ими особое внимание должно быть уделено доказательственной ценности цифровых доказательств, что влияет на оценку доказательств в ходе основного слушания и вынесения судебного решения.

Digital Footprints as Evidence in the Criminal Procedure

Irina V. Chadnova, Tomsk State University (Tomsk, Russian Federation). E-rolandab@yandex.ru

Artyom V. Izvekov, Lomonosov Moscow State University (Moscow, Russian Federation). Email: Izvekofff@gmail.com

Keywords: digital footprints, procedural form, proof, proof, investigative actions.

DOI: 10.17223/9785946218566/24

Digital data has a significant potential for changing various forms of communication. Adaptation of the existing norms of criminal and criminal procedure law should fully and timely follow the development of the digital space. Therefore, it is important to find a way to include digital media and their features in the existing legal framework of the criminal justice system and thereby create standards that meet the requirements of criminal proceedings. The specificity of recording digital evidence suggests the need for an early identification of the "place" of the committed digital crime and for special tactical techniques during its examination. Of utmost importance is the full preservation of evidence. The received data must be properly protected, if necessary, a full copy of the corresponding data carrier is made. In order to use the obtained digital footprints in full, the place of digital evidence in the system of evidence in criminal proceedings must be determined. The problem with this lies in the fact that digital data are not yet taken into account in the legislation to the extent that corresponds to their practical significance. The criminal procedure lacks specific provisions that have already found their application in other branches of law. The application of Article 85 of the RF Code of Criminal Procedure when considering the possibility of classifying digital evidence as evidence contained in Article 74 of the same code seems obvious, but only in referring to the content of the data. In the list of evidence, Article 74 treats other documents as documents or conclusions by experts or specialists, that is, as thoughts already embodied on paper that can be read without prior processing. Digital evidence lacks this property. According to Part 1 of Article 17 of the RF Code of Criminal Procedure, all evidence must comply with the principle of freedom of assessment of evidence. If the guilty verdict is based on digital sources of information, the court should investigate them at a level of security sufficient to ensure that there is no doubt about the authenticity and reliability of such evidence. Today, the criminal procedure faces many complex and unsolved problems in the field of digital data. Due to the sometimes dubious security of data and the often often difficult-to-understand ability to manipulate them, special attention should be paid to the evidentiary value of digital evidence, which affects the assessment of evidence during the main hearing and adjudication.