Научная статья
УДК 343.140.02:004.63(470)

Ранис Ришатович Абдразяпов
Уфимский юридический институт МВД России, Уфа, Россия, ranis_a2009@mail.ru

ОТДЕЛЬНЫЕ ВОПРОСЫ ИСПОЛЬЗОВАНИЯ ЦИФРОВЫХ СЛЕДОВ В ДОКАЗЫВАНИИ ПО УГОЛОВНЫМ ДЕЛАМ

Аннотация. В статье рассмотрены отдельные аспекты выявления и документирования цифровых следов в ходе расследования уголовных дел. Проанализированы особенности использования цифровых следов при расследовании уголовных дел, описаны проблемные моменты, которые необходимо учитывать при работе с ними. В частности, указаны сложности выявления, документирования цифровых следов, опасность утраты следов в результате их удаления, перемещения. Предложен алгоритм действий по документированию цифрового следа, проведен анализ уголовно-процессуального законодательства в части определения места цифрового документа в числе доказательств. Рассматривая различные точки зрения, автор приходит к выводу о необходимости дополнения ч. 2 ст. 74 Уголовно-процессуального кодекса Российской Федерации новым доказательством в виде цифрового документа.

Ключевые слова: преступление, уголовное дело, уголовный процесс, цифровые следы, цифровые доказательства, доказывание

Для цитирования: Абдразяпов Р. Р. Отдельные вопросы использования цифровых следов в доказывании по уголовным делам // Общество, право, государственность: ретроспектива и перспектива. 2024. № 1 (17). С. 34–40.

Original article

Ranis R. Abdrazyapov
Ufa Law Institute of the Ministry of Internal Affairs of Russia, Ufa, Russia, ranis_a2009@mail.ru

SEPARATE ISSUES OF THE USE OF DIGITAL TRACES IN PROVING CRIMINAL CASES

Abstract. The article discusses some aspects of the identification and documentation of digital traces during the investigation of criminal cases. The features of the use of digital traces in the investigation of criminal cases are analyzed, the problematic points that need to be taken into account when working with them are described. In particular, the difficulties of identifying and documenting digital traces, the danger of losing traces as a result of their removal and relocation are indicated. An algorithm of actions for documenting a digital trace is proposed, an analysis of criminal procedure legislation is carried out in terms of determining the place of a digital document among the evidence. Considering various points of view, the author comes to the conclusion that it is necessary to supplement Part 2 of Article 74 of the Criminal Procedure Code of the Russian Federation with new evidence in the form of a digital document.

Keywords: crime, criminal case, criminal procedure, digital traces, digital evidence, proof

For citation: Abdrazyapov R. R. Separate issues of the use of digital traces in proving criminal cases // Society, law, statehood: retrospective and perspective. 2024. No. 1 (17). P. 34–40. (In Russ.)

Введение

Развитие современных технологий и техники, таких как дистанционное банковское обслуживание, сотовая связь пятого поколения, широкополосный Интернет, смарт-

фоны, которые уже сейчас не уступают персональным компьютерам, с одной стороны, облегчают повседневную жизнь населения нашей страны, но с другой стороны, они же способствуют появлению новых видов и способов совершения преступлений, о которых еще около 10 лет назад ничего не было известно. В этой связи государство в лице законодательных и исполнительных органов, понимая важность, сложность и необходимость борьбы с преступлениями, совершаемыми дистанционным способом, вводит в действующее уголовное законодательство новые составы преступлений, разрабатывает методики их раскрытия, создает различного рода и вида специализированные учеты и базы данных [1, с. 39].

Немаловажной проблемой является то обстоятельство, что в результате подобных преступных действий населению причиняется колоссальный материальный ущерб, исчисляемый миллиардами рублей. К сожалению, приходится констатировать тот факт, что преступность в данном направлении развивается намного быстрее, появляются все новые и новые способы хищений денежных средств, а государство в этом плане отстает и находится в позиции «догоняющего».

Тем не менее, преследуя цель консолидации, соединения всех усилий и возможностей по противодействию указанной категории преступлений, Министерство внутренних дел Российской Федерации в октябре 2022 г. в структуре центрального аппарата создало специализированное Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий. Оно призвано реализовывать функции головного подразделения в области борьбы с преступлениями в указанной сфере, а также противодействия распространению противоправной информации в сети Интернет. Кроме того, начиная с 2019 г. в структуре Министерства внутренних дел на региональном уровне создаются аналогичные специализированные подразделения.

Стоит также отметить, что раскрытие указанного вида преступлений в свете проведения нашей страной специальной военной операции на территории Украины стало особенно актуальным и требует практически ежедневного контроля и внимания.

Так, если в конце февраля – начале марта 2022 г., после начала проведения Специальной военной операции, количество зарегистрированных преступлений, совершаемых дистанционным способом, снизилось, что объяснялось необходимостью некоторого периода времени для передислокации так называемых «колл-центров» (место, где находятся злоумышленники, занимающиеся обзвоном населения под видом сотрудников службы безопасности банков, правоохранительных и иных органов), которые в основном располагаются на территории Украины, то уже с середины апреля регистрация преступлений вернулась на прежний уровень. По таким составам преступлений, как мошенничество с использованием сети Интернет и средств мобильной связи на протяжении нескольких месяцев наблюдался хоть и незначительный, но стабильный рост [2, с. 228].

За 2022 г. на территории Республики Башкортостан зарегистрировано 13 329 преступлений рассматриваемой категории, что на 662 больше по сравнению с 2021 г., приостановлено 9 686 преступлений, окончено всего лишь 3 245. Для сравнения: всего на территории Республики Башкортостан за указанный выше период зарегистрировано 50 751 преступление[1]; доля преступлений, совершаемых дистанционным способом, составляет 26,2 %, то есть фактически каждое 4 преступление.

Среди вопросов расследования хищений, совершаемых дистанционным способом, с которыми сталкиваются сотрудники органов внутренних дел, наиболее актуальным является проблема раскрытия дистанционных хищений. Сложность раскрытия заключается в отсутствии прямого контакта потерпевшего с преступником, невозможности надлежащей идентификации пользователя, а также в срав-

[1] Данные информационного центра МВД по Республике Башкортостан.

нительно быстром переводе безналичных денежных средств на дальние расстояния, в том числе и за границу.

Несмотря на различие способов хищений, совершаемых дистанционно, механизм следообразования имеет свою общую специфику. В первую очередь он обусловлен действиями преступника по сокрытию своих следов в сети Интернет: замена адреса пользователя, применение возможностей сервиса подменных номеров с использованием SIP-телефонии и т. д. Технологии подменных номеров позволяют злоумышленнику звонить потерпевшему с любого абонентского номера, в том числе с общеизвестных номеров, которые закреплены за правоохранительными, государственными, надзорными и иными контролирующими органами [3, с. 23]. В результате у потерпевшего создается впечатление добропорядочности звонящего.

В этой связи наибольшее значение для следователя приобретает выявление цифровых следов. В настоящее время они повсеместно используются в раскрытии и расследовании преступлений. Например, при расследовании преступлений, совершенных посредством сети Интернет, следователю необходимо выявить и изъять цифровые следы, оставленные преступником при совершении противоправного деяния. В настоящее время имеется возможность отслеживать действия пользователя в информационном пространстве, разрушая его предполагаемую скрытность и анонимность действий.

Возможность использования цифрового следа в доказывании по уголовным делам явилась темой исследования различных ученых-процессуалистов, таких как В. Ф. Васюков, Е. А. Семенов [4, с. 204], В. В. Поляков [5, с. 101], О. Г. Иванова, П. П. Недбайлов [6, с. 146], М. С. Смолин [7, с. 96] и др.

Методы

Методологическую базу исследования определяют такие общенаучные теоретические приемы (методы) исследования, как обобщение, анализ, синтез и др. Материалами исследования являются нормы Уголовно-процессуального кодекса Российской Федерации (далее – УПК РФ) и иные документы, посвященные тематике исследования, различные статистические данные, практика деятельности правоохранительных органов, а также иные материалы.

Результаты

Несмотря на очевидную востребованность в использовании цифровых следов, необходимо учитывать определенные аспекты:

Во-первых, особенностью подобных следов, находящихся в оперативной памяти устройства, на различных электронных носителях информации, а также в сети Интернет, является то, что они легко могут быть изменены, уничтожены либо распространены и иным образом трансформированы. В результате при выявлении цифровых следов следователь сталкивается с проблемой установления изначальной информации.

Однако любые уничтоженные либо измененные данные могут быть восстановлены. Это возможно в ходе производства судебных экспертиз.

Во-вторых, уголовно-процессуальный закон не содержит понятия «цифровой след». Вместе с тем, несмотря на отсутствие правовой регламентации, цифровые следы отражают событие совершенного преступления в информационной среде и имеют зачастую важное доказательственное значение.

Согласно ч. 1 ст. 74 УПК РФ, доказательствами по уголовному делу признаются «любые сведения, на основе которых устанавливается наличие или отсутствие подлежащих доказыванию при производстве по уголовному делу обстоятельств, а также иных имеющих значение для уголовного дела обстоятельств»[1]. Кроме того, уголовно-процессуальный закон содержит перечень доказательств, к числу которых относится категория «иные документы».

Несмотря на широкое использование в доказывании цифровой информации,

[1] Уголовно-процессуальный кодекс Российской Федерации : федеральный закон от 18 декабря 2001 г. № 174-ФЗ (ред. от 14.02.2024) // Доступ из справ.-правовой системы «КонсультантПлюс».

УПК РФ не дает ей определения. Указанный недостаток нормативного регулирования отрицательно сказывается на качестве деятельности органов предварительного расследования, которая по большей части является правоограничительной, а значит, не допускает вольной трактовки понятий, которые в той или иной степени затрагивают права и свободы участников уголовного процесса.

В этой связи представляется целесообразным предложение ряда ученых-процессуалистов, предлагающих дополнить УПК РФ таким понятием, как «цифровое доказательство» или «электронное доказательство» [8, с. 134].

Так, И. В. Чадаев и А. В. Извеков отмечают, что ст. 178 Гражданского процессуального кодекса Российской Федерации использует понятие «цифровые данные», имеются принятые стандарты, которые также апеллируют понятием «цифровые данные», однако уголовно-процессуальный закон такое понятие не использует. Вместе с тем авторы в своей работе констатируют, что цифровые данные подпадают под положения п. 6 ч. 2 ст. 74 УПК РФ, которые по сути выполняют функцию собирания всех потенциальных доказательств, не подпадающих под конкретно регламентированные случаи свидетельских, экспертных и документальных доказательств [9, с. 184].

Практика свидетельствует и о том, что некоторые суды относят электронные носители информации к категории иных документов[1].

В связи с тем, что рассматриваемый вопрос однозначно не решен ни на законодательном уровне, ни в практике судов, ни в доктрине, то правоприменитель сам решает, к какому источнику доказательств относить цифровые следы. Для этого он оценивает полученную доказательственную информацию, определяет ее значение для расследования преступления.

Отсутствие законодательного определения понятия «цифровое доказательство» не позволяет единообразно и четко определить сущность рассматриваемого понятия, а также перечень объектов, относящихся к нему, что в конечном итоге затрудняет практику применения цифровых следов в доказывании по уголовным делам. По мнению Ю. В. Гаврилина, «следует сформулировать определение термина так, чтобы исключить на практике его произвольную интерпретацию и подмену. Добиться этого возможно не техническим описанием понятия, а указанием на значимую для дела составляющую таких источников доказательств» [10, с. 48]. Данное высказывание имеет свою практическую значимость, однако если речь идет о «цифровом доказательстве» и оно выделяется законодателем в отдельную категорию, то все же технические понятия должны учитываться при производстве процессуальных и следственных действий.

Проведя анализ информации по исследуемой тематике, считаем, что для использования в доказывании по уголовному делу цифровые следы должны обладать следующими основными признаками:

– значимость информации для расследования конкретного уголовного дела;

– достоверность источника, из которого получена информация (возможность проверки данного источника);

– доступность информации для восприятия участниками процесса (видеозапись, скриншот сайтов и т. д.);

– фиксация (изъятие) информации в строгом соответствии с уголовно-процессуальным порядком, закрепленным действующим законодательством [11, с. 288].

Споры среди ученых-процессуалистов вызывают вопрос о месте цифровых доказательств в системе доказательств по уголовным делам. Это связано с тем, что уголовно-процессуальный закон не относит

[1] Определение Конституционного Суда Российской Федерации от 11 мая 2012 г. № 814-О // Судебные и нормативные акты Российской Федерации. URL: http://sudact.ru/regular/doc (дата обращения: 27.04.2023); Апелляционное определение Верховного Суда Российской Федерации от 4 июня 2013 г. № 41-АПУ13-13сп // Судебные и нормативные акты Российской Федерации. URL: http://sudact.ru/regular/doc. (дата обращения: 05.10.2023).

их к какому-либо конкретному источнику доказательств из перечня, указанного в ч. 2 ст. 74 УПК РФ. По мнению одних ученых, цифровые доказательства следует относить к иным документам, другие – признают их отдельным видом доказательств.

Считаем обоснованным мнения тех ученых-процессуалистов, которые предлагают выделить цифровые следы в отдельную категорию доказательств, дополнив таким образом ч. 2 ст. 74 УПК РФ еще одним пунктом.

Как отмечает в своей работе Е. А. Гамбарова, цифровые следы обладают специфичными свойствами, что не позволяет их отнести к доказательствам, которые исходят от материальных либо идеальных носителей. В этой связи цифровые следы представляют собой отдельный самостоятельный вид уголовно-процессуального доказательства [12, с. 16].

В-третьих, возникает необходимость выявления и фиксации цифровых следов, которые представлены в электронном виде и зачастую хранятся не в памяти установленного компьютера либо ином носителе информации, а на другом носителе, который может находится не в юрисдикции Российской Федерации и доступ к нему может отсутствовать [13, с. 148–153].

В настоящее время не существует единообразной практики фиксации информации, представленной в электронном виде, в материалах уголовного дела [14, с. 3]. Здесь стоит предложить следующий порядок действий: 1) проведение осмотра, например, страницы в сети Интернет посредством проверки предметов, где на компьютере выводится необходимая страница; 2) к протоколу прилагаются электронные носители информации, на которые скопирована интересующая информация с других источников, либо фиксация посредством скрин-копий страниц Интернета, видео и фотосъемки; 3) приобщение к материалам дела иных документов, полученных от операторов сотовых компаний, интернет-провайдеров.

В-четвертых, для надлежащего выявления, фиксации и изъятия цифровых следов обязательным является привлечение соответствующего специалиста, область познаний которого должна быть достаточна широка: в сфере компьютерных устройств и программирования, в области сетевого взаимодействия и эксплуатации сетевой инфраструктуры и т. п. Либо следует привлекать нескольких специалистов с углубленными познаниями в определенных областях компьютерно-информационных технологий [15, с. 182]. В этой связи следователю также необходимо обладать познаниями о работе компьютерных устройств, возможностях программирования, модификации и копировании информации.

Заключение

В заключение отметим, что цифровые следы повсеместно выявляются и изымаются в ходе расследования уголовных дел, совершенных в информационной среде, благодаря чему формируются цифровые или электронные доказательства. Складывающаяся практика использования в доказывании цифровых следов указывает на необходимость процессуальной регламентации данного процесса, так как отсутствие понятийного аппарата и установленного порядка их документирования негативно сказывается на правильности оценки правоприменителем выявленных данных. В этой связи представляется целесообразным проведение научно-исследовательских работ по указанной тематике с целью устранения пробела в уголовно-процессуальном законе.

СПИСОК ИСТОЧНИКОВ

1. Койнов М. Ю. Развитие и внедрение современных информационно-телекоммуникационных технологий и систем в повседневную деятельность органов внутренних дел // Вестник Тюменского института повышения квалификации сотрудников МВД России. 2018. № 2 (11). С. 38–43.

2. Ройтберг Л. А. Телефонное мошенничество: актуальность проблемы // Право и правопорядок в фокусе научных исследований : сборник научных трудов. Выпуск 4. Хабаровск : Дальневосточный государственный университет путей сообщения, 2023. С. 226–230.

3. Давыдов В. О., Тишутина И. В. Цифровые следы в расследовании дистанционного мошенничества // Известия Тульского государственного университета. Экономические и юридические науки. 2020. № 3. С. 20–27.

4. Васюков В. Ф., Семенов Е. А. Некоторые проблемы получения и использования цифровой информации при расследовании уголовных дел // Известия Тульского государственного университета. Экономические и юридические науки. 2016. № 3-2. С. 203–210.

5. Поляков В. В. Анализ судебной практики алтайского края по преступлениям в сфере компьютерной информации // Вестник Новосибирского государственного университета. Серия: Право. 2014. Т. 10. № 1. С. 99–103.

6. Иванова О. Г., Недбайлов П. П. Цифровая информация и ее место в уголовно-процессуальном доказывании // Вестник Сибирского юридического института МВД России. 2022. № 2 (47). С. 144–149.

7. Смолин М. С. Аспекты собирания и использования в доказывании цифровых следов // Противодействие киберпреступлениям и преступлениям в сфере высоких технологий : материалы международной научно-практической конференции. М. : Московская академия Следственного комитета Российской Федерации, 2022. С. 96–100.

8. Маслов А. В. К вопросу о статусе цифровых доказательств и электронной информации в уголовном процессе // Международный научно-исследовательский журнал. 2023. № 8 (134).

9. Чаднова И. В., Извеков А. В. Цифровые следы как доказательство в уголовном процессе // Правовые проблемы укрепления российской государственности : сборник статей / научные редакторы: О. И. Андреева, Т. В. Трубникова; отв. секретарь И. В. Чаднова. Томск, 2019. С. 181–188.

10. Гаврилин Ю. В. Электронные носители информации в уголовном судопроизводстве // Труды Академии управления МВД России. 2019. № 4 (44). С. 45–50.

11. Орлова А. А. Место электронных носителей информации в системе доказательств по уголовным делам // Молодой ученый. 2017. № 15 (149). С. 287–289.

12. Гамбарова Е. А. Изъятие цифровых следов из сети интернет и использование их в доказывании: уголовно-процессуальные аспекты // Вектор науки Тольяттинского государственного университета. Серия: Юридические науки. 2023. № 3 (54). С.13–19.

13. Демин К. Е., Васильев А. А. Криминалистические аспекты получения доказательственной информации с электронных носителей данных // Публичное и частное право. 2011. № 3(11). С. 147–161.

14. Долженко Н. И., Черкасова А. П. Цифровые следы в криминалистике: понятие и значение в расследовании преступлений, особенности обнаружения, изъятия и фиксации // Научный альманах Центрального Черноземья. 2022. № 2-4. С. 249–255.

15. Семикаленова А. И., Рядовский И. А. Использование специальных знаний при обнаружении и фиксации цифровых следов: анализ современной практики // Актуальные проблемы российского права. 2019. № 6 (103). С. 178–184.

REFERENCES

1. Koinov M. Yu. Development and implementation of modern information and telecommunication technologies and systems in the daily activities of internal affairs bodies // Bulletin of Tyumen Institute for Advanced Training of Employees of the Ministry of Internal Affairs of Russia. 2018. No. 2 (11). P. 38–43. (In Russ.)

2. Roytberg L. A. Telephone fraud: relevance of the problem // Law and order in the focus of scientific research : collection of scientific papers. Issue 4. Khabarovsk : Far Eastern State Transport University, 2023. P. 226–230. (In Russ.)

3. Davydov V. O., Tishutina I. V. Digital traces in the investigation of remote fraud // News of Tula State University. Economic and legal sciences. 2020. No. 3. P. 20–27. (In Russ.)

4. Vasyukov V. F., Semenov E. A. Some problems of obtaining and using digital information in the investigation of criminal cases // News of Tula State University. Economic and legal sciences. 2016. No. 3-2. P. 203–210. (In Russ.)

5. Polyakov V. V. Analysis of judicial practice of the Altai region on crimes in the field of computer information // Bulletin of Novosibirsk State University. Series: Law. 2014. Vol. 10. No. 1. P. 99–103. (In Russ.)

6. Ivanova O. G., Nedbailov P. P. Digital information and its place in criminal procedural evidence // Bulletin of the Siberian Law Institute of the Ministry of Internal Affairs of Russia. 2022. No. 2 (47). P. 144–149. (In Russ.)

7. Smolin M. S. Aspects of collection and use in proving digital traces // Combating cybercrimes and crimes in the field of high technologies: Proceedings of the international scientific and practical conference. M. : Moscow Academy of the Investigative Committee of the Russian Federation, 2022. P. 96–100. (In Russ.)

8. Maslov A. V. On the issue of the status of digital evidence and electronic information in criminal proceedings // International scientific research journal. 2023. No. 8 (134). (In Russ.)

9. Chadnova I. V., Izvekov A. V. Digital traces as evidence in criminal proceedings // Legal problems of strengthening Russian statehood : collection of articles / Scientific editors: O. I. Andreeva, T. V. Trubnikova. Exec. Secretary I. V. Chadnova. Tomsk, 2019. P. 181–188. (In Russ.)

10. Gavrilin Yu. V. Electronic media in criminal proceedings // Proceedings of the Academy of Management of the Ministry of Internal Affairs of Russia. 2019. No. 4 (44). P. 45–50. (In Russ.)

11. Orlova A. A. The place of electronic storage media in the system of evidence in criminal cases // Young scientist. 2017. No. 15 (149). P. 287–289. (In Russ.)

12. Gambarova E. A. Removal of digital traces from the Internet and their use in proof: criminal procedural aspects // Vector of science of Togliatti State University. Series: Legal sciences. 2023. No. 3 (54). P. 13–19. (In Russ.)

13. Demin K. E., Vasiliev A. A. Forensic aspects of obtaining evidentiary information from electronic data carriers // Public and private law. 2011. No. 3 (11). P. 147–161. (In Russ.)

14. Dolzhenko N. I., Cherkasova A. P. Digital traces in forensics: concept and significance in the investigation of crimes, features of detection, seizure and recording // Scientific almanac of the Central Chernozem Region. 2022. No. 2-4. P. 249–255. (In Russ.)

15. Semikalenova A. I., Ryadovsky I. A. The use of special knowledge in detecting and recording digital traces: analysis of modern practice // Current problems of Russian law. 2019. No. 6 (103). P. 178–184. (In Russ.)

Информация об авторе:
Абдразяпов Р. Р. – кандидат юридических наук.

Information about the author:
Abdrazyapov R. R. – Candidate of Law.

Статья поступила в редакцию 02.10.2023; одобрена после рецензирования 25.10.2023; принята к публикации 21.03.2024.

The article was submitted 02.10.2023; approved after reviewing 25.10.2023; accepted for publication 21.03.2024.