УДК/UDC 343.1

Использование цифровой информации в доказывании при расследовании преступлений

Тарасов Анатолий Вячеславович
кандидат юридических наук, доцент, заслуженный юрист Кубани
Северо-Кавказский филиал Российского государственного университета правосудия
г. Краснодар, Россия
e-mail: tarasov-av@mail.ru

Аннотация

В статье затронуты основные проблемы использования цифровых технологий в расследовании преступлений. Рассматриваются возможности цифровых технологий для фиксации следов преступлений и доказывания в уголовном судопроизводстве. Отмечается, что, хотя правоприменитель стал широко использовать технические (электронные) средства в повседневной жизни, законодатель оставил вне поля правового регулирования целый ряд вопросов, возникающих в ходе применения этих средств. Наиболее актуальными проблемами применения цифровых технологий в расследовании преступлений являются легализация оперативно-розыскной цифровой информации, надлежащая фиксация результатов оперативно-розыскных мероприятий, изъятие электронных носителей информации при проведении следственных действий с точки зрения участия в них специалиста. Также обращается внимание на отсутствие закрепления ряда фундаментальных понятий в уголовно-процессуальном законодательстве. Автор приходит к выводу о том, что рассматриваемый институт требует дальнейшего осмысления и совершенствования со стороны законодателя.

Ключевые слова: цифровые технологии, интернет, следы преступления, цифровые средства фиксации, оперативно-розыскная деятельность, расследование преступлений.

Digital information in evidence in the investigation of crimes

Tarasov Anatoliy Vyacheslavovich
Candidate of Law, assistant professor, honored lawyer of Kuban
North Caucasus branch of the Russian State University of Justice
Krasnodar, Russia
e-mail: tarasov-av@mail.ru

Abstract

The article touches upon the main problems of using digital technologies in the investigation of crimes. The possibilities of digital technologies for fixing traces of crimes and proving them in criminal proceedings are considered. It is noted that, although the law enforcement officer began to widely use technical (electronic) means in everyday life, the legislator left outside the field of legal regulation a number of issues that arise in the course of the use of these means. The most pressing problems of the use of digital technologies in the investigation of crimes are the legalization of operational-investigative digital information, the proper recording of the results of operational-search activities, the seizure of electronic media during investigative actions from the point of view of the participation of a specialist in them. Attention is also drawn to the lack of consolidation of a number of fundamental concepts in the criminal procedure legislation. The author comes to the conclusion that the institution under consideration requires further understanding and improvement on the part of the legislator.

Key words: digital technologies, Internet, traces of crimes, digital means of fixation, operational investigations, crime investigation.

В современных условиях развития России, которые характеризуются внедрением во все области права новейших технологий, инновацией существующих систем, глобальной информатизацией общества, особо остро встает вопрос о применении в качестве доказательств информации с электронных носителей (далее по тексту - цифровая информация).

Казалось бы, технические средства к 2020 г. стали постоянными спутниками современного человека. Ежедневно общество тратит несколько часов на общение в социальных сетях, мессенджерах, по теле-

фону. В этом огромном информационным потоке, к сожалению, совершаются преступления. Все это, безусловно, должно включаться в процесс доказывания.

Тем не менее законодательство в этой части несовершенно: правоприменитель стал широко использовать технические средства, особенно электронные, а законодатель оставил вне поля правового регулирования целый ряд вопросов, возникающих в ходе применения этих средств. Создается впечатление, что законодатель недооценивает возможности, позволяющие эффективно применять названные средства с целью получения доказательств и для уголовно-процессуального доказывания. Ввиду этого не вызывает сомнения актуальность рассматриваемых вопросов в части существующих пробелов в законодательстве.

В первую очередь существенным пробелом является легализация оперативно-розыскной цифровой информации. Предлагаем рассмотреть ее на примере прослушивания телефонных переговоров.

Так, еще в 2016 г. в ст. 6 Федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» [1] (далее по тексту - Закон «Об ОРД») был введен новый пункт - «Получение компьютерной информации».

На сегодняшний день в соответствии с Федеральным законом от 6 июля 2016 г. № 374-ФЗ «О внесении изменений в Федеральный закон "О противодействии терроризму"и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» [2] и 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» [3], внесшими изменения в Федеральный закон от 7 июля 2003 г. №126 «О связи» [4] (далее по тексту - Закон «О связи»), в закон «Об ОРД», и еще в ряд нормативных правовых актов, вся цифровая информация аккумулируется у провайдеров. Так, информация о

любых соединениях между абонентами хранится в течение трех лет, а сама звуковая информация - в течение шести месяцев.

Ст. 64 Закона «О связи» регламентирует, что операторы связи обязаны при необходимости предоставлять цифровую информацию (текстовые сообщения, изображения, звуки, видео и иные сообщения пользователей услугами связи) уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность.

Также в 2019 г. были внесены изменения в ст. 8 Закона «Об ОРД», согласно которым при соблюдении определенных условий «допускается получение информации о соединениях абонентского устройства, находящегося у несовершеннолетнего, с иными абонентами и (или) их абонентскими устройствами, иным оборудованием, а также о местоположении данного абонентского устройства путем снятия информации с технических каналов связи с обязательным уведомлением суда (судьи) в течение 24 часов».

Таким образом, законодатель в целом регламентировал осуществление оперативно-розыскной деятельности в этой части и получение от операторов связи необходимых данных. Но логично возникает вопрос о способе использования таких данных (например, результатов прослушивания телефонных переговоров) в тех случаях, когда латентное преступление совершается «сегодня», а, допустим, цифровая информация, которую необходимо получить, появилась «до» (например, когда происходила подготовка к преступлению). Или в части таких составов, как мошенничество или коррупционные преступления, которые в принципе по своей природе латентные (ведь они могут быть скрыты на протяжении полугода или даже больше).

Как нами уже было отмечено ранее, цифровая информация о таких преступлениях также хранится. Но возникает парадокс в следующей части: если преступление расследуется в настоящее время, то согласно Уголовно-процессуальному кодексу Российской Федерации (далее по тексту - УПК РФ) [5] следователь в судебном порядке получает судебное решение на прослушивание телефонных переговоров и, например, про-

слушивает цифровую информацию за шесть месяцев (уголовное дело в таком случае уже возбуждено). Оперативные подразделения также могут совершать подобные действия в рамках оперативно-розыскных мероприятий, но только на основании судебного решения, а затем передавать рассекреченные прослушанные телефонные переговоры следователю, который приобщает их к материалам дела, и они облачаются в доказательственную базу. В таких случаях цифровые доказательства законны.

Но как быть в ситуации, когда ни следователь, ни оперативные подразделения к суду не обращались, у них нет разрешения на прослушивание, но они знают, что цифровая информация сохранена на серверах и могут в течение шести месяцев получить эту информацию и прослушать. Как узаконить такую информацию? Ведь на тот момент судебного решения на прослушивание этих телефонов не было, а был лишь закон, упомянутый выше, обязывающий всех провайдеров сохранять такую информацию.

Таким образом, на сегодняшний момент складывается ситуация, когда определенная оперативно-розыскная информация не может быть легализована, поскольку ст. 89 УПК РФ регламентирует запрет использования результатов оперативно-розыскной деятельности, если они не отвечают требованиям, предъявляемым к доказательствам.

Получается, что вышеуказанная возможность правоохранительных органов порой нивелируется УПК РФ, запрещающим использовать полученные результаты в качестве доказательств. Ведь непонятно, каким образом правоохранительным органам соблюсти все требования к доказательствам в так называемых неотложных ситуациях, когда медлить, например, с прослушиванием телефонных переговоров нельзя (когда они прослушиваются без решения суда).

Складывается судебная практика, согласно которой все полученные при проведении оперативно-розыскных мероприятий данные остаются лишь оперативно-значимой информацией, которую не представляется возможным легализовать. Так, например, в кассации приговор по уголовному делу был изменен: телефонные переговоры двух осужден-

ных исключены как недопустимые доказательства (как раз потому, что разрешалось прослушивать их переговоры только с момента вынесения постановлений, но не содержалось решение о законности и обоснованности уже проведенных «неотложных» мероприятий [6]).

Еще одним нерегламентированным законодателем моментом является надлежащая фиксация результатов оперативно-розыскных мероприятий.

Так, отсутствуют требования к технике, с помощью которой обеспечивается запись прослушиваемых телефонных переговоров, а также к носителям такой информации. Лишь в ст. 8 Закона «Об ОРД» закрепляется требование, согласно которому «фонограммы, полученные в результате прослушивания телефонных и иных переговоров, хранятся в опечатанном виде в условиях, исключающих возможность их прослушивания и тиражирования посторонними лицами». Но, по нашему мнению, указанной нормы в этом вопросе недостаточно.

Интересным также представляется рассмотрение проблемы изъятия электронных носителей информации при проведении следственных действий с точки зрения участия в них специалиста.

Согласно ч. 2 ст. 164.1 УПК РФ электронные носители информации изымаются в ходе производства следственных действий с участием специалиста. Законодатель исходил из необходимости использования специальных знаний, однако на практике следователь вполне успешно справляется с этой задачей самостоятельно. Таким образом, зачастую указанная норма приводит к формальным нарушениям процедуры изъятия электронных носителей.

Целесообразным является внесение изменений в УПК РФ, согласно которым следователь вправе самостоятельно определять необходимость привлечения специалиста в каждом конкретном случае.

Заключительным пробелом, на наш взгляд, является недостаточность дефинитивного «фундамента» в УПК РФ, что в т. ч. сильнейшим образом тормозит и разработку вышеуказанных вопросов. Ведь в УПК

РФ легальное определение понятий «технические средства», «электронные носители» отсутствует.

Безусловно, ст. 2 Закона «О связи» вносит ясность в эти вопросы понятием «средства связи». А в п. 2 ст. 138.1 Уголовного кодекса Российской Федерации [7] дается определение понятию «специальные технические средства, предназначенные для получения негласной информации». А в Указе Президента Российской Федерации от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 гг.» [8] даются определения понятий «информационное пространство», «технологически независимые программное обеспечение и сервис» и «сети связи нового поколения».

Тем не менее в УПК РФ понятийный аппарат не аккумулируется для наиболее точного понимания рассматриваемых вопросов, что является недостаточным для правового регулирования.

Можно сделать вывод о том, что размытость понятий порождает некорректность права, а такое неоднородное понимание в совокупности с отсутствием соответствующего регламентирования, на наш взгляд, сдерживает эффективное применение технических средств и электронных носителей на практике.

Электронное доказывание сейчас находится «в стадии осмысления и теоретического обоснования» [9]. При этом согласно статистическим данным, предоставленным на официальном сайте Генеральной прокуратуры Российской Федерации, только в 2017 г. число преступлений в сфере информационно-телекоммуникационных технологий увеличилось с 65 949 до 90 587. Их доля от числа всех зарегистрированных в России преступных деяний составляет 4,4% — это почти каждое 20-е преступление. Если в 2017 г. зарегистрировано 1 883 таких преступления (+7,7%), то за 2018 г. — около 2500 (+6%). При этом на 19,6% уменьшилось количество расследованных преступлений по указанным статьям (с 903 до 726), выросло на 30,5% (с 790 до 1031) число нераскрытых преступлений [10].

Следует согласиться с точкой зрения А. Е. Федюнина, полагающего, что отсутствие законодательно закрепленных понятий технических средств и электронных носителей не только влечет за собой неясность нормативно-правовых формулировок, но и негативно сказывается на качестве дознания, предварительного следствия и судебного разбирательства уголовных дел [11].

Суть вышеизложенного сводится к тому, что рассматриваемый институт требует дальнейшего осмысления, ведь, как совершенно справедливо отмечал В. Д. Зорькин, нельзя оторвать нормотворчество от правоприменения — это две стороны одной медали [12].

Список литературы

1. Об оперативно-розыскной деятельности: Федеральный закон от 12.08.1995 № 144-ФЗ // Собрание законодательства РФ.14.08.1995. № 33. Ст. 3349.

2. О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности: Федеральный закон от 06.07.2016 № 374-ФЗ // Собрание законодательства РФ. 2016. № 28. Ст. 4558.

3. 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: Федеральный закон от 06.07.2016 № 375-ФЗ // Собрание законодательства РФ. 2016. № 28. Ст. 4559.

4. О связи: Федеральный закон от 07.07.2003 № 126-ФЗ (ред. от 01.11.2019) // Собрание законодательства РФ. 14.07.2003. № 28. Ст. 2895.

5. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 18.02.2020) // Собрание законодательства РФ. 24.12.200.1 № 52 (часть I). Ст. 492.

6. Кассационное определение Верховного Суда РФ от 13.12.2012 № 48-О12-110 // СПС «Гарант». URL: http://www.garant.ru/products/ipo/prime/doc/70201682/ (дата обращения: 08.03.2021).

7. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 18.02.2020) // Собрание законодательства РФ. 17.06.1996. № 25. Ст. 2954.

8. О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: Указ Президента РФ от 09.05.2017 № 203 // Собрание законодательства РФ. 15.05.2017. № 20. Ст. 2901.

9. Григорьев В. Н. Результаты смены парадигмы в исследованиях уголовного процесса // Вестник ВИПК МВД России. 2017. № 2 (42). С. 38–46.

10. О преступлениях, совершаемых с использованием современных информаци онно-коммуникационных технологий // Официальный сайт Генеральной прокуратуры РФ. URL: https://genproc.gov.ru/smi/news/genproc/news-1431104/ (дата обращения: 08.03.2021).

11. Федюнин А. Е. Правовое регулирование технических средств в уголовном процессе: автореф. дисс. ... д-ра юрид. наук. Саратов: СЮИ МВД России, 2008. 390 с. С. 36.

12. Зорькин В. Д. Правоприменение как стратегическая проблема // Право и правоприменение в России: междисциплинарные исследования / Под ред. В. В. Волкова. М.: Статут, 2011. С. 15–24. С. 20.

References

1. On operational-search activity: Federal Law of 12.08.1995 No. 144-FZ // Collected Legislation of the Russian Federation. No. 33. Art. 3349.

2. On amendments to the Federal Law "On Countering Terrorism"and certain legislative acts of the Russian Federation in terms of establishing additional measures to counter terrorism and ensuring public safety: Federal Law of 06.07.2016 No. 374-FZ // Collected Legislation of the Russian Federation. 2016. No. 28. Art. 4558.

3. On amendments to the Criminal Code of the Russian Federation and the Criminal Procedure Code of the Russian Federation in terms of establishing additional measures to counter terrorism and ensure public safety: Federal Law of 06.07.2016 No. 375-FZ // Collected Legislation of the Russian Federation. 2016. No. 28. Art. 4559.

4. On communication: Federal Law of 07.07.2003 No. 126-FZ (as amended on 01.11.2019) // Collected Legislation of the Russian Federation. July 14, 2003. No. 28. Art. 2895.

5. The Criminal Procedure Code of the Russian Federation of December 18, 2001 No. 174-FZ (as amended on February 18, 2020) // Collected Legislation of the Russian Federation. 12.24.200.1 No. 52 (Part I). Art. 492.

6. The cassation ruling of the Supreme Court of the Russian Federation dated 13.12.2012 No. 48-O12-110 // Garant. URL: http://www.garant.ru/products/ipo/prime/doc/70201682/ (date of access: 08.03.2021).

7. The Criminal Code of the Russian Federation of 13.06.1996 No. 63-FZ (as amended on 18.02.2020) // Collected Legislation of the Russian Federation. 17.07.1996. No. 25. Art. 2954.

8. On the Strategy for the Development of the Information Society in the Russian Federation for 2017–2030: Decree of the President of the Russian Federation dated 09.05.2017 No. 203 // Collected Legislation of the Russian Federation. 15.05.2017. No. 20. Art. 2901.

9. Grigoriev V. N. The results of the paradigm shift in the research of the criminal process // Bulletin of the VIPK Ministry of Internal Affairs of Russia. 2017. No. 2 (42). Pp. 38–46.

10. On crimes committed with the use of modern information and communication technologies // Official site of the General Prosecutor's Office of the Russian Federation. URL: https://genproc.gov.ru/smi/news/genproc/news-1431104/ (date of accessed: 08.03.2021).

11. Fedyunin A. E. Legal regulation of technical means in criminal proceedings: author. diss. ... Dr. legal sciences. Saratov: SUI Ministry of Internal Affairs of Russia, 2008. 390 p. P. 36.

12. Zorkin V. D. Law enforcement as a strategic problem // Law and law enforcement in Russia: interdisciplinary research / Ed. V. V. Volkov. Moscow: Statut, 2011. Pp. 15–24. P. 20.