УДК: 343.14; 343.985
DOI: 10.24411/2312-3184-2019-10037

Родивилина Виктория Александровна
доцент кафедры криминалистики
Восточно-Сибирского института
МВД России
кандидат юридических наук
E-mail: 377b@bk.ru

Rodivilina Victoria Aleksandrovna
Associate Professor of the Department
of Criminalistics East-Siberian Institute
of the Ministry of Internal Affairs of Russia
Candidate of Law
E-mail: 377b@bk.ru

Цуканов Николай Николаевич
заместитель начальника Сибирского
юридического института МВД России
(по научной работе)
доктор юридических наук, доцент

Tsukanov Nikolay Nikolaevich
Deputy Head of the Siberian Law Institute
of the Ministry of Internal Affairs of Russia
(for scientific work)
Doctor of Law, Associate Professor

ИЗЪЯТИЕ И ОСМОТР МОБИЛЬНОГО ТЕЛЕФОНА КАК ЭЛЕКТРОННОГО НОСИТЕЛЯ ИНФОРМАЦИИ

Введение: средства телекоммуникации в настоящее время являются неотъемлемой частью жизнедеятельности любого человека и умеют хранить и передавать всевозможные виды информации. Само устройство может стать источником получения следов преступления, выяснения других обстоятельств, имеющих значение для уголовного дела.

Материалы и методы: нормативную основу исследования образуют Конституция Российской Федерации, уголовно-процессуальное законодательство, локальные нормативные акты. Методологическую основу исследования составил общий диалектический метод научного познания, позволивший полно и всесторонне рассмотреть особенности проведения следственных действий, в ходе которых возможно изъятие телекоммуникационных технических средств. Также использовались методы логической дедукции, индукции, познавательные методы и приемы наблюдения, сравнения, анализа, обобщения и описания.

Результаты исследования: в статье анализируются криминалистические и процессуальные аспекты осмотра мобильных телефонов. Даются отдельные рекомендации по тактике проведения изъятия и осмотра телекоммуникационных средств,

рассматриваются общие требования и основания для проведения осмотра мобильных телефонов. Акцентируется внимание на тайне переписки и телефонных переговоров.

Выводы и заключения: авторы обращают внимание на пробелы в уголовно-процессуальном законодательстве и некоторые неточности, требующие устранения.

Ключевые слова: технические средства, телекоммуникационные средства, электронные доказательства, электронный носитель информации, цифровая информация, тайна переписки и телефонных переговоров, следственные действия, изъятие информации.

SEIZURE AND INSPECTION OF MOBILE PHONE AS ELECTRONIC INFORMATION MEDIUM

Introduction: Telecommunications is now an integral part of any person's life and is able to store and transmit all kinds of information. The device itself can become a source of traces of crime, clarification of other circumstances relevant to the criminal case.

Materials and methods: the normative basis of the study is formed by the Constitution of the Russian Federation, criminal procedure legislation, local normative acts. The methodological basis of the study was the general dialectical method of scientific knowledge, which allowed fully and comprehensive considering of the peculiarities to carry out investigative actions, during which it is possible to remove telecommunication technical means, as well as in what cases it is possible to examine them, the need to obtain a court decision for this purpose. Methods of logical derivation, induction, cognitive methods and techniques of observation, comparison, analysis, generalization and description were also used.

Results of the study: the article analyses the forensic and procedural aspects of mobile phone inspection. Several recommendations are made on tactics for the seizure and inspection of telecommunications equipment, and general requirements and grounds for the inspection of mobile phones are considered. Emphasis is placed on the secrecy of correspondence and telephone conversations.

Conclusions and conclusions: the authors draw attention to gaps in criminal procedure legislation and some inaccuracies that need to be addressed.

Key words: technical means, telecommunication means, electronic evidence, electronic information medium, digital information, secret of correspondence and telephone conversations, investigative actions, seizure of information.

Технический прогресс и его результаты перестали быть исключительной прерогативой государства, военных, космических и иных высокотехнологичных структур, получив широкое распространение в быту. Сейчас практически каждый человек

имеет собственный смартфон, представляющий собой современное вычислительное устройство, снабженное мощным аппаратным комплексом и сложным программным обеспечением. Значение мобильного устройства для коммуникации и ведения дел вовлекло его в социальные процессы.

Мобильный телефон, изначально предназначенный для голосовых звонков и обмена короткими текстовыми сообщениями, сейчас умеет хранить всевозможные виды информации, создавать и воспроизводить текстовые, графические, аудио- и видеофайлы, передавать информацию по различным каналам: электронной почте, мессенджерам и т.д. Он постоянно соединяется через сеть Интернет со всевозможными серверами, отправляя на них и получая с них информацию. Разнообразные приложения позволяют не только общаться, но и вести финансовые дела, управлять счетами в банках, использовать устройство для оплаты и получения платежей.

Как верно отметила Е.И. Третьякова, в настоящее время «средство мобильной связи становится чаще всего не предметом преступного посягательства, а средством его совершения. И в этом случае наибольший интерес представляет не сам предмет с его внешними индивидуальными характеристиками, а информация, хранящаяся в его памяти» [9, с. 49].

Все это породило всевозможные сценарии использования мобильных устройств и вполне логично, что часть из этих сценариев – криминальные. Соответственно, само устройство может стать источником получения информации о совершенном или готовящемся преступлении, а также собрать интересующие правоохранительные органы сведения о лице и его действиях [10]. Как показывает статистика, мобильные устройства чаще всего становятся орудиями совершения мошенничеств, преступлений в сфере компьютерной информации, используются при незаконном обороте наркотических средств и психотропных веществ.

Законодательство по мере развития научно-технического прогресса, совершенствования компьютерной техники, появления новых видов коммуникаций между людьми включало все новые и новые виды правовых средств, направленных на использование информационных технологий для собирания доказательственной цифровой информации. Особенно это проявляется в сфере развития телефонной связи, электронного наблюдения, геолокации и геоинформационных систем, аналитической деятельности при добывании информации в компьютерных сетях и всевозможных базах данных.

Информационная природа электронных средств доказывания состоит в том, что сведения в них представлены в форме особого вида информации – цифровой информации, т.е. сведений, закодированных в двоичной системе исчисления и передаваемых посредством сигналов, не воспринимаемых человеком непосредственно.

Правоохранительные органы, осознавая высокую криминалистическую значимость информации, которую можно получить с мобильного устройства, уделяют им особое внимание. В то же время, по замечанию Н.А. Архиповой «практические работники нередко недооценивают технические возможности средств сотовой связи по

хранению в них текстовой, звуковой информации, фото- и видеозаписей, сведений о входящих и исходящих телефонных номерах, содержание SMS-, EMS-, MMS-сообщений, что приводит к сужению доказательственной базы уголовного дела» [1, с. 16].

Изъятие телекоммуникационных средств связи возможно при таких следственных действиях, как осмотр места происшествия, жилища, помещений, выемка, обыск, личный обыск. Отметим, что для производства осмотра жилища при отсутствии согласия проживающих в нем лиц, обыска и выемки в жилище, выемки в ломбарде, личного обыска (за исключением личного обыска задержанного) требуется разрешение суда, либо после их производства в случаях, не терпящих отлагательств, суд проверяет законность произведенного следственного действия и выносит постановление о его законности или незаконности. Следовательно, судебное решение на осмотр информации о соединениях абонентских устройств, если оно получено в ходе одного из перечисленных следственных действий, следователю (дознавателю) получать не надо, равно как и при извлечении данных из записной книжки, заметок в календаре.

Аналогичную позицию занимает и Верховный суд Российской Федерации. Так, рассматривая кассационные жалобы на приговор Верховного суда Республики Хакасия, в которых среди прочего говорилось, что осмотр изъятого у осужденного мобильного телефона, содержащего данные о его телефонных переговорах, проведен с нарушением закона ввиду отсутствия судебного решения, Верховный суд РФ указал, что осмотр мобильного телефона проведен следователем в соответствии со ст. 176 УПК РФ и для этого не требовалось судебного решения [4].

На месте обнаружения мобильного устройства, прежде всего, следует предпринять действия, исключающие утрату возможных доказательств. Для этого следователю необходимо:

– исключать прикосновение к мобильным устройствам других участников следственного действия, а также посторонних лиц, выключение устройств;

– при осмотре устройства не совершать действий, результат которых следователю не известен;

– мобильное устройство следует перенести в помещение, в котором будет исключено воздействие на него посторонних веществ, материалов и излучений.

Мобильные устройства, с помощью которых совершаются преступления в сфере информационных технологий, оставляют специфические следы, на поиск которых должна быть ориентирована деятельность следователя.

Условно эти следы можно разделить на следующие виды:

– электронные динамические следы, т. е. следы о времени, частоте, характере и содержании соединения с другими абонентами или устройствами (серверами);

– электронные следы на устройстве, т. е. записи в телефонных книгах, заметках, справочниках, фотографии, электронные файлы, установленные программы и т.д.;

– следы на SIM-карте, т. е. физические и электронные следы, оставленные непосредственно на чипе карты или в его памяти.

В настоящее время единого мнения о том, в каком состоянии следует изымать устройство (включенном или выключенном), нет. Так, О.С, Бутенко и В.А. Расчетов рекомендуют в том случае, если к моменту осмотра телефон был включен, проводить конструктивный осмотр только после изучения его информационной среды (включает изучение и фиксацию сведений, которые содержатся в памяти мобильного телефона, флеш-карты, SIM-карты) [2, с. 30]. А.Н. Архипова установила, что электронные устройства чаще всего изымаются в выключенном состоянии. Она дает рекомендации о том, что в ходе осмотра места происшествия, осмотра помещений или участка местности, а также обыска и выемки устройство следует описать и сфотографировать во включенном состоянии, после чего отключить и изъять в выключенном состоянии. Она указывает, что это позволит сохранить информацию, хранящуюся в устройстве, от уничтожения [1, с. 17]. Это связано с тем, что современные устройства постоянно сопряжены с удаленными серверами и пользователь имеет возможность управлять находящейся в устройствах информацией – модифицировать ее, блокировать или уничтожать. В частности, такая функция является базовой для всех устройств под управлением OS Android и iOS. Г.В. Семенов дает противоположные рекомендации, указывая, что «в случае изъятия мобильного устройства не следует отключать его, так как при дальнейшем включении могут возникнуть проблемы с разблокировкой, которые необходимы для работы мобильного устройства и соответственно исследования его содержимого» [5, с. 47]. Думается, позиция А.Н. Архиповой более правильная. Несмотря на то, что при последующем включении устройство, вероятно потребует введения PIN-кода и иных средств, обойти их с применением современных программных и аппаратных средств не так сложно. По крайней мере, риск утраты информации в результате удаленного доступа пользователя гораздо выше, чем риск от возможного блокирования устройства при его выключении.

Идеальным решением следует признать помещение устройства во включенном состоянии в такое помещение или упаковку, которое бы исключало соединение его с сетью, любо включение в работу специального устройства, блокирующего действие сотовой связи в периметре нахождения устройства.

Отметим, что электронная почта изымается по правилам общей выемки (ч. 3^1 ст. 183 УПК РФ) или по правилам обыска (ч. 9^1 ст. 182 УПК РФ). Исключение составляет дипломатическая почта, в отношении которой применяется особый правовой режим, вытекающий из иммунитета дипломатических и консульских представительств иностранных государств, находящихся на территории России.

Как верно отмечено К.А. Виноградовой и Л.А. Савиной, при анализе законодательства «у следователя нет возможности проводить осмотр электронных устройств и электронной информации в качестве самостоятельного следственного действия» [3, с. 58]. Поэтому все, что ему остается – проводить осмотр предметов.

Мобильное устройство, представляющее собой сложный аппаратно-программный комплекс, подлежит осмотру, как и любой другой предмет, в порядке ст. ст. 176–180 УПК РФ. Отличие осмотра обычных предметов от осмотра мобильных устройств заключается в том, что основная часть информации не может быть воспри-

нята непосредственно, с помощью человеческих органов чувств, в связи с чем для этих целей используются специальные технические приспособления и программное обеспечение.

Применение программного комплекса «Мобильный криминалист», программно-аппаратных комплексов Ufed touch logical (UFED), CellXtract и других фактически представляет собой не осмотр в привычном его понимании, а осмотр с элементами криминалистического исследования. В этой связи, например, Н.Н. Федоров вообще утверждает, что следует проводить не осмотр, а экспертизу мобильного устройства [7, с. 21]. С.Ю. Скобелин утверждает, что осмотр предполагает собирание доказательств путем непосредственного внешнего наблюдения за объектом. А при использовании специальных устройств исследуется содержимое памяти устройства, восстанавливается удаленная информация, что уже ближе не к внешнему осмотру, а к компьютерно-техническому исследованию. Осмотру скорее должна подлежать сводка об извлечении, полученная в результате использования специальных знаний и устройств, а не сам телефон [6, с. 90]. Не согласимся с данной точкой зрения и в качестве аргументации проведем следующую аналогию: при использовании осветительного фонарика в ходе осмотра в темном месте видны следы, которые невозможно увидеть при непосредственном внешнем наблюдении. Так и «удаленные» электронные документы, которые на самом деле лишь называются так операционной системой, видны при восстановлении с помощью различных программ. Организационные сложности, связанные, прежде всего, с загруженностью работы экспертов и утратой в связи с этим оперативности расследования, требуют от следователя самостоятельности при получении информации с изъятых устройств. Таким образом, считаем, что следует проводить осмотр телекоммуникационных устройств.

Под осмотром понимается деятельность следователя, осуществляемая им в предусмотренном УПК РФ порядке, в ходе которого осуществляется обнаружение, выяснение и фиксация обстоятельств, которые имеют значение для уголовного дела.

В качестве процессуальной гарантии законного и обоснованного вмешательства правоохранительных органов в частную жизнь граждан и в связанные с ней тайны, в Конституции РФ установлено получение судебного разрешения на ограничение права на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (ст. 23), проникновение в жилище против воли проживающих в нем лиц (ст. 25).

Перед проведением осмотра мобильного устройства следует получить согласие его владельца или судебное разрешение, так как содержащаяся в нем информация составляет тайну переписки и личной жизни его владельца. Как правило, обвиняемые и подозреваемые против такого действия, в связи с этим судебное разрешение становится обязательно. Потерпевшие, напротив, как правило, дают такое согласие. В том случае, если владелец устройства не установлен, следует получить судебное разрешение в установленном порядке. В противном случае полученные сведения могут быть признаны недопустимыми доказательствами.

Понятые и другие участники осмотра должны быть предупреждены о недопу-

стимости разглашения сведений, полученных в ходе исследования мобильного устройства. Как совершенно верно предлагает И.В. Смолькова, в таких случаях следует отбирать подписку у понятых о неразглашении данных предварительного расследования и привлекать к участию в качестве понятых тех лиц, которые не являются знакомыми [8, с. 167] с лицами, которым принадлежит средство телекоммуникации.

Все производимые в ходе осмотра действия, а также получаемая информация в соответствии с требованиями УПК РФ должны быть зафиксированы в протоколе осмотра.

Обобщая теоретический и практический опыт, отметим, что в настоящее время имеются пробелы и некоторые неточности в законодательстве, из-за которых совершаются ошибки, приводящие к недопустимости доказательств и нарушению конституционных прав граждан. Имеется необходимость во внесении изменений в уголовно-процессуальное законодательство с учетом технического прогресса, с работой с электронной (цифровой) информацией.

БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ

1. Архипова Н.А. К вопросу об использовании возможностей средств мобильной связи в раскрытии и расследовании преступлений // Криминалистические чтения: сб. материалов / Барнаульский юрид. институт МВД России. – 2014. – № 10. – С. 16–17.

2. Бутенко О.С., Расчетов В.А. Возможности изучения мобильных телефонов в рамках предварительного следствия // Современные инновации: актуальные направления научных исследований: сб. науч. трудов по мат-лам VII междунар. науч.-практич. конф. – М.: Проблемы науки, 2017. – С. 30–32.

3. Виноградова К.А., Савина Л.А. Изъятие и осмотр мобильных телефонов и находящейся на них электронной информации по преступлениям, совершенным военнослужащими // Вестник военного права. – 2019. – № 2. – С. 55–58.

4. Об отказе в принятии к рассмотрению жалобы гр-на Т.Н. Алексеевича на нарушение его конституционных прав ч. 1 ст. 176 и ч. 1 ст. 285 УПК РФ: определение Конституционного суда Российской Федерации от 8 апр. 2010 г. № 433-0-0 (Извлечение) //СПС «Консультант Плюс» (дата обращения 11.08.2019).

5. Семенов Г.В. Расследование преступлений в сфере мобильных телекоммуникаций: монография. – М.: Юрлитинформ, 2008. – 336 с.

6. Скобелин С.Ю. Возможности получения криминалистически значимой информации при осмотре мобильных средств связи и пределы ограничения конституционных прав граждан на тайну переписки // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. – Воронеж, 2017. – № 1. – С. 89–98.

7. Следственный осмотр. Понятие, виды и доказательственное значение: учебно-практическое пособие / отв. ред. О.А. Луценко. – Элиста, 2007. – 121 с.

8. Смолькова И.В. Актуальные проблемы охраняемых федеральным законом тайн в российском уголовном судопроизводстве: монография – М.: Юрлитинформ, 2014. – 352 с.

9. Третьякова Е.И. Мобильный телефон как источник криминалистически значимой информации // Вестник Уральского финансово-юридического института. – 2018. – № 3 (13). – С. 49–51.

10. Шувалов М.Н., Шувалова А.М. Применение криминалистической техники при расследовании коррупционных преступлений // Гуманитарные, социально-экономические и общественные науки. – 2016. – № 12. – С. 210–214.

BIBLIOGRAPHIC REFERENCES

1. Arhipova N.A. To the question of the use of mobile communication facilities in the detection and investigation of crimes. – Barnaul, 2014. – № 10. – P. 16–17.

2. Butenko O.S., Raschetov V.A. Possibilities of studying mobile phones within the framework of the preliminary investigation // Modern innovations: current directions of scientific research. – M.: Problems of science. – 2017. – P. 30–32.

3. Vinogradova K.A., Savina L.A. Seizure and inspection of mobile phones and electronic information on crimes committed by military personnel // Military Law Gazette. – 2019. – № 2. – P. 55–58.

4. About refusal in acceptance to consideration of the complaint to T.N. Alekseevich on violation of his constitutional rights part one of Article 176 and part one of Article 285 of the Code of Criminal Procedure of the Russian Federation: definition of the Constitutional Court of the Russian Federation of April 8, 2010 No 433-0-0 (Extraction) // Union of Right Forces "Consultant Plus". (Date of appeal 11.08.2019).

5. Semenov G.V. Investigation of crimes in the field of mobile telecommunications: monograph. – M., 2008. – 336 p.

6. Skobelin S.Y. Possibilities of obtaining criminological significant information when examining mobile means of communication and limits of restriction of constitutional rights of citizens to confidentiality of correspondence // Crime in the field of information and telecommunication technologies: problems of prevention, disclosure and investigation of crimes. Publishing House Voronezh Institute of the Ministry of Internal Affairs of Russia. – 2017. – № 1. – P. 89–98.

7. Investigative examination. Concept, types and evidentiary meaning: Study. Allowance / Hole. Ed. O.A. Lutsenko. – Elista, 2007. – 121 p.

8. Smolkova I.V. Current problems of secrets protected by federal law in Russian criminal proceedings: monogorsk. – M.: Jurlitinform, 2014. – 352 p.

9. Tretiakova E.I. Mobile Phone as a source of forensic information // Journal of the Ural Financial and Legal Institute. – 2018. – № 3 (13). – P. 49–51.

10. Shuvalov M.N., Shuvalova A.M. Use of forensic technology in the investigation of corruption crimes // Humanities, socio-economic and social sciences. – 2016. – № 12. – P. 210–214.