УДК 343.132 № 1 (16) / 2018, с. 99—104

ПРОБЛЕМА РАЗГРАНИЧЕНИЯ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ: ОСМОТР И ОБЫСК ПРИ ПОЛУЧЕНИИ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Виктор Сергеевич Черкасов
Дальневосточный юридический институт МВД России
E-mail: viktor.kmsx@gmail.com.

В условиях интенсивного развития информационно-телекоммуникационных технологий, отсутствие четких разграничительных критериев между следственными действиями осмотром и обыском имеет не только теоретическое, но и практическое значение, так как приводит к нарушению конституционных прав на неприкосновенность частной жизни человека и гражданина. В статье анализируются причины подобных нарушений. Приводятся примеры из судебно-следственной практики. Делается вывод, что разграничительным критерием между осмотром и обыском должен стать критерий «степени вторжения правоохранительных органов в частную жизнь человека».

Ключевые слова: электронное сообщение; осмотр; обыск; критерии разграничения; тайна связи; нарушение права, электронный носитель информации.

THE DIFFERENTIATION VALUE OF THE INVESTIGATIVE ACTION: INSPECTION AND SEARCH AT THE RECEIVING COMPUTER INFORMATION

V. S. Cherkasov

In the conditions of intensive development of information and telecommunication technologies, the lack of clear demarcation criteria between the investigative action, the inspection and search is not only of theoretical but also of practical importance, since it leads to violation of constitutional rights to privacy of a person and citizen. The article analyzes the causes of such violations. Provides examples from investigative and judicial practice. The conclusion is that the dividing criterion between inspection and search should be possible «degree of intrusion of law enforcement into the private life of man».

Keywords: electronic communication; inspection; search; criteria of differentiation; the secret of connection; a violation of law, electronic media.

Цифровые технологии плотно интегрировались в жизнь современного человека. Электронные устройства, помещающиеся в ладонь, способны выполнять многочисленные операции, связанные с передачей, воспроизведением, хранением и преобразованием информации. Следует признать, что благодаря современным возможностям электронных технологий, основной массив сведений о частной жизни лица концентрируется в электронных носителях информации и различных сервисах в сети «Интернет».

Электронные носители информации позволяют осуществлять телефонные переговоры, отправлять электронные сообщения в различных интернет сервисах, то есть в полной мере использовать телематические и телефонные услуги связи. Современные «смартфоны» позволяют управлять личными финансами дистанционно. Так, при помощи технологии «Apple Pay», сотовый

телефон можно использовать вместо банковской карты, а при помощи специальных приложений, к примеру «Мобильный банк», управлять банковским счетом и видеть всю информацию о транзакциях по счету. Электронные носители информации позволяют получать информацию о транспортном средстве и управлять его функциями, что отлично демонстрируется в автомобилях компании «Tesla». Технология «Умный дом» позволяет дистанционно управлять жилищем и получать о нем информацию. И это только часть сведений, которыми можно управлять с помощью одного носителя информации.

Очевидно, что процесс интеграции информационных технологий в различные сферы жизнедеятельности человека продолжается, что многократно увеличивает возможности индивида по управлению личной информацией, и обуславливает многообразие вариаций частных сведений, которые могут содержаться, или доступ к которым может открываться, при помощи электронного носителя информации.

Подобные обстоятельства делают компьютер ценным источником доказательственных сведений для органов предварительного расследования. Анализ правоприменительной практики демонстрирует, что одним из способов, который используют сотрудники органов предварительного расследования для непосредственного исследования и приобщения к уголовному делу сведений, выраженных в электронной форме, является осмотр предметов (компьютера, планшета, мобильного телефона и т. д.).

Для подтверждения данного умозаключения обратимся к приговору Советского городского суда № 1-315/20156 от 04 октября 2016 года [4]. Согласно приговору суда Х был признан виновным в совершении преступления, предусмотренного ч. 3 ст. 30, п. «г» ст. 228.1 УК РФ (покушение на сбыт наркотических средств в крупном размере). Исходя из материалов дела, Х 23 апреля 2016 года праздновал свой день рождения совместно с Б и В. Так, Х употреблял спиртные напитки и, не желая управлять транспортным средством в состоянии алкогольного опьянения, Х передал управление В. При передвижении по городу В сообщил, что необходимо подъехать на определенное место, где ему кто-то оставил в тайнике наркотическое средство, которое необходимо за плату забрать и разложить по разным местам. После чего Х, Б, и В подъехали на определенное место, где Х разложил наркотическое средство по 5 тайникам. Далее Х, Б, и В поехали раскладывать наркотическое средство по другим тайникам. Однако Х не смог довести свой преступный умысел до конца, по не зависящим от него обстоятельствам, поскольку был задержан сотрудниками полиции. Часть второго наркотического средства, Х не смог разместить по тайникам.

Среди доказательств по уголовного делу, подтверждающих вину Х, содержится протокол осмотра предметов, а именно сотового телефона «Samsung Duos GT-S6802», изъятого у Х в ходе выемки. Согласно протоколу осмотра, в приложении «WhatsApp» был обнаружен архив переговоров между Х и В, где имеются загруженные файлы фотографий сделанных тайников. Кроме того в приложении «Telegram» обнаружен архив переговоров с неустановленным пользователем с комментариями относительно сделанных закладок и их фотографиями.

Необходимо отметить, что следователь для осмотра электронных сообщений в указанных выше интернет-сервисах Х, судебного разрешения не получал.

Более того, в настоящее время существуют специальные программно-аппаратные комплексы, которые позволяют извлекать информацию с цифровых устройств, обходя установленные пароли. К таким комплексам С. Ю. Скобелин относит: «универсальное устройство извлечения судебной информации (UFED — Universal Forensic Extraction Devise), мобильный криминалист, XRY, MOBILedit, Тарантула и др.» [6, с. 31—32].

Дополнительно С. Ю. Скобелин отмечает, что посредством комплекса UFED: «Можно получить информацию о паролях, журналах вызовов, текстовых сообщениях, контактах в электронной почте, мессенджерах, записях в календаре, медиафайлах, геотегах, приложениях, служебных данных (список IMSI, данные последней сим-карты, коды блокировки); данных журнала «Lifeblog», содержащего список действий с телефоном; переписке в различных социальных сетях («ВКонтакте», «Одноклассники», «Twitter», «Facebook»), с помощью таких приложений, как «Skype», и др.» [6, с. 31—32]. Подобные устройства используются специалистом при производстве осмотра предметов.

Для подтверждения сказанного обратимся к приговору Аксайского районного суда города Аксая от 10 мая 2017 г. № 1-489/2017 [3]. Согласно приговору, К был признан виновным в совершении преступления предусмотренного ч. 3 ст. 30, ч. 4 ст. 159 УК РФ (организация хищения чужого имущества путем обмана в особо крупном

размере). Так, К, занимая должность заместителя директора ООО «Х», получил на временное хранение бухгалтерскую документацию ООО «Х». Достоверно зная, что Н в 2013—2014 годах занимал должность директора ООО «Х», и что данная бухгалтерская документация ранее изымалась сотрудниками органов внутренних дел и являлась предметом изучения в рамках процессуальной проверки, у К созрел преступный умысел на хищение денежных средств в размере 3 000 000 рублей. Далее К написал Н анонимное письмо, где указал, что на основе находящейся у него бухгалтерской документации ООО «Х» в отношении Н может быть возбуждено уголовное дело. После чего К общался с Н через приложение «WhatsApp», создавая ложное представление о том, что он является сотрудником правоохранительных органов. Через указанное приложение К договорился о встрече с Н для передачи 1/3 суммы, однако преступный умысел К довести до конца не смог по независящим от него обстоятельствам, так как был задержан сотрудниками УФСБ России по Ростовской области.

Среди доказательств, подтверждающих вину К, имеется протокол осмотра предметов, а именно мобильного телефона «iPhone 5S», изъятого при его задержании. При осмотре телефона использовался «UFED TOUCH», с помощью которого вся информация с телефона перенесена на флеш-карту. При осмотре флеш-карты, на ней обнаружен архив сообщений приложения «WhatsApp» между К и Н, где имеются фотографии бухгалтерской документации ООО «Х».

Таким образом, уголовно-процессуальный осмотр предмета (компьютера, мобильного телефона, планшета и т. д.) является распространенным следственным действием. Однако, электронный носитель информации не является обычным предметом, а способен воспроизводить, хранить, передавать компьютерную информацию. Необходимо учитывать, что электронное устройство может содержать широкий спектр сведений о частной жизни лица, которые относятся к различным видам охраняемых законом тайн. К примеру, к тайне переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, предусмотренной ч. 2 ст. 23 Конституции РФ. Более того, владелец электронного носителя информации может установить определенные ограничения доступа к самому устройству или определенной информации, доступ к которой осуществляется при помощи электронного носителя информации.

Любопытно, что в судебно-следственной практике можно обнаружить факты, когда следователи возбуждают перед судом ходатайство о разрешении производства осмотра мобильных телефонов, понимая, что без разрешения суда на производство следственного действия, будет нарушено положение ч. 2 ст. 23 Конституции РФ. Однако суд отказывает в удовлетворении ходатайства, мотивируя тем, что «уголовно-процессуальным законом не предусмотрено получение разрешения на указанное следственное действие» [1].

При производстве осмотра электронного носителя информации, сотрудник органа предварительного расследования принудительно проникает в частную жизнь лица без его разрешения. В процессе осмотра подбираются пароли от электронных устройств, что является прямой аналогией вскрытия любых помещений (в том числе сейфов, иных хранилищ), которое можно производить при производстве обыска. Принимая во внимание технические особенности электронного устройства как предмета, необходимо задаться вопросом о правомерности использования следственного осмотра, а не обыска?

Чтобы ответить на этот вопрос, необходимо обратиться к подходам по разграничению следственного осмотра и обыска. Так, А. П. Рыжаков указывает, что главное отличие осмотра от обыска и некоторых других следственных действий — при осмотре нельзя применять принуждение [5]. На наш взгляд, данный разграничительный критерий является недостаточно точным, так как на основании п.п. 4—5 ст. 27 УПК РФ ст. 29 суд принимает решение о производстве осмотра и обыска в жилище при отсутствии согласия проживающих в нем лиц, что является прямым принуждением. Необходимо отметить, что на основании ч. 3 ст. 177 УПК РФ при производстве осмотра допускается изъятие предметов, имеющих отношение к уголовному делу, что также можно отнести к принуждению по аналогии с принудительным изъятием предметов при обыске.

Анализируя позицию некоторых авторов можно прийти к выводу, о разграничении осмотра и обыска по объекту. Так, Н. В. Ткачева указывает, что «обыск предназначен для обнаружения, фиксации и изъятия объектов, имеющих значение для уголовного дела, при этом объектами обыска являются предметы, документы, орудия преступления, трупы, тогда как при осмотре целью являются установления следов преступления и обстановки места происшествия» [8, с. 169]. Если в ч. 1 ст. 176 УПК РФ прямо говорится про следы

преступления, то в ч. 1 ст. 182 УПК РФ о следах нет никаких упоминаний. Разграничение следственных действий, осмотр и обыск по объекту будет представлять проблематику в правоприменительной деятельности.

К примеру, если при производстве обыска, следователь обнаруживает следы нового преступления (пятна крови, следы борьбы и т. д.), то, исходя из названного разграничивающего критерия, необходимо прекращать обыск и начинать осмотр места происшествия, что в практической деятельности будет недопустимо.

В свою очередь А. В. Смирнов и К. Б. Калиновский под осмотром понимают «непосредственное восприятие и процессуальная фиксация участниками этого следственного действия внешних признаков объектов, к которым, как правило, имеется свободный доступ» [7, с. 12]. На наш взгляд, данная позиция, содержит верный вектор для дальнейших умозаключений. Тем не менее, недостаток рассматриваемого подхода заключается в том, что концепция «свободного доступа» не согласуется относительно технических свойств электронных носителей информации. Если руководствоваться критерием «свободного доступа» при производстве следственных действий, то каждый раз при исследовании содержания электронного носителя информации будет необходимо производить обыск, так как непосредственное восприятие компьютерной информации невозможно.

По данному вопросу интересно мнение Р. И. Оконенко, который предлагает понимать «свободный доступ» не с материальной точки зрения, а с абстрактно-юридической, а именно «о возможной степени вторжения органов предварительного расследования в частную жизнь человека» [2, с. 29]. Данный критерий, приводя аналогию правоприменительной практики США, автор объясняет, исходя из разумного ожидания гражданина относительно сохранности тайны его личной жизни. Подобная позиция объясняет, почему на основании ч. 5 ст. 177 УПК РФ требуется получить разрешение владельца жилища на производства осмотра.

Основываясь на разграничительном критерии, предложенном Р. И. Оконенко, можно полагать, что при производстве осмотра, следователь вправе собирать информацию об объектах, которые доступны его непосредственному восприятию, поскольку только такая деятельность не нарушает разумные ожидания граждан по поводу сохранности тайны их личной жизни.

Исходя из этого, следователь может осмотреть электронный носитель информации, к примеру, с записью общественного места камер видеонаблюдения, так как не вторгается в личную жизнь человека, а последний может разумно ожидать, что запись может быть осмотрена. Но при этом следователь не может осматривать компьютер лица (планшет, мобильный телефон, и т. д.), так как вторгается в личную жизнь человека и ограничивает право, предусмотренное ст. 23 Конституции РФ, чего последний разумно ожидать не может. К тому же, изымая электронное устройство у другого лица, и осматривая содержащиеся на нем данные, следователь, исследуя информационную систему, выходит за рамки «свободного доступа» и вторгается в частную жизнь человека и гражданина, ограничивая право на неприкосновенность частной, семейной жизни, тайну связи. Также подобное вторжение наглядно прослеживается при подборе пароля, защищающего личные сведения владельца электронного носителя информации.

Основываясь на разграничительном критерии следственного осмотра и обыска по объему прав сотрудника органа предварительного расследования на вторжение в личную жизнь гражданина, можно сделать вывод о подмене обыска осмотром предмета (компьютера, мобильного телефона, планшета и т. д.).

Однако, понимая, что для исследования информации на электронном устройстве необходимо производить обыск, уголовно-процессуальное законодательство создаёт перед следователем ограничения. Так, в настоящий момент ч. 1 ст. 182 УПК РФ предусматривает в качестве объектов обыска «какое-либо место» или «лицо». Отдельно взятый предмет, как объект обыска, уголовно-процессуальным законом не предусмотрен, что делает невозможным производство обыска в отношении отдельно взятого электронного носителя информации.

Несмотря на положительные стороны разграничительного критерия «степени вторжения в частную жизнь человека», данный критерий сложно прямо реализовать в УПК РФ, так как он является достаточно абстрактным и оценочным, что может привести к его произвольному толкованию в правоприменительной практике. В уголовно-процессуальном праве должны быть закреплены точные условия выбора «осмотра» или «обыска».

Используя указанный критерий в качестве правотворческого принципа, автором

были предложены комплексные изменения в УПК РФ, содержащие точные императивные условия, предписывающие применить «осмотр» или «обыск», а также необходимые случаи получения судебного разрешения на производство следственных действий в отношении электронного носителя информации. Основополагающими уголовно-процессуальными условиями выступают: во-первых, воля владельца электронного носителя информации, во-вторых, техническое свойство электронного носителя информации, обуславливающее возможность передавать данные посредством электросвязи, что создаёт возможность априорного получения доступа к сведениям, попадающим под действие тайны связи [9, с. 45—46].

Таким образом, действующее уголовно-процессуальное законодательство не в достаточной мере регулирует все существующие общественные отношения, которые сформировались под воздействием электронно-информационных технологий, что порождает ошибки со стороны правоприменителя в выборе следственного действия по исследованию электронного носителя информации и последующему нарушению конституционных прав человека и гражданина.

Список литературы

1. Апелляционное постановление Приморского краевого суда от 2 февраля 2015 г. № 22К-455/2015 [Электронный ресурс] URL: // http://docs.pravo.ru/document/view/68631850/79991497/ (дата обращения: 18.04.2017).

2. Окоменко, Р. И. К вопросу о правомерности осмотра компьютера как следственного действия / Р. И. Окоменко // Адвокат. — 2015. — № 1. — С. 27—30.

3. Приговор Аксайского районного суда города Аксая от 10 мая 2017 г. № 1–489/2017 [Электронный ресурс] // «Судебные и нормативные акты РФ». — URL: http://sudact.ru/regular/doc/N5upNCBNs9UT (дата обращения: 01.08.2017).

4. Приговор Советского городского суда № 1-315/20156 от 04 октября 2016 года [Электронный ресурс] // «Судебные и нормативные акты РФ». — URL: http://sudact.ru/regular/doc/e2D8ohGvccWW/?page (дата обращения: 01.05.2017).

5. Рыжаков, А. П. Комментарий к Уголовно-процессуальному кодексу Российской Федерации [Электронный ресурс] / А. П. Рыжаков. — 9-е издание, переработанное. — СПС «Консультант плюс», 2014.

6. Скобелин, С. Н. Использование специальных знаний при работе с электронными следами / С. Н. Скобелин // Российский следователь. — 2014. — № 20. — С. 31—33.

7. Смирнов, А. В. Следственные действия в российском уголовном процессе : учеб. пособие / А. В. Смирнов, К. Б. Калиновский. — СПб., 2004. — 73 с.

8. Ткачева, Н. В. Пределы применения уголовно-процессуального принуждения при проведении следственных действий в жилище (обыск) / Н. В. Ткачева // Вестник Томского государственного университета. — 2007. — № 300-1. — С. 169—172.

9. Черкасов, В. С. Проблемы регулирования правового режима компьютерной информации в уголовном досудебном производстве / В. С. Черкасов // Вестник ДВЮИ МВД России. — 2017. — № 2. — С. 40—46.

References

1. Apellyacionnoe postanovlenie Primorskogo kraevogo suda ot 2 fevralya 2015 g. № 22K-455/2015 [Ehlektronnyj resurs] URL: // http://docs.pravo.ru/ document/view/68631850/79991497/ (data obrashcheniya: 18.04.2017).

2. Okonenko, R. I. K voprosu o pravomernosti osmotra komp'yutera kak sledstvennogo dejstviya / R. I. Okonenko // Advokat. — 2015. — № 1. — S. 27—30.

3. Prigovor Aksajskogo rajonnogo suda goroda Aksaya ot 10 maya 2017 g. № 1–489/2017 [Ehlektronnyj resurs] // «Sudebnye i normativnye akty RF». — URL: http://sudact.ru/regular/doc/N5upNCBNs9UT (data obrashcheniya: 01.08.2017).

4. Prigovor Sovetskogo gorodskogo suda № 1-315/20156 ot 04 oktyabrya 2016 goda [Ehlektronnyj resurs] // «Sudebnye i normativnye akty RF». — URL: http://sudact.ru/regular/doc/e2D8ohGvccWW/?page (data obrashcheniya: 01.05.2017).

5. Ryzhakov, A. P. Kommentarij k Ugolovno-processual'nomu kodeksu Rossijskoj Federacii [Ehlektronnyj resurs] / A. P. Ryzhakov. — 9-e izdanie, pererabotannoe. — SPS «Konsul'tant plyus», 2014.

6. Skobelin, S. N. Ispol'zovanie special'nyh znanij pri rabote s ehlektronnymi sledami / S. N. Skobelin // Rossijskij sledovatel'. — 2014. — № 20. — S. 31—33.

7. Smirnov, A. V. Sledstvennye dejstviya v rossijskom ugolovnom processe : ucheb. posobie / A. V. Smirnov, K. B. Kalinovskij. — SPb., 2004. — 73 s.

8. Tkacheva, N. V. Predely primeneniya ugolovno-processual'nogo prinuzhdeniya pri provedenii sledstvennyh dejstvij v zhilishche (obysk) / N. V. Tkacheva // Vestnik Tomskogo gosudarstvennogo universiteta. — 2007. — № 300-1. — S. 169—172.

9. Cherkasov, V. S. Problemy regulirovaniya pravovogo rezhima komp'yuternoj informacii v ugolovnom dosudebnom proizvodstve / V. S. Cherkasov // Vestnik DVYUI MVD Rossii. — 2017. — № 2. — S. 40—46.