УДК 343.13 С. 122–127

ПРОБЛЕМА ОБЕСПЕЧЕНИЯ РЕЖИМА ТАЙНЫ ЭЛЕКТРОННОЙ ИНФОРМАЦИИ ПРИ УГОЛОВНОМ ПРЕСЛЕДОВАНИИ

Черкасов В. С.
Дальневосточный юридический институт МВД России
г. Владивосток, Российская Федерация
E-mail: viktor.kmsx@gmail.com
https://orcid.org/0000-0002-4241-3650.

Аннотация. Человек доверяет информационным технологиям огромный массив личных данных: банковские транзакции, пароли, электронные сообщения, персональный данные, а также множество иной информации. С одной стороны, возможность использования информационных технологий делает жизнь современно человека более комфортной, но с другой, позволяет аккумулировать всю данные о жизнедеятельности каждого члена современного общества в единых информационных системах. Данное обстоятельство обеспечивает правоохранительным органам удобный источник доказательств. При этом ключ от названных информационных систем каждый из нас хранит при себе. Таким ключом является «смартфон» или иное оконечное оборудование. В представленной статье рассматриваются особенности соблюдения режимов различных видов тайн при производстве следственных действий в отношении оконечного оборудования (смартфона, компьютера, планшета) пользователей электросвязи. Раскрываются уязвимости законодательных гарантий, которые в условиях цифровизации должны обеспечить ограничение доступа и последующего использования профессиональной, свидетельской, коммерческой, государственной тайны в рамках уголовного преследования. Сложность совершенствования правового регулирования юридических гарантий, обеспечивающих неприкосновенность названной информации, детерминируется: во-первых, многообразием видов режимов тайн, во-вторых, отсутствием у сотрудника органа предварительного расследования возможности знать с каким видом тайны ему предстоит столкнуться при производстве следственного действия.

Ключевые слова: электронные доказательства, электронные носитель информации, коммерческая тайна, профессиональная тайна, государственная тайна, свидетельский иммунитет, уголовный процесс.

Для цитирования: Черкасов, В. С. Проблема обеспечения режима тайны электронной информации при уголовном преследовании / В. С. Черкасов // Правопорядок: история, теория, практика. — 2021. — № 2 (29). — С. 122–127.

THE PROBLEM OF ENSURING THE SECRECY OF ELECTRONIC INFORMATION IN CRIMINAL PROSECUTION

V. S. Cherkasov
Far Eastern Law Institute of the Ministry of Internal Affairs of the Russia
Vladivostok, Russian Federation
E-mail: viktor.kmsx@gmail.com
https://orcid.org/0000-0002-4241-3650

Abstract. A person trusts information technologies with a huge array of personal data: bank transactions, passwords, electronic messages, personal data, as well as many other information. On the one hand, the possibility of using information technologies makes the life of a modern person more comfortable, but on the other hand, it allows you to accumulate all the data about the life of each member of modern society in unified information systems. This circumstance provides law enforcement agencies with a convenient source of evidence. At the same time, each of us keeps the key to these information systems with us. Such a key is a “smartphone” or other terminal equipment. The article deals with the peculiarities of compliance with the regimes of various types of secrets in

the production of investigative actions in relation to the terminal equipment (smartphone, computer, tablet) of telecommunications users. The article reveals the vulnerabilities of legislative guarantees that, in the context of digitalization, should ensure the restriction of access and subsequent use of professional, witness, commercial, and state secrets in the framework of criminal prosecution. The complexity of improving the legal regulation of legal guarantees that ensure the inviolability of the above-mentioned information is determined: first, by the variety of types of secrecy regimes, and secondly, by the lack of an employee of the preliminary investigation body to know what kind of secrecy he will face in the course of an investigative action.

Keywords: electronic evidence, electronic media, commercial secret, professional secret, state secret, witness immunity, criminal procedure.

For citation: Cherkasov V. S. The Problem of Ensuring the Secrecy of Electronic Information in Criminal Prosecution. *Pravoporyadok: istoriya, teoriya, praktika* [Legal Order: History, Theory, Practice], 2021, no. 2 (29), pp. 122–127. (In Russ.)

Введение

Информационные технологии являются неотъемлемой частью жизнедеятельности современного общества. Используя различные интернет-сервисы, человек доверяет информационным технологиям большой объем личных данных. В подобных условиях необходимо поставить вопрос о защищенности личных данных, в частности, при уголовном преследовании.

Описание проводимого исследования

В науке уже неоднократно обсуждалась проблема распространения тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, предусмотренной ч. 2 ст. 23 Конституции РФ, на все виды «электронных коммуникаций» [1; 3; 5]. Кроме названного вида режима тайны, существуют и другие. В настоящем исследовании рассмотрен вопрос о защищенности профессиональной, свидетельской, коммерческой, государственной тайны при производстве следственных действий в отношении оконечного оборудования пользователей электросвязи.

Результат исследования и обсуждение

Свидетельский иммунитет, предусмотренный ст. 51 Конституции РФ, закрепляет правило, связанное с волеизъявлением лица о даче показаний, относительно обстоятельств, имеющих значения для уголовного дела. В данном случае закон закрепляет запрет на получения идеальных (личных) доказательств, содержащихся в сознании свидетеля без его волеизъявления. Однако электронная информация существует объективно в окружающей среде.

Исходя из этого, можно привести аналогию с собиранием материальных следов преступления, которые не содержатся в сознании участника уголовного судопроизводства (трасологических следов, предметов, документов, почтовых отправлений, телефонных переговоров и т. д.). При производстве следственных действий, направленных на сбор указанных доказательств, сотруднику органа предварительного расследования совершенно безразлично волеизъявление свидетеля, подозреваемого или обвиняемого. Поэтому логично предположить, что действие свидетельского иммунитета на получение электронной информации не распространяется.

Однако в условиях развития информационных технологий названное правило допустимо подвергнуть критическому осмыслению.

Достаточно важным вопросом является допустимость использования электронных сообщений лиц, обладающих «профессиональным» свидетельским иммунитетом, предусмотренным ч. 3 ст. 56 Уголовно-процессуального кодекса Российской Федерации (далее — УПК РФ).

Не исключен вариант того, что лица, перечисленные в ч. 3 ст. 56 УПК РФ, могут использовать интернет-мессенджеры в своей профессиональной деятельности. При этом электронные сообщения указанных лиц не являются показаниями, из чего можно сделать вывод, что и свидетельский иммунитет на них не распространяется.

Так, детальную регламентацию получила адвокатская тайна. В соответствии с ч. 1 ст. 8 Федерального закона «Об адвокатской деятельности и адвокатуре Российской Федерации»[1] проведение оперативно-розыскных мероприятий и следственных действий в отношении адвоката (в том числе в жилых и служебных помещениях, используемых им для осуществления адвокатской деятельности) допускается только на основании судебного решения. При этом в ст. 450.1 УПК РФ указано, что производство осмотра обыска, выемки

[1] Об адвокатской деятельности и адвокатуре в Российской Федерации : Федеральный закон от 31.05.2002 № 63-ФЗ // Российская газета. — 2002. — 05 июня.

в жилых и служебных помещениях, используемых адвокатом для осуществления профессиональной деятельности, а также самого адвоката, возможно при соблюдении неприкосновенности адвокатской тайны. Не исключены случаи, когда адвокат сам совершает преступление, и сведения имеющие значение для уголовного дела, могут содержаться на его мобильном телефоне или ином электронном носителе информации.

Исходя из положения ст. 450.1 УПК РФ, по судебному решению допустимо производить следственные действия, в ходе которых возможно изъять электронный носитель информации, принадлежащий адвокату. Но в данном случае следователь получит доступ не только к электронным сообщениям адвоката, содержащим сведения, имеющим значение для уголовного дела, но и электронным сообщения, которые отправляли друг другу адвокат и его доверитель. Данные сведения могут представлять интерес для правоохранительных органов. Приведенная ситуация возможна и для других лиц, перечисленных в ч. 3 ст. 56 УПК РФ.

В этом случае уголовно-процессуальный закон не дает однозначного ответа о распространении режима адвокатской тайны на электронные сообщения между адвокатом и его доверителем, содержащиеся на изъятом электронном носители информации. Тем не менее, совершенно очевидно, что осмотр изъятого у адвоката электронного носителя информации также необходимо производить по судебному решению с соблюдением неприкосновенности сведений, которые составляют адвокатскую тайну.

Подобная информация во всех случаях должна признаваться недопустимым доказательством, что обусловлено положением ст. 450.1, где указано, что предметы и сведения, составляющие адвокатскую тайну, не могут быть изъяты или зафиксированы (в том числе с использованием технических средств) при производстве следственных действий. В данном случае адвокатская тайна законодательно получила распространение не только на показания адвоката, но и на сведения, объективно существующие во внешней среде: документы, электронную информацию (материальные доказательства).

Следует отметить, что Европейский суд по правам человека (далее — ЕСПЧ) придерживается позиции, согласно которой на электронную информацию, изъятую в ходе правомерного обыска, также распространяется режим адвокатской тайны. Изъятие и исследование подобной информации ЕСПЧ оценивает как нарушение права на уважение частной корреспонденции, предусмотренной ст. 8 «Конвенции о защите прав человека и основных свобод»[1].

Показательным примером, относительно обозначенного тезиса является Постановление ЕСПЧ от 16 октября 2007 года «Визер и компания «Бикос бетейлигунген ГмбХ» (Wieser and Bicos Beteiligungen GmbH) против Австрии»[2]. Согласно постановлению, Визер (физическое лицо) совмещал адвокатскую деятельность с владением и управление холдинговой компанией «Бикос бетейлигунген ГмбХ», являющейся вторым заявителем по делу. Компания «Бикос бетейлигунген ГмбХ» фактически располагалась в юридическом офисе Визер. Региональный суд Австрии выдал судебное разрешение на производство обыска в офисе компании.

В ходе обыска изымались и исследовались документы, если заявитель возражал против немедленного исследования документов, они опечатывались и передавались в региональный суд в соответствии с УПК Австрии. Также было произведено исследование компьютера, находившегося в офисе, и записано несколько файлов на диск. При исследовании компьютера присутствовал представитель адвокатской коллегии.

Оценивая производство обыска ЕСПЧ указал, что обыск и изъятие электронных данных заявителей представляли собой вмешательство властей в право на уважение «корреспонденции». Суд указал, что обыск является правомерным, однако при этом гарантии адвокатской тайны соблюдались в отношении документов, а не электронных данных. Уклонение полицейских от соблюдения определенных процессуальных гарантий, имевших целью помешать «произволу» и защитить профессиональную тайну адвоката, делает обыск и изъятие электронных данных первого заявителя несоразмерными преследуемой законном цели. ЕСПЧ констатировал нарушение ст. 8 «Конвенции о защите прав человека и основных свобод» в части исследования электронной информации, попадающей под режим адвокатской тайны.

Таким образом, ЕСПЧ распространяет действие адвокатской тайны на сведения, выраженные в электронной форме, и указывает на необходимость соблюдения специальных

---

[1] Конвенция о защите прав человека и основных свобод (заключена в г. Риме 04.11.1950) // Бюллетень международных договоров. — 2001. — № 3.

[2] Постановление ЕСПЧ от 16 октября 2007 года «Визер и компания «Бикос бетейлигунген ГмбХ» (Wieser and Bicos Beteiligungen GmbH) против Австрии» // Бюллетень Верховного Суда РФ. — 2008. — № 4.

правил при производстве обыска в отношении адвоката. Однако вопрос о распространении адвокатской тайны на электронные носители информации (смартфон, планшет и т. д.), которые находятся при адвокате (не в его кабинете или жилище), ЕСПЧ не затронул. Представляется верным что, в данном случае адвокатская тайна также имеет юридическую силу, так как фактически нет никакой разницы между электронными носителями информации, находящимися в жилище или служебном помещении адвоката, и электронном устройстве, находящемся непосредственно при нем, или в ином месте (автомобиле, гараже и т. д.).

В настоящий момент УПК РФ не содержит норм, раскрывающих вопрос распространения свидетельского иммунитета на электронные сообщения в связи осуществлением профессиональной деятельности лиц, указанных в ч. 3 ст. 56 УПК РФ. Следует признать, что в уголовно-процессуальном законодательстве существует необходимость расширения границ режима адвокатской тайны, а также аналогичных видов профессиональных тайн, вытекающих из лиц, предусмотренных ч. 3 ст. 56 УПК РФ.

Для сравнения в Уголовно-процессуальном кодексе Федеральной Республики Германия (далее — УПК ФРГ)[1] режим свидетельского иммунитета распространяется на электронные сообщения, доступ к которым можно получить через электронный носитель информации, находящийся в фактическом владении лица. Как указывает П. В. Головненков: «Согласно § 97 (абз. 1 № 1) УПК ФРГ не подлежит выемке переписка между обвиняемым и лицами, которые имеют право отказаться от дачи показаний на основании § 52, 53 (абз. 1 предл. 1 № 1-3b), 53a УПК ФРГ (супруг/супруга, помолвленный/-ая, лица, состоящие с обвиняемым в родстве или свойстве, священнослужители, защитники, адвокаты, налоговые консультанты, врачи, сотрудники признанных государством консультаций и т. д., а также их профессиональные помощники). Запрет на выемку распространяется, согласно § 97 (абз. 1 № 2) УПК ФРГ, также на записи, которые лица, перечисленные в § 53 (абз. 1 предл. 1 № 1-3b), 53a УПК ФРГ, сделали о сообщениях, доверенных им обвиняемым, или о других обстоятельствах, на которые распространяется право на отказ от дачи показаний» [2].

Вопрос о распространение режима «коммерческой тайны» на электронную информацию, доступ к которой открывается с помощью электронного носителя. В соответствии с п. 2 ст. 3 закона «О коммерческой тайне»[2], информация, составляющая коммерческую тайну — это «сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны».

Очевидно, что указанные сведения могут быть распространены с помощью различных интернет-сервисов между заинтересованными лицами (между учредителями юридического лица, контрагентами договора коммерческой концессии «франчайзинг» и т. д.). Так, ч. 3 ст. 6 закона «О коммерческой тайне» предусматривает для обладателя информации, составляющей коммерческую тайну, а также для органа государственной власти, местного самоуправления, получившего такую информацию, обязанность предоставлять названную информацию по запросу органа предварительного расследования по делам, находящимся в их производстве.

Необходимо отметить, что ч. 2 ст. 6 закона «О коммерческой тайне», предусматривает для обладателя подобной информации механизм самозащиты. Как указывает К. В. Пронин: «Во всех случаях, когда обладатель коммерческой тайны считает требования государственного органа (органа местного самоуправления) о предоставлении ему тех или иных конфиденциальных сведений незаконными и отказывается исполнить запрос, инициатор запроса, согласно части 2 статьи 6 Закона «О коммерческой тайне», наделяется правом затребовать эту информацию в судебном порядке.

Рассмотрение дела в суде дает обеим сторонам спора равные процессуальные возможности для отстаивания своей позиции, что является дополнительной правовой гарантией от злоупотреблений со стороны чиновников. Кроме того, обладатель коммерческой тайны также наделен правом на обращение в суд — он может подать иск о признании

[1] Уголовно-процессуальный кодекс Федеральной Республики Германии от 12.09.1950 года // Bundesministerium der Justiz und für Verbraucherschutz : Bundesamt für Justiz. — URL: http://www.gesetze-im-internet.de/englisch_stpo/index.html (дата обращения 10.04.2021).

[2] О коммерческой тайне : Федеральный закон от 29.07.2004 № 98-ФЗ // Российская газета. — 2004. — 05 авг.

соответствующего предписания государственного органа (органа местного самоуправления) не соответствующим закону, иному нормативному правовому акту» [4]. Доступ к информации, составляющей коммерческую тайну, через электронный носитель фактически лишает обладателя данной информации механизма судебной самозащиты.

В настоящее время существуют специальные приложения (программы), которые позволяют управлять банковским счетом (производить транзакции, оплачивать счета, брать кредит, осуществлять вклады, наблюдать информацию по счету и т. д.) с помощью оконечного оборудования. Исходя из этого, через электронный носитель информации возможно получить доступ к банковской тайне. Согласно ст. 26 Федерального закона «О банках и банковской деятельности»[1], справки по операциям и счетам юридических лиц, граждан, осуществляющих предпринимательскую деятельность без образования юридического лица, а также физических лиц, выдаются кредитной организацией, при наличии согласия руководителя следственного органа, по делам, находящимся в их производстве.

При этом, согласно п. 3 ч. 2 ст. 38 УПК РФ, следователь уполномочен самостоятельно направлять ход расследования, принимать решение о производстве следственных и иных процессуальных действий, за исключением случаев, когда в соответствии с УПК РФ требуется получение судебного решения или согласия руководителя следственного органа.

Взаимосвязанные положения п. 3 ч. 2 ст. 38 УПК РФ и ст. 26 Федерального закона «О банках и банковской деятельности» накладывают на следователя ведомственный контроль со стороны руководителя следственного органа. Согласно названным положениям следователь вправе собирать сведения, попадающие под режим банковской тайны, только при наличии согласия руководителя следственного органа по возбужденному уголовному делу. Очевидно, что осмотр электронного носителя информации, который может быть произведен до возбуждения уголовного дела и соответственно «банковского» приложения, согласия руководителя следственного органа не требует, что фактически необоснованно исключает ведомственный контроль, и содержит предпосылки для нарушения режима банковской тайны.

Электронный носитель информации может содержать сведения или открывать доступ к сведениям, составляющим государственную тайну. В соответствии со вторым абзацем ст. 2 закона «О государственной тайне»[2], под носителями сведений, составляющих государственную тайну, понимаются «материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов». Представляется, что лица, обладающие доступом к информации, составляющей государственную тайну, могут обмениваться между собой электронными сообщениями, в которых может содержаться государственная тайна.

При этом, исходя из положения п. 4 ч. 2 ст. 29 УПК РФ, судебное решение необходимо получать, только при производстве выемки предметов и документов, составляющих государственную тайну. Для следственного осмотра такого требования в УПК РФ не содержится. Следуя логике законодателя, можно предположить, что если судебное разрешение на изъятие предметов и документов уже получено, то повторное разрешение на их осмотр уже не нужно. Названный механизм позволяет сотрудникам органов предварительного расследования получать доступ к сведениям, составляющим государственную тайну без судебного решения.

Заключение

Электронный носитель открывает доступ к информации, которая может относиться к многообразию вариаций режимов тайн, предусмотренных законодательством. Существующий в правоприменительной практике уголовно-процессуальный порядок получения электронной информации позволяет игнорировать законодательные ограничения получении доступа к рассмотренным видам тайн.

Вывод

Юридические гарантии, обеспечивающие защиту различных видов тайн при производстве следственных действий в отношении оконечного оборудования пользователей электросвязи, не соответствуют сформировавшимся под воздействием информационных технологий общественным отношениям. Сложность правого регулирования заключается: во-первых, в многообразии видов режимов тайн, во-вторых, отсутствием у сотрудника органа предварительного расследования возможности знать с каким видом тайны ему предстоит столкнуться при производстве следственного действия.

[1] О банках и банковской деятельности : Федеральный закон от 02.12.1990 № 395-1 // Российская газета. — 1996. — 10 февр.

[2] О государственной тайне : Закон РФ от 21.07.1993 № 5485-1 // Российская газета. — 1993. — 21 сент.

Список литературы

1. Васюков, В. Ф. Осмотр, выемка электронных сообщений и получение компьютерной информации / В. Ф. Васюков // Уголовный процесс. — 2016. — № 10. — С. 64–67.

2. Головненков, П. В. Уголовное уложение (Уголовный кодекс) Федеративной Республики Германия : Strafgesetzbuch (StGB) : научно-практический комментарий и перевод текста закона / П. В. Головненков. — Изд. 2-е, перераб. и доп. — Москва : Проспект, 2016. — 311 с.

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

4. Пронин, К. В. Защита коммерческой тайны / К. В. Пронин. — Москва : ГроссМедиа : ГроссМедиа Ферлаг, 2006. — 143 с.

5. Хайдаров, А. А. Незаконная практика фиксации личной переписки граждан на мобильных устройствах / А. А. Хайдаров // Уголовный процесс. — 2017. — № 5. — С. 36–41.

References

1. Vasyukov, V. F. Osmotr, vyemka elektronnykh soobshcheniy i poluchenie kompyuternoy informatsii / V. F. Vasyukov // Ugolovnyy protsess. — 2016. — № 10. — S. 64–67.

2. Golovnenkov, P. V. Ugolovnoe ulozhenie (Ugolovnyy kodeks) Federativnoy Respubliki Germaniya : Strafgesetzbuch (StGB) : nauchno-prakticheskiy kommentariy i perevod teksta zakona / P. V. Golovnenkov. — Izd. 2-e, pererab. i dop. — Moskva : Prospekt, 2016. — 311 s.

3. Okonenko, R. I. K voprosu o pravomernosti osmotra kompyutera kak sledstvennogo deystviya / R. I. Okonenko // Advokat. — 2015. — № 1. — S. 27–30.

4. Pronin, K. V. Zashchita kommercheskoy tayny / K. V. Pronin. — Moskva : GrossMedia : GrossMedia Ferlag, 2006. — 143 c.

5. Khaydarov, A. A. Nezakonnaya praktika fiksatsii lichnoy perepiski grazhdan na mobilnykh ustroystvakh / A. A. Khaydarov // Ugolovnyy protsess. — 2017. — № 5. — S. 36–41.

Дата поступления статьи: 16.04.2021.