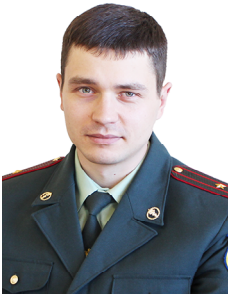




УДК 343.1:343.141



Андрей Леонидович КАРЛОВ,
преподаватель кафедры уголовного процесса
Сибирского юридического института ФСКН
России (г. Красноярск)

dys_karlov@mail.ru

ИСПОЛЬЗОВАНИЕ В ДОКАЗЫВАНИИ ПО УГОЛОВНЫМ ДЕЛАМ СВЕДЕНИЙ, СОСТАВЛЯЮЩИХ ТАЙНУ СВЯЗИ, РАСПОЛОЖЕННЫХ В СЕТИ ИНТЕРНЕТ

THE USAGE OF THE SECRET COMMUNICATION DATA LOCATED ON THE INTERNET IN PROVING CRIMINAL CASES

В статье дается правовая оценка переписки и иных сведений, расположенных в сети Интернет, с точки зрения их отнесения к тайне связи, на основании которой рассматривается вопрос о возможности и порядке уголовно-процессуальной фиксации интернет-переписки и ее использования в доказывании по уголовным делам.

The article is devoted to the legal assessment of correspondence and other data located on the Internet from the point of view of their reference to the secret communication on the basis of which the issue of opportunity and order of criminal and procedural record of the Internet correspondence and its application in proving criminal cases is considered.

Ключевые слова: Интернет, доказательство, ограничение тайны переписки, личная тайна в уголовном судопроизводстве.

Keywords: the Internet, proof, restriction of secret of correspondence, privacy in criminal proceeding.

Сегодня компьютерная техника в целом и глобальная сеть Интернет в частности являются неотъемлемыми атрибутами социально-активного населения и повседневными спутниками каждого из нас. Указанные особенности развития общества отражаются в том числе и на характере преступной деятельности.

С одной стороны, информационный обмен данными способствует появлению новых общественно опасных деяний, формированию новых способов совершения преступлений, с другой – компьютерная техника и Интернет существенно облегчают совершение преступлений, выступают их эффективными средствами и орудиями. Именно благодаря развитию средств коммуникации, среди преступлений в сфере незаконного оборота наркотиков появи-

лись такие, как бесконтактный сбыт, контрабанда, совершенная путем заказа наркотика через сеть Интернет, и др.

Использование преступниками компьютерной техники и сети Интернет при совершении преступлений влечет качественное изменение следовой картины, а соответственно, ставит перед следователем новые задачи, которые зачастую не могут быть решены из-за отсутствия в законе адекватных средств доказывания. В статье мы рассмотрим лишь одну из проблем, с которой сталкиваются сотрудники практических органов в рассматриваемой сфере, а именно проблему правового режима получения и процессуальной фиксации интернет-переписки злоумышленников в уголовном судопроизводстве.



Прежде всего нужно пояснить, что под интернет-перепиской мы предлагаем понимать сообщения и связанные с ними данные, которые хранятся не в памяти электронных устройств пользователя, а на удаленных серверах операторов связи. Значение такого разделения заключается в том, что информация, сохранившаяся на электронном носителе любого устройства пользователя, уже не может относиться к тайне связи, а является личной тайной, правовой режим доступа к которой существенно отличается. [подр.: 4]

Первая проблема, с которой сталкивается правоприменитель, – это вопрос отнесения получаемых сведений к тайне связи. На наш взгляд, можно выделить несколько обязательных признаков, наличие которых позволяет говорить об отнесении той или иной информации к тайне связи.

1. Одним из признаков является нахождение переписки (либо сведений о переписке) в ведении оператора связи. Обязательность данного признака подтверждается в том числе положениями ст. 63 Федерального закона от 7 июля 2003 г. №126-ФЗ "О связи", согласно которому соблюдение тайны связи обязаны обеспечивать именно операторы связи. Помимо этого ст. 186.1 УПК РФ требует получения судебного решения именно при получении информации о соединениях между абонентами и (или) абонентскими устройствами в организациях, предоставляющих услуги связи.

2. Сведения, содержащиеся в переписке, должны носить личный характер, т.е. отражать отдельные стороны частной жизни конкретного человека (содержание переписки служебного или рекламного характера не образует тайну связи). Необходимо помнить, что в соответствии с решением Конституционного Суда РФ от 2 октября 2003 г. №435-О тайной связи является не только непосредственно текст переданного или полученного сообщения, но и информация о самом факте отправки или получения сообщения, адресате, времени и т.д. Адрес электронной почты, IP-адрес и другие идентификаторы к тайне связи относить нельзя. [3]

3. Переписка или иная информация должна находиться в ограниченном доступе, то есть доступ к ней должен иметь не любой пользователь сети Интернет, а только тот, кого определил отправитель (переписка в открытых чатах, комментариях к чему-либо тайну связи составлять не может).

При наличии указанных признаков получение и (или) просмотр интернет-переписки должны расцениваться как ограничение тайны связи и в соответствии с ч. 2 ст. 23 Конституции РФ требуют обязательного получения судебного решения.

Следующий важный вопрос, который необходимо разрешить: посредством какого следственного действия может быть получена интернет-переписка. Анализ материалов следственной практики территориальных органов ФСКН России и МВД России позволяет привести несколько возможных вариантов.

Первый заключается в том, что следователь получает судебное решение о наложении ареста на почтово-телеграфные отправления (ст. 185 УПК РФ), их осмотр и выемку в учреждениях связи, после чего производит выемку и осмотр переписки, представленной либо на электронном носителе, либо в виде распечатанного текста. Нам такой вариант представляется неприемлемым, поскольку, во-первых, данное следственное действие направлено на ознакомление с бандеролями, посылками, другими почтово-телеграфными отправлениями либо телеграммами или радиограммами (такой вывод следует из анализа положений Федерального закона "О почтовой связи", что позволяет прийти к выводу, что интернет-переписка к предметам регулирования ст. 185 УПК РФ не относится). Во-вторых, данное следственное действие подразумевает "задержание" отправления до его получения адресатом, тогда как в большинстве случаев следствие интересуется интернет-перепиской за предшествующий период (то есть уже полученная адресатом).

Достаточно распространены случаи получения интернет-переписки в ходе выемки предметов и документов, содержащих



охраняемую федеральным законом тайну, которая производится непосредственно у представителя оператора связи на основании полученного следователем судебного решения. С учетом положений ст. 13 и п. 7 ч. 2 ст. 29 УПК РФ данный подход можно признать в полной мере законным и обоснованным, однако в силу расположения организаций, владеющих серверами крупных социальных сетей и других коммуникационных сервисов (г. Москва, г. Санкт-Петербург) производство таких выемок становится достаточно затратным как по времени, так и по средствам реализации, а в случае нахождения сервера за пределами Российской Федерации (электронные почтовые ящики вида @gmail.com, @google.com, @hotmail.com, социальная сеть Facebook) – практически невозможным.

Встречаются случаи производства следственного эксперимента, в ходе которого лицо, чья переписка представляет интерес, самостоятельно заходит на соответствующий ресурс сети Интернет и, открывая входящие и исходящие сообщения, позволяет следователю зафиксировать в протоколе их содержание. Стоит отметить, что данный подход не лишен логики, поскольку результат совершаемых действий заранее не известен (страница в сети Интернет может быть удалена, изменена и т.д.), а цели в общем соответствуют заявленным в ст. 181 УПК РФ (проверяется возможность восприятия каких-либо фактов, совершения определенных действий, наступления какого-либо события, а также выявляются последовательность произошедшего события и механизм образования следов). Также к допустимым, на наш взгляд, можно отнести случаи производства такой разновидности компьютерно-технической экспертизы, как компьютерно-сетевая, в ходе которой могут быть получены сведения о переписке, однако примеров её фактического проведения в ходе изучения материалов найти не удалось.

Также одним из приемлемых, на наш взгляд, вариантов является фиксация интернет-переписки в ходе такого оператив-

но-розыскного мероприятия, как снятие информации с технических каналов связи, с дальнейшим предоставлением материалов следователю в качестве результатов оперативно-розыскной деятельности, при этом все рассмотренные в данной статье требования об обеспечении права на тайну связи также должны быть учтены. Единственным препятствием реализации такого подхода в рамках возбужденного уголовного дела может выступить запрет на подмену оперативно-розыскными мероприятиями процессуальных действий, для осуществления которых уголовно-процессуальным законом установлена специальная процедура [2], однако, как мы смогли убедиться, таковой УПК РФ как раз не предусматривает.

Одним из вариантов дистанционной фиксации интернет-переписки является её осмотр, производимый с использованием компьютера, подключенного к сети Интернет. Говоря об осмотре как о следственном действии, необходимо отметить, что ст. 176 УПК РФ предусматривает два наиболее подходящих к нашей ситуации варианта – осмотр предметов и осмотр документов. Автору встречались примеры осмотра страницы сети Интернет посредством такого следственного действия, как осмотр предметов, в протоколе которого следователь указывал, что объектом осмотра является компьютер, однако нужно понимать, что фиксируемые данные находятся не в памяти компьютера, который в данном случае выступает лишь используемым техническим средством.

За неимением ничего более подходящего мы предлагаем использовать в подобных случаях протокол осмотра электронного документа (электронным документом предлагаем считать интернет-страницу). Данная позиция косвенно подтверждается положениями Федерального закона от 27 июля 2006 г. №149-ФЗ "Об информации, информационных технологиях и защите информации".

Вне зависимости от средства фиксации очень остро встает вопрос о необходимости получения судебного решения для оз-



накомления с интернет-перепиской. На примере осмотра разберем две исходные ситуации:

1) лицо, чья переписка подлежит фиксации, установлено и согласно с осмотром своей переписки;

2) лицо, чья переписка подлежит фиксации, не установлено либо не дает согласия на осмотр.

В первом случае целесообразно получить письменное согласие на ознакомление с личной перепиской, после чего с использованием логина и пароля, предоставленных участвующим в осмотре лицом, осуществляется доступ к входящим и исходящим сообщениям. Решение вопроса о допустимости ознакомления с интернет-перепиской при наличии согласия лица зависит от признания права на тайну связи в полной мере неотчуждаемым (как право на неприкосновенность жилища при производстве обыска в жилище) либо допускающим ограничение с согласия правообладателя (как в случае производства осмотра жилища). В ст. 17 Конституции РФ говорится о том, что основные права и свободы человека неотчуждаемы и принадлежат каждому от рождения, однако решению поставленного вопроса данное положение не способствует. В то же время положения ч. 2 ст. 186 УПК РФ указывают на возможность производства контроля и записи телефонных переговоров отдельных лиц при наличии угроз на основании их письменного заявления (без получения судебного решения), что косвенно подтверждает возможность правообладателя частично распоряжаться своим правом на тайну связи.

Во второй ситуации ознакомление с перепиской в любом случае может быть произведено только после получения судебного решения на производство осмотра (следственного эксперимента, экспертизы). Предложенный вариант также не бесспорен, поскольку ст. 29 УПК РФ не предус-

матривает принятие подобных решений судом, однако представляется, что суд в данном случае может применить не запрещенную в уголовном процессе аналогию закона, используя право на принятие решения о производстве выемки предметов и документов, содержащих иную охраняемую федеральным законом тайну (п. 7 ч. 2 ст. 29 УПК РФ).

Помимо получения судебного решения отсутствие согласия лица предполагает необходимость получения логина (или иного идентификатора) и пароля к нему. Доступ к соответствующему электронному сервису может быть получен посредством:

- осмотра изъятой компьютерной техники или судебной экспертизы (при стандартных настройках логины и пароли сохраняются в браузере либо в системных файлах);

- подбора пароля (существуют специальные справочники и программные средства);

- использования логина и пароля, имеющих в материалах уголовного дела (сведения могут быть получены в результате оперативно-розыскной деятельности, анализа личных записей лица, а также получены у оператора связи).

Рассмотренные аспекты раскрывают проблему получения и процессуальной фиксации интернет-переписки далеко не в полной мере. Так, зачастую в следственной практике возникает вопрос о возможности ознакомления с перепиской на сервере при проведении обыска в жилище (при наличии судебного решения); далеко не однозначно разрешается вопрос о получении удаленной с сервера переписки и т.д. Проведенный анализ позволяет наметить направления дальнейших исследований с целью обеспечения законности, эффективности и оптимизации деятельности сотрудников следственных подразделений.



Библиографический список

1. О связи : Федеральный закон от 07 июля 2003 г. №126-ФЗ // СПС Консультант-Плюс.
2. Определение Конституционного Суда РФ от 25 февраля 2010 г. № 261-О-О // СПС КонсультантПлюс.
3. Постановление Девятого арбитражного апелляционного суда от 19 сентября 2013 г. по делу № А40-56844/2013 // СПС КонсультантПлюс.
4. Карлов, А.Л. Правовой режим использования в доказывании по уголовным делам электронной переписки, содержащейся в памяти технических средств коммуникации / А.Л. Карлов // Актуальные проблемы профилактики наркомании и противодействия правонарушениям в сфере легального и незаконного оборота наркотиков: национальный и международный уровни : материалы XVII международной научно-практической конференции (17-18 апреля 2014 года). – Красноярск: СибЮИ ФСКН России, 2014. – Ч 2. – С.194-198.