Правоведение

УДК 343.98

С.В. Баринов

СЛЕДЫ ПРЕСТУПНЫХ НАРУШЕНИЙ НЕПРИКОСНОВЕННОСТИ ЧАСТНОЙ ЖИЗНИ КАК ЭЛЕМЕНТ КРИМИНАЛИСТИЧЕСКОЙ ХАРАКТЕРИСТИКИ

Рассматриваются вопросы всестороннего изучения такого важного элемента криминалистической характеристики нарушений неприкосновенности частной жизни, как сведения о типичных следах преступлений. Выделены три группы следов преступных нарушений неприкосновенности частной жизни: материальные, идеальные и виртуальные. Определено значение каждой группы следов для расследования. Установлено, что в связи с наблюдаемым ростом количества преступных нарушений неприкосновенности частной жизни, совершенных в сети Интернет, важное значение в процессе выявления и расследования приобретают виртуальные следы. Обращено внимание на то, что одним из факторов, осложняющих проведение следственного осмотра, следует признать огромный массив компьютерной информации, необходимость изучения которой может возникнуть в ходе расследования. Даны некоторые рекомендации по соблюдению требований уголовно-процессуального законодательства, которые необходимо учитывать при изъятии электронных носителей информации в ходе производства обыска и выемки. Сделан вывод о том, что следы рассматриваемой группы преступлений в значительной степени зависят от выбранного преступниками способа доступа к сведениям о частной жизни, фиксации и обработки информации, ее распространения.

Ключевые слова: неприкосновенность частной жизни, преступные нарушения неприкосновенности частной жизни, следы преступлений, виртуальные следы.

Группу преступных нарушений неприкосновенности частной жизни образуют преступные деяния, ответственность за совершение которых установлена ст. 137-139 УК РФ. Криминалистическая характеристика преступных нарушений неприкосновенности частной жизни представляется нами как система обобщенных криминалистически значимых сведений (данных) о преступлениях рассматриваемой группы, знание которых призвано способствовать верному выбору лицом, производящим расследование, наиболее эффективных методов, приемов и средств, используемых для обнаружения, раскрытия, расследования и предотвращения указанных преступлений. В типовой криминалистической характеристике преступных нарушений неприкосновенности частной жизни выделяются следующие элементы: предмет преступного посягательства, мотив и цель совершения преступления, способы совершения, сведения о времени и обстановке преступлений, характеристика личности преступника [1. С. 5-7]. Сведения о типичных следах совершения преступлений автор рассматривает также в качестве одного из основных элементов типовой криминалистической характеристики данной группы преступлений.

Значение следов в криминалистике трудно переоценить. Практическую криминалистику фактически можно признать следоведением, то есть наукой о закономерностях следообразования в результате преступной деятельности, а также об установлении и исследовании следов в целях изобличения преступников. Сам термин «след» является основой для понятий «следователь» и «расследование». Успешность расследования преступления напрямую зависит от результатов реализации действий по выявлению, изъятию и исследованию следов преступной деятельности.

В то же время О.Я. Баев отмечает, что «следом является не каждое из неисчерпаемого количества “всех самых разнообразных материальных изменений”, связанных с преступлениями, а лишь те из них, которые на современном этапе развития криминалистики осознаются в этом качестве. Осознаются как следы, возникшие в результате преступной деятельности либо с ней связанные причинно, и, что главное, которые мы в настоящее время умеем обнаруживать, фиксировать, изымать, исследовать и использовать в целях познания, реконструкции преступных событий» [2. С. 234].

Значительный вклад в изучение понятия «след» и механизма следообразования внесли исследования таких ученых, как И.Н. Якимов, Л.К. Литвиненко, Д.А. Турчин, Б.И. Шевченко, Г.Л. Грановский, И.Ф. Крылов, Р.С. Белкин.

Традиционно в исследованиях криминалистов выделялись материальные и идеальные следы. Однако в связи с распространением преступлений, совершаемых с использованием цифровых информационных технологий, возникает необходимость введения ещё одной формы, которая бы смогла объективно представить понятие механизма следообразования в виртуально-информационной сфере [3. С. 148]. Речь идет о «виртуальных следах», формирующихся в автоматизированных информационных системах и обладающих свойствами идеальных и материальных следов. В связи с вышеизложенным среди следов преступных нарушений неприкосновенности частной жизни нами выделяются материальные, идеальные и виртуальные.

Материальные следы преступления – это «результаты материального отражения свойств взаимодействующих в ходе преступной деятельности материальных объектов, исследование которых позволяет формировать доказательственную информацию об отдельных обстоятельствах совершенного преступления» [4. С. 263]. Материальные следы принято подразделять на следы-отображения, следы-предметы и следы-вещества.

Наиболее традиционными в трасологии считаются следы-отображения, которые появляются в процессе воздействия одного материального объекта на другой и представляют собой воспроизведение в различных формах особенностей отображаемого объекта. Однако специфической чертой следовой картины рассматриваемой группы преступлений является то, что классические материальные следы-отображения (рук, ног, инструментов, приспособлений и т. п.) должны выявляться, но их значение зачастую не будет первостепенным.Такие следы могут оставаться на месте совершения преступления, а также присутствовать на материальных объектах, используемых в процессе хранения информации. Наиболее вероятными местами обнаружения данных следов являются:

– средства управления, которые применялись в процессе совершения преступления техническими средствами (манипуляторы: клавиатура, мышь, стилус, сенсорный экран и т.д.);

– поверхности технических средств: рабочие, наружные и внутренние (особенно при наличии признаков модификации устройств);

– средства упаковки;

– места крепления, присоединения к сети;

– средства обеспечения энергией (кнопки включения/выключения, электророзетки, аккумуляторы, блоки питания, блоки бесперебойного питания, электроудлинители и т.д.).

Количество следов-отображений будет тем больше, чем более контактный способ получения информации был выбран преступниками. Например, целую группу специфических следов взлома запорных устройств можно обнаружить при незаконном проникновении в жилище.

Следы-предметы могут встречаться в виде различных специальных технических средств получения и обработки информации, компьютерной техники, периферийных устройств, носителей информации, других предметов, а также их отдельных частей.

При обнаружении таких следов-предметов необходимо определить возможность их изъятия. Как показывает следственная практика, обнаружение, фиксация и приобщение к материалам дела следов-предметов совершения преступлений оказывает положительный эффект на ход расследования.

Наибольшая вероятность обнаружения следов-веществ возникает при совершении нарушения неприкосновенности частной жизни, заключающемся в распространении сведений о частной жизни лица, составляющих его личную или семейную тайну, в печатных средствах массовой информации. Так, например, используемые в полиграфии красители могут быть исследованы в целях установления соответствия с оригиналами печатной продукции.

Преступные нарушения неприкосновенности частной жизни относятся к группе информационных преступлений, под которыми понимаются «общественно опасные противоправные деяния, причиняющие вред общественным отношениям по обеспечению информационной безопасности, способом совершения которых является информационное воздействие или (и) предметом которых является информация как особый нематериальный объект» [5. С. 7].

Как следует из приведенного определения, именно информация считается предметом преступного посягательства. Данное обстоятельство обусловливает придание особого значения именно информационным (идеальным) следам преступлений.

В соответствии с положениями ст. 2 Федерального закона от 7 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» под информацией понимаются любые сведения (сообщения, данные) независимо от формы их представления. Информацией о част-

ной жизни в таком случае будут являться любые сведения (сообщения, данные), составляющие личную или семейную тайну лица независимо от формы их представления.

К группе идеальных следов относятся отражения преступного деяния в виде образов событий и обстоятельств совершения преступления, зафиксированных в памяти человека. О.Я. Баев, называя такие следы интеллектуальными, или памятными следами, относит к ним отпечатки события в сознании, памяти людей, совершивших преступление и (или) к нему прикосновенных (например, укрыватели преступления и т.п.), потерпевших от преступления, очевидцев, других свидетелей и т. д. [6. С. 57]. К типичным идеальным следам, нашедшим отражение в их памяти, можно отнести сведения:

1) непосредственно составляющие личную или семейную тайну лица;
2) о форме представления информации;
3) об оценке достоверности информации;
4) о конфиденциальности информации;
5) о мерах, принимаемых для защиты информации;
6) о лицах, имевших доступ к информации;
7) об обстоятельствах совершения преступления;
8) о дальнейших действиях с информацией.

Современный этап развития общества, как отмечено в Доктрине информационной безопасности Российской Федерации (утв. Президентом РФ 09.09.2000 № Пр-1895), характеризуется возрастающей ролью информационной сферы. Одним из наиболее важных факторов, влияющих на формирование общества XXI в., является появление таких информационно-телекоммуникационных систем, как Интернет – международная сеть соединенных между собой компьютеров, уникальное средство всемирной коммуникации [7. С. 380].

В то же время сформировавшаяся новая среда общественных отношений – киберпространство считается в высокой степени уязвимой для совершения разного рода преступных действий. Правоведы вполне обоснованно выделяют самостоятельный вид преступности, совершаемой с использованием компьютеров и/или через Интернет – киберпреступность. Компьютерные преступления против личных прав и неприкосновенности частной сферы выделяются как отдельная группа киберпреступлений [8].

В связи с наблюдаемым ростом количества преступных нарушений неприкосновенности частной жизни, совершенных в сети Интернет, важное значение в процессе выявления и расследования приобретают так называемые виртуальные следы, под которыми, по мнению В.А. Мещерякова, следует понимать «любое изменение состояния автоматизированной информационной системы (образованного ею “кибернетического пространства”), связанное с событием преступления и зафиксированное в виде компьютерной информации (т.е. информации в виде, пригодном для машинной обработки) на материальном носителе, в том числе и на электромагнитном поле» [9. С. 21]. В данном случае необходимо обратить внимание на включение в содержание компьютерной информации всей информации, которая может быть обработана ЭВМ. Это утверждение обоснованно в связи с тем, что такого рода информация может оставаться не только в компьютерных, но и в иных цифровых устройствах (в мобильных телефонах, диктофонах, фото- и видеокамерах и т.д.).

К принципиальным особенностям виртуальных следов относят следующие:

а) формирование виртуальных следов (электронно-цифровое отражение) происходит в искусственно созданной среде (компьютерной системе);

б) цифровой вид записи параметров, используемой в регистрирующем устройстве формализованной модели, приводит к возможности априорной оценки его изобразительных возможностей при фиксации реального физического явления;

в) виртуальный след не имеет физически целостной структуры;

г) зафиксированный на цифровом носителе виртуальный след представляет собой сложную информационную структуру, в которой, наряду со значимой (смысловой уголовно-релевантной) информацией, содержится значительный объем вспомогательных данных, отвечающих за целостность и доступность компьютерной информации виртуального следа [10. С. 8].

Наиболее популярным способом совершения рассматриваемой группы преступлений в сети Интернет в настоящее время является распространение сведений, составляющих личную или семейную тайну. Распространяется чаще всего фото- или видеоизображение, запечатлевшее потерпевших в интимной обстановке, а также их аудиозаписи и номера телефонов. Такие сведения могут сопровождаться оскорбительными характеристиками. Достаточно часто встречается размещение ложного предложения, например, об оказании потерпевшей услуг интимного характера.

Распространение информации о частной жизни может производиться адресно: направление сообщения с вложенными файлами сожителю, соседям, знакомым, работодателю, а также безадресно: путем размещения в социальных сетях («Мой мир», «ВКонтакте», «Одноклассники»), на сайтах знакомств, на порнографических ресурсах. Таким образом, в качестве источников виртуальных следов преступных нарушений неприкосновенности частной жизни могут рассматриваться веб-страницы пользователей сети Интернет.

При совершении преступного нарушения неприкосновенности частной жизни в форме незаконного собирания сведений, составляющих личную или семейную тайну лица, следы неправомерного доступа к компьютерной информации могут отражаться в виде изменений в хранящейся на магнитных носителях информации. Таковыми могут являться следы уничтожения или модификации информации (удаление из каталогов имен файлов, стирание или добавление отдельных записей, физическое разрушение или размагничивание носителей) [11. С. 117]. При исследовании компьютера потерпевшего следует учитывать такую верно подмеченную А.Ю. Семеновым особенность, что на компьютере-«жертве» преступнику сложнее уничтожить виртуальные следы, но они и несут меньше информации, полезной для расследования преступлений [12. С. 54].

Анализируя механизм «виртуально-информационного следообразования», П.В. Мочагин отмечает, что его можно найти при работе и с беспроводными технологиями *blue-ray*, *bluetooth*, *wi-fi* и т.д., а также при хищении информации с помощью технического устройства, которое позволяет считывать электронно-цифровое отражение с экрана компьютерного монитора и при записи человеческого голоса на расстоянии и т.д. [13. С. 192]

В зависимости от вида физических носителей виртуальных следов А.Г. Волеводз выделяет:

1) следы на жестком диске (винчестере), магнитной ленте («стримере»), оптическом диске (CD, DVD), на дискете (флоппи диске);

2) следы в оперативных запоминающих устройствах (ОЗУ) ЭВМ;

3) следы в ОЗУ периферийных устройств (например, лазерного принтера);

4) следы в ОЗУ компьютерных устройств связи и сетевых устройств;

5) следы в проводных, радио-оптических и других электромагнитных системах и сетях связи [14. С. 159-160].

Приведенную классификацию следует учитывать при проведении отдельных следственных действий. Одним из факторов, осложняющих, например, проведение следственного осмотра, следует признать огромный массив компьютерной информации, необходимость изучения которой может возникнуть в ходе расследования. Так, согласно подсчетам, сделанным В.Ю. Агибаловым, на осмотр содержимого винчестера объемом 1 ТБ, который может содержать до 50 млн страниц в текстовом редакторе Word, потребуется минимум полтора года непрерывной работы [15. С. 103-104]. На практике, если для производства следственного осмотра виртуальных следов преступления требуется продолжительное время или осмотр на месте затруднен, то в соответствии с требованиями ч. 3 ст. 177 УПК РФ предметы осмотра должны быть изъяты.

Следует также учитывать, что изъятие электронных носителей информации при производстве обыска и выемки в соответствии с требованиями ч. 9.1 ст. 182 и ч. 3.1 ст. 183 УПК РФ должно производиться с участием специалиста.

По ходатайству законного владельца изымаемых электронных носителей информации или обладателя содержащейся на них информации специалистом, участвующим в обыске или выемке, в присутствии понятых с изымаемых электронных носителей информации осуществляется копирование информации. Копирование информации осуществляется на другие электронные носители информации, предоставленные законным владельцем изымаемых электронных носителей информации или обладателем содержащейся на них информации. При производстве обыска не допускается копирование информации, если это может воспрепятствовать расследованию преступления либо, по заявлению специалиста, повлечь за собой утрату или изменение информации. Электронные носители информации, содержащие скопированную информацию, передаются законному владельцу изымаемых электронных носителей информации или обладателю содержащейся на них информации. Об осуществлении вышеописанных действий законному владельцу изымаемых электронных носителей информации или обладателю содержащейся на них информации в протоколе делается запись.

В отдельных случаях для обнаружения и фиксации виртуальных следов преступных нарушений неприкосновенности частной жизни необходимо применять специальные аппаратные и технические

средства. В соответствии с положениями ч. 3 ст. 180 УПК РФ о применении таких средств должно быть указано в протоколе осмотра.

В отдельную следовую группу преступных нарушений неприкосновенности частной жизни можно выделить следы преодоления средств защиты от постороннего доступа. Наличие таких средств предполагает необходимость совершения преступниками дополнительных действий, которые могут заключаться, например, в проведении контрольных прозвонов телефонного номера, выведении из строя сигнализации, кибератаках, подборе паролей, использовании имени и кода доступа посторонних лиц, запуске программ, присваивающих преступнику функции системного администратора и т.д. Совершение вышеуказанных действий становится возможным при наличии определенного «арсенала» средств, которые могут быть использованы преступниками (хакерские программы, реестры пользователей и паролей, технические средства и т.д.) и обнаружены при проведении следственных действий.

Таким образом, следы рассматриваемой группы преступлений в значительной степени зависят от выбранных преступниками способов доступа к сведениям о частной жизни, фиксации и обработки информации, ее распространения. По описанным нами группам следов преступных нарушений неприкосновенности частной жизни субъекты расследования смогут установить способ совершения преступления и иные обстоятельства, имеющие значение для дела.

СПИСОК ЛИТЕРАТУРЫ

1. Юрин В.М., Баринов С.В. Расследование преступных нарушений неприкосновенности частной жизни: учеб. пособие. М.:: А-Приор, 2009.
2. Баев О.Я. Уголовно-процессуальное доказательство: атрибутивные признаки и качество // Российский журнал правовых исследований. 2015. № 1 (2).
3. Мочагин П.В. Виртуально-информационный и невербальный процесс отражения следообразований как новое направление в криминалистике и судебной экспертизе // Вестн. Удм. ун-та. Сер. Экономика и право. 2013. Вып. 2.
4. Мороз А.В. Понятие «материальные следы преступления» // Общество и право. 2010. №5 (32).
5. Суслопаров А.В. Информационные преступления : автореф. дис. ... канд. юрид. наук. Красноярск, 2008.
6. Баев О.Я. Основы криминалистики: курс лекций. М., 2001.
7. Российская юридическая энциклопедия. М.: Изд. дом «ИНФРА-М», 1999.
8. Бекряшев А.К., Белозеров И.П. Теневая экономика и экономическая преступность: электронный учебник. URL: http://www.juristlib.ru/book_3349.html.
9. Мещеряков В.А. Основы методики расследования преступлений в сфере компьютерной информации : автореф. дис. ... докт.юрид.наук. Воронеж, 2001.
10. Агибалов В.Ю. Виртуальные следы в уголовном процессе и криминалистике: автореф. дис. ... канд. юрид. наук. Воронеж, 2010.
11. Расследование неправомерного доступа к компьютерной информации / под ред. Н.Г. Шурухнова. М.: Щит-М, 1999.
12. Семенов А.Ю. Некоторые аспекты выявления, изъятия и исследования следов, возникающих при совершении преступлений в сфере компьютерной информации // Сибирский юридический вестник. 2004. № 1.
13. Мочагин П.В. О пяти механизмах следообразований, их кодах и информационном содержании // Вестн. Удм. ун-та. Сер. Экономика и право. 2015. Вып. 1.
14. Волеводз А.Г. Противодействие компьютерным преступлениям. М., 2002.
15. Агибалов В.Ю. Виртуальные следы в криминалистике и уголовном процессе: монография. М.: Юрлитинформ, 2012.

Поступила в редакцию 09.11.15

S.V. Barinov

VESTIGES OF CRIMINAL VIOLATIONS OF PRIVACY AS AN ELEMENT OF CRIMINALISTIC CHARACTERISTICS

The paper discusses issues of a comprehensive study of such important element of criminalistic characteristics of privacy violations as information about typical signs of a crime. Three groups of traces of criminal violations of privacy have been distinguished: material, ideal, and virtual. The value of each group of traces for investigation has been determined. It is established that in connection with the observed increase in the number of criminal violations of privacy committed in the Internet, virtual traces become important in the process of crime detection and investigation. Attention is drawn to the fact that one of the factors complicating the investigative inspection is a huge array of computer information which may be

necessary to study during the investigation. The author gives some recommendations on compliance with the criminal procedural law that must be considered in the case of electronic media seizure during search and seizure. It is concluded that vestiges of considered group of crimes largely depend on the way chosen by criminals to access information about the private life, to clamp and process this information, as well as to distribute it.

Keywords: personal privacy, criminal breach of privacy, vestiges of a crime, virtual traces.

Баринов Сергей Владимирович,
кандидат юридических наук

Филиал военного учебно-научного центра
Военно-воздушных сил
«Военно-воздушная академия имени профессора
Н.Е. Жуковского и Ю.А. Гагарина» (г. Сызрань)
446012, Россия, г. Сызрань, ул. Маршала Жукова, 1;

Сызранский филиал ФГБОУ ВО «Самарский
государственный экономический университет»
446022, Россия, г. Сызрань, ул. Людиновская, 23
E-mail: metel2000@rambler.ru

Barinov S.V., Candidate of Law

Syzran Branch of Air Force Educational
and Science Center
«N.E. Zhukovsky and Yu.A. Gagarin Air Force Academy»
Marshala Zhukova st., 1, Syzran, Russia, 446012

Syzran branch of Samara State University of Economics
Lydinovskaya st., 23, Syzran, Russia, 446022
E-mail: metel2000@rambler.ru