УДК 343.98

М.А. Новикова

ОБНАРУЖЕНИЕ СЛЕДОВ ЭЛЕКТРОННЫХ УСТРОЙСТВ В ПРОЦЕССЕ РАССЛЕДОВАНИЯ РАЗГЛАШЕНИЯ ДАННЫХ ПРЕДВАРИТЕЛЬНОГО РАССЛЕДОВАНИЯ

Рассматриваются проблемы обнаружения, изъятия и обработки электронных (виртуальных, цифровых) следов при расследовании преступления, заключающегося в разглашении данных предварительного расследования. Анализируются возможности современной криминалистической техники при работе с изъятыми электронными устройствами подозреваемых и обвиняемых. Предлагается методика осмотра изъятых аппаратов в целях обеспечения максимальной сохранности информационной среды устройства.

Ключевые слова: разглашение данных предварительного расследования, электронный след, электронное цифровое устройство, информационная среда устройства.

M.A. Novikova

DETECTION OF TRACES OF ELECTRONIC DEVICES DURING THE INVESTIGATION DISCLOSURE OF PRELIMINARY INVESTIGATION DATA

The article deals with the problems of detecting, removing and processing electronic (virtual, digital) traces in the investigation of a crime involving the disclosure of preliminary investigation data. The possibilities of modern forensic technology when working with seized electronic devices of suspects and accused persons are analyzed. The method

of inspection of the seized devices is proposed in order to ensure maximum safety of the device's information environment.

Keywords: the disclosure of preliminary investigation data, electronic signature, electronic digital device, the information device environment.

«Под разглашением данных предварительного расследования вопреки установленному запрету, изложенному в подписке о неразглашении, следует понимать их необоснованное предание огласке – без согласия субъекта расследования, независимо от формы такого сообщения, передачи либо доведения их до сведения хотя бы одного постороннего лица, если разглашением был причинен вред интересам предварительного расследования, правам и законным интересам участников уголовного судопроизводства» [1].

При этом в качестве постороннего лица можно признать любого гражданина, который:

1) не обладает этой информацией;

2) не имеет права в силу своего служебного или процессуального положения либо характера порученной работы иметь доступ к этой информации или получить ее от конкретного лица;

3) не имеет отношения к числу субъектов, которые получили разрешение от следователя передать соответствующую информацию.

К наиболее *характерным способам* разглашения данных предварительного расследования следует отнести:

«1) предоставление в средства массовой информации ксерокопий, видео-, фотоматериалов уголовного дела, составляющих тайну предварительного расследования;

2) выступления в СМИ защитников подозреваемых (обвиняемых), работников правоохранительных органов

разного уровня, разглашающих данные, составляющие тайну предварительного расследования;

3) передача данных об участниках уголовного судопроизводства иным лицам;

4) сообщение сведений о показаниях обвиняемых, свидетелей и иных участников уголовного судопроизводства иным лицам;

5) передача сведений иным лицам о ранее данных показаниях самим лицом, которое эти сведения сообщило;

6) ознакомление посторонних лиц с копиями процессуальных документов, официально полученных участниками уголовного судопроизводства в ходе расследования уголовного дела;

7) передача из ИВС, СИЗО и в обратном направлении записок, писем и т.д., содержащих информацию о расследовании дела, а также сотовых телефонов и других передающих устройств;

8) передача сведений о следственных версиях, планируемых следственных действиях, о направленных следователем запросах, о предоставлении тех или иных документов, характеристик, справок и т.д.» [2].

В условиях постоянно развивающегося технического прогресса передача данных, составляющих тайну предварительного расследования, осуществляется посредством использования разнообразных девайсов, или цифровых (электронно-цифровых) устройств. В связи с этим можно утверждать, что технические устройства, обеспечивающие передачу информации и ее обработку, также хранят в своей памяти следы преступных действий, образуя новую для криминалистики категорию виртуальных (компьютерных, электронных, цифровых) следов, выделяемую наравне с материальными и идеальными следами преступления. Под виртуальными следами предлагается понимать криминалистически значимую информацию, имеющую доказательственное значение, возникающую ввиду функционирования электронных устройств и хранящуюся на цифровых носителях [3, 4].

Иными словами, виртуальный, или электронный, след – это совокупность данных, передача которых осуществлена посредством их преобразования в электрические сигналы, при этом в данных целях могут использоваться любые средства обработки информации, ее передачи и хранения.

В то же время выделение категории виртуальных следов является весьма условным, так как в сущности электронный (цифровой, компьютерный) след есть не что иное, как невидимый материальный след, имеющий специфический механизм возникновения, в основе которого – электромагнитное взаимодействие как минимум двух заряженных тел, выступающих объективной формой представления электронных данных.

Одни и те же с точки зрения формы материальные объекты, участвующие в электромагнитном взаимодействии, могут быть и следообразующими, и следовоспринимающими. Речь идет как о непосредственно электромагнитных сигналах, так и о базах данных, программном обеспечении, файлах, интернет-сайтах и интернет-страницах, электронных документах, подписях, сообщениях, журналах, электронных денежных средствах и др.

Нельзя не отметить, что в современной криминалистике вопросы следообразования, связанного с преступной деятельностью в виртуальной среде, остаются в большинстве своем неразрешенными, а потому сохраняют особую актуальность. Дискуссионными на сегодняшний день можно считать проблемы определения формы и механизма электронного следообразования, разграничения следообразующих и следовоспринимающих объектов с уточнением данных дефиниций применительно к виртуальным следам, установления момента следового контакта и места последнего в традиционной классификации [5].

Любые действия человека, совершенные с использованием электронно-технических устройств (как стацио-

нарных, так и мобильных), обязательно отпечатываются в памяти девайса. Так, например, ставшие непременным атрибутом современной жизни мобильные телефоны сохраняют в памяти информацию о контактах владельца, в связи с чем следы телефонного разговора или переписки фиксируются сразу на двух устройствах: передающем и принимающем. Поэтому в случае разглашения данных предварительного расследования посредством использования сотовой связи следы этого преступного деяния образуются в мобильных телефонах обоих участников разговора либо переписки: и разглашателя, и получателя конфиденциальных сведений.

Все переданные с помощью мобильной связи данные могут быть отнесены к следам. В то же время осязаемые материальные следы в таком случае не образуются, а то, что с точки зрения криминалистики признается следом, на самом деле является только его математической моделью, конструируемой посредством электронного синтеза. Отсюда потребность в выделении особой категории следов – электронных (компьютерных, виртуальных, цифровых, информационно-технологических и др.).

Фиксируемые цифровыми устройствами данные имеют свою специфику, в связи с чем их обработка и криминалистический анализ требуют специальной подготовки в сфере IT.

Так, в случае изъятия у подозреваемого или обвиняемого по делу о разглашении данных предварительного расследования средства мобильной связи обязательно должен быть проведен осмотр последнего, осуществляемый в три этапа.

Первый этап сопряжен с внешним осмотром, предполагающим выявление и фиксацию присущих устройству внешних признаков, а также характеристику его состояния. Протокол, составляемый в ходе проводимого следственного действия, должен на этом этапе отражать марку гаджета, его модель, тип и форму устройства.

Второй этап может быть охарактеризован как конструктивный осмотр. Он предполагает описание отдельных частей конструкции аппарата: передней и задней панелей, аккумулятора, разъемов, слотов, камеры (при наличии), SIM-карты и карт памяти.

Третий этап связан с осмотром непосредственно информационной среды, то есть данных, хранящихся в памяти устройства (внутренней, внешней и оперативной), а также на SIM-картах и SD-картах [6].

В том случае, когда осмотр устройства мобильной связи сопровождается его включением субъектом расследования, благодаря чему становятся доступными функции аппарата и сохраненные на нем данные, протокол следственного действия должен отражать абсолютно все операции с телефоном, зафиксированные строго в хронологическом порядке. Кроме того, этапы конструктивного осмотра и осмотра информационной среды могут меняться местами в том случае, если аппарат, в отношении которого проводится следственное действие, на момент начала осмотра является включенным.

Необходимо иметь в виду, что данные, полученные в результате осмотра используемых подозреваемым или обвиняемым в разглашении конфиденциальной информации средств связи, приобщаются к уголовному делу как доказательства. Причем это касается как входящих, так и исходящих сведений. Информация извлекается из электронных устройств путем использования криминалистической техники с применением цифровых технологий, что позволяет восстановить даже те материалы, которые были стерты пользователем – как разглашателем данных предварительного расследования, так и лицом, эти данные получившим, начиная с момента поступления информации о факте разглашения. Причем такая кримтехника дает возможность обрабатывать информацию, хранящуюся в памяти гаджетов почти любой модификации (в том числе компьютеров и ноутбуков с разны-

ми операционными системами, смартфонов, планшетов, навигаторов и пр.), а также извлекать данные из аппаратов с разной степенью повреждения.

Возможности данной криминалистической техники таковы, что позволяют обходить логины и пароли при проникновении в систему, извлекать данные из сотовых телефонов даже в отсутствие аккумуляторной батареи, исследовать SIM-карту без аппарата. Таким образом, появляется возможность получения и систематизации как сохраненной, так и удаленной пользователем информации в рамках структурированного отчета.

Ведя расследование по делу о разглашении данных предварительного расследования, субъект расследования при проведении следственных действий (обыска, осмотра, выемки) вправе осуществить изъятие различных электронных устройств, которые, предположительно, могут содержать виртуальные следы. Упаковка и опечатка девайсов должна обеспечивать сохранность информационной среды устройства. Особое внимание должно быть уделено опечатке портов, разъемов, слотов, к котором следует прикрепить пояснительные записи, удостоверенные подписями субъекта расследования, специалиста, понятых и иных участников следственного действия.

Чтобы провести исследование изъятых электронных следов, требуется использование специальных знаний. Субъекту расследования следует вынести постановление о назначении экспертизы, причем в зависимости от объекта, который необходимо исследовать, может быть назначен один из следующих видов экспертизы: компьютерно-техническая, программная либо сетевая. Выданное по результатам экспертизы заключение приобщается к делу как доказательство.

Данные, хранящиеся на изъятых субъектом расследования электронных устройствах, должны быть скопированы на специальную карту памяти или же на

стационарное устройство для последующей их обработки с помощью приложения «UFED Physical Analyzer». Результатом использования данного программного продукта становится автоматическое составление структурированного отчета с высокой степенью детализации, что позволяет органам предварительного расследования вычленить ту информацию, которая имеет доказательственное значение по уголовному делу. Сам отчет без изъятий также приобщается к уголовному делу.

Носитель виртуальных следов (сам аппарат или же карта памяти, SIM-карта и пр.) приобщается к материалам дела как вещественное доказательство на основании специального постановления субъекта расследования. Каждое приобщенное к делу вещественное доказательство должно отвечать требованиям о сохранности опечатки, наличии пояснительных бирок и подписей лиц, привлекавшихся к производству следственного действия. В обязанности субъекта расследования также входит обеспечение условий, исключающих доступ посторонних к носителям цифровых следов.

Посредством электронных данных, полученных из мобильного телефона, ноутбука, планшета и т.д., возможно:

а) напрямую изобличить лицо в совершении разглашения данных предварительного расследования в зависимости от способа разглашения; так, на электронном носителе может содержаться видео либо фото совершенного разглашения, SMS-сообщение о совершенном разглашении и т.д.;

б) косвенно указать на лицо, причастное к совершенному разглашению, например, путем извлечения медиафайлов, переписки, мета-данных, опровергающих алиби;

в) способствовать установлению иных значимых для уголовного дела о разглашении данных предварительного расследования фактических обстоятельств, имеющих доказательственное значение.

Литература

1. *Новикова М.А.* Определение понятия «разглашение данных предварительного расследования» // Библиотека уголовного права и криминологии. М.: Юрлитинформ, 2017. № 1 (16). С. 32–37.
2. *Новикова М.А.* Способы разглашения следственной тайны и сведений о мерах безопасности участников уголовного судопроизводства // Вестник Московского университета МВД России. М.: ЮНИТИ-ДАНА, 2008. № 2.
3. *Краснова Л.Б.* Компьютерные объекты в уголовном процессе и криминалистике: автореф. дис. ... канд. юрид. наук. Воронеж, 2005. С. 15–17.
4. *Поляков В.В.* Особенности расследования неправомерного удаленного доступа к компьютерной информации: автореф. дис. ... канд. юрид. наук. Омск, 2008. С. 13.
5. *Каминский М.К., Мочагин П.В.* Виртуально-информационный процесс отражения следообразований как новое направление в криминалистике // Вестник криминалистики. 2013. № 3. С. 52, 54.
6. *Васюков В.Ф., Булыжкин А.В.* Некоторые особенности осмотра средств сотовой связи при расследовании уголовных дел // Российский следователь. 2014. № 2. С. 2–4

Literatura

1. *Novikova M.A.* Opredelenie ponyatiya «razglashenie dannyx predvaritelnogo rassledovaniya» // Biblioteka ugolovnogo prava i kriminologii. M.: Yurlitinform, 2017. № 1 (16). S. 32–37.
2. *Novikova M.A.* Sposoby razglasheniya sledstvennoj tajny i svedenij o merax bezopasnosti uchastnikov ugolovnogo sudoproizvodstva // Vestnik Moskovskogo universiteta MVD Rossii. M.: YUNITI-DANA, 2008. № 2.

3. *Krasnova L.B.* Kompyuternye obekty v ugolovnom processe i kriminalistike: avtoref. dis. ... kand. yurid. nauk. Voronezh, 2005. S. 15–17.
4. *Polyakov V.V.* Osobennosti rassledovaniya nepravomernogo udalennogo dostupa k kompyuternoj informacii: avtoref. dis. ... kand. yurid. nauk. Omsk, 2008. S. 13.
5. *Kaminskij M.K., Mochagin P.V.* Virtualno-informacionnyj process otrazheniya sledoobrazovanij kak novoe napravlenie v kriminalistike // Vestnik kriminalistiki. 2013. № 3. S. 52, 54.
6. *Vasyukov V.F., Bulyzhkin A.V.* Nekotorye osobennosti osmotra sredstv sotovoj svyazi pri rassledovanii ugolovnyx del // Rossijskij sledovatel. 2014. № 2. S. 2–4

УДК 323.2

О.В. Мезинова

ПРИОРИТЕТЫ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ РФ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Рассматривается смена приоритетов государственной политики Российской Федерации, продиктованная условиями создания цифрового общества. В качестве доминирующих анализируются развитие научной инноватики, реформирование образования, здравоохранения и медицины, законодательства, обеспечение национальной безопасности, создание цифрового государства.

Ключевые слова: государственная политика, цифровизация, государственное управление национальная безопасность, цифровое государство.