Научная статья
УДК 343
https://doi.org/10.36511/2078-5356-2024-3-272-276

Необходимость установления цифрового следа при незаконном обороте лекарственных препаратов, содержащих наркотические средства, психотропные, сильнодействующие вещества

Вихарев Данил Дмитриевич
Нижегородская академия МВД России, Нижний Новгород, Россия, Dvikharev@mvd.ru, Danil19-92@inbox.ru

Аннотация. В данной статье рассматривается вопрос об использовании криминальным элементом сети «Интернет» и цифровых устройств в преступной деятельности. Подчеркнуто активное использование информационно-телекоммуникационных сетей и цифровых устройств при совершении преступлений в сфере незаконного оборота лекарственных препаратов, содержащих в составе наркотические средства, психотропные и сильнодействующие вещества. Дано понятие «цифровой след». Указано на его оставление при использовании лицом цифровых устройств и сети «Интернет». Рассмотрены основные преимущества, которые получает криминальный мир перед правоохранительной системой при активном использовании цифровизации при совершении преступлений. Указано на необходимость в обязательном обнаружении, фиксации и анализе цифровых следов в правоохранительной деятельности с целью идентификации личности предполагаемого преступника, установления причастности лица к совершению преступления. Приведены примеры возможностей правоохранительных органов при собирании цифрового следа для идентификации личности лица и установления причастности к преступлению. Подведен итог о необходимости активизации деятельности правоохранительных органов, связанной с обнаружением, фиксацией, закреплением и анализом цифрового следа в целях полного и всестороннего документирования преступных деяний и расследования уголовных дел в сфере незаконного оборота лекарственных препаратов, содержащих в составе наркотические средства, психотропные, сильнодействующие вещества.

Ключевые слова: лекарственные препараты, содержащие подконтрольные вещества, сеть «Интернет», цифровые устройства, цифровой след

Для цитирования: Вихарев Д. Д. Необходимость установления цифрового следа при незаконном обороте лекарственных препаратов, содержащих наркотические средства, психотропные, сильнодействующие вещества // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2024. № 3 (67). С. 272–276. https://doi.org/10.36511/2078-5356-2024-3-272-276.

Original article

The need to establish a digital trace in the illicit trafficking of medicines containing narcotic drugs, psychotropic and potent substances

Danil D. Vikharev
Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia, Nizhny Novgorod, Russian Federation, Dvikharev@mvd.ru, Danil19-92@inbox.ru

Abstract. This article examines the use of the criminal element of the Internet and digital devices in criminal activities. The active use of information and telecommunication networks and digital devices in the commission of crimes in the field of illicit trafficking in medicines containing narcotic drugs, psychotropic and potent substances is emphasized. The concept of a digital footprint is given and its abandonment is indicated when a person uses digital devices and the Internet. The main advantages that the criminal world receives over the law enforcement system, with the active use of digitalization in the commission of crimes, are considered. It is pointed out the need for mandatory detection, fixation and analysis of digital traces in law enforcement activities, in order to identify the identity of the alleged offender and in order to establish the involvement of a person in the commission of a crime. Examples of the capabilities of law enforcement agencies in collecting a digital footprint in order to identify a person and establish involvement in a crime are given. The article summarizes the need to intensify the activities of law enforcement agencies related to the detection, fixation, consolidation and analysis of the digital footprint in order to fully and comprehensively document criminal acts and investigate criminal cases in the field of illicit trafficking in medicines containing narcotic drugs, psychotropic, potent substances.

Keywords: medications containing controlled substances, the network is the "Internet", digital devices, digital footprint

For citation: Vikharev D. D. The need to establish a digital trace in the illicit trafficking of medicines containing narcotic drugs, psychotropic and potent substances. *Legal Science and Practice: Journal of Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia,* 2024, no. 3 (67), pp. 272–276. (In Russ.). https://doi.org/10.36511/2078-5356-2024-3-272-276.

Жизнь современного общества невозможно представить без использования цифровых устройств (мобильные телефоны, планшеты, персональные компьютеры и т. п.) и всемирной сети «Интернет». Созданная для блага общества цифровизация имеет двойственный характер и является одновременно инструментом преступной деятельности криминальной среды. Появление такого вида преступлений и условий их совершения, как с использованием цифровых технологий, Л. В. Бертовский и Б. Р. Сембекова справедливо относят к наступившей «технологической эволюции преступности». [1] Согласно официальной статистике за 2023 год, опубликованной на сайте Министерства внутренних дел Российской Федерации, каждое третье преступление совершено с использованием информационно-телекоммуникационных технологий [2], их профилактика по-прежнему остается одной из важнейших задач органов внутренних дел. При этом криминальный мир постоянно повышает уровень своей цифровой защиты, используя возможности для стирания, запутывания, сокрытия цифрового следа, который неизбежно остается при любом использовании цифровых устройств и сети «Интернет».

В криминалистической науке вопрос о возможности применения и самом понятии электронный или цифровой след возник еще со времени первых преступлений, совершенных с помощью электронно-вычислительных машин. Проанализировав мнения различных авторов, можно сделать вывод, что под цифровым, или электронным следом можно понимать любой уникальный набор действий на цифровых устройствах или в сети «Интернет». Грамотное обнаружение, фиксация и анализ (далее — собирание) цифровых следов точно так же как и аналогичная деятельность по уже привычным материальным и идеальным следам, являются неотъемлемой частью правоохранительной деятельности. В этом ключе нельзя не согласиться с мнением А. В. Ростовцева [3], который утверждает, что выявление, фиксация и экспертное исследование цифровых следов будут способствовать раскрытию и расследованию самых различных преступлений.

Современными цифровыми возможностями пользуются во всех криминальных сферах, в том числе и при незаконном обороте лекарственных препаратов, содержащих в своем составе наркотические средства, психотропные,

сильнодействующие вещества (далее — подконтрольные вещества). Способы совершения данного вида преступлений с использованием цифровых устройств и сети «Интернет» отличаются нестандартностью, сложностью, многообразием и частым обновлением. При этом реализация сложных сценариев совершения преступления может осуществляться как одним человеком, так и группой лиц, включающей в себя изготовителей, оптовиков-перевозчиков, оптовых и мелких закладчиков, расположенных в разных субъектах страны и не знающих лично друг друга. Массовость, простота и доступность цифровых устройств, возможность доступа к сети «Интернет» из любой точки мира дали такие преимущества лицам, совершающим преступления с подконтрольными веществами, как анонимность и скорость взаимодействия. Следовательно, на наш взгляд, понятие цифрового следа в отношении преступлений в сфере незаконного оборота лекарственных препаратов, содержащих в своем составе подконтрольные вещества, можно выделить как категорию следов, включающих в себя набор действий на цифровых устройствах или в сети «Интернет», позволяющих зафиксировать связь между организатором преступления, исполнителями (лица, непосредственно незаконно сбывающие вещества) и потребителями (лица их приобретающие).

Самым распространенным способом сбыта лекарственных препаратов, содержащих подконтрольные вещества, является их бесконтактный сбыт, совершенный с использованием цифровых устройств и информационно-телекоммуникационной сети «Интернет», который происходит анонимно, без физического контакта продавца и покупателя.

Кроме анонимности, распространению применения цифровых технологий при совершении преступлений в сфере незаконного оборота подконтрольных веществ способствует ряд иных факторов:

— возможность использовать достаточно защищенные каналы связи, которые весьма трудно, а иной раз практически невозможно идентифицировать и расшифровать. К примеру, мессенджеры: *Signal, Telegram, ViPole* и другие [4, с. 30], где обычно при регистрации не нужно указывать абонентский номер устройства, а достаточно придумать только ник своей учетной записи;

— использование сложных для идентификации способов оплаты услуг и получения преступного дохода исполнителем-закладчиком, при которых используются системы денежных переводов, которые не предполагают открытия банковского счета, вследствие этого могут быть использованы удаленно, анонимно или путем регистрации на третьих лиц. К примеру, активно используются биржи по обмену криптовалют (*WEX.com, EXMO.com* и др.), где основными средствами платежа, как правило, выступают *Bitcoin* и *Ethereum* [5];

— применение преступными группами фотохостингов, таких как *Imgur, Radikal, Postimg,* для хранения и передачи фотоизображений с местами тайников-закладок с подконтрольными веществами в целях исключения прямой связи между устройствами при обмене данной информацией;

— использование различных картографических сервисов *Google maps* для передачи покупателям точных координат мест нахождения тайников, а также программ, автоматически проставляющих на фотографии точные координаты и удаляющих личные данные со снимка (вид устройства, время съемки и т. п.), к примеру *NoteCam*;

— использование программного обеспечения *VPN*, шифрующего соединение, позволяющее обходить блокировку со стороны государственных органов с невозможностью дальнейшего определения *IP*-адресов, выхода на интернет-ресурсы и системы шифрования места нахождения пользователя.

Таким образом, при незаконном обороте подконтрольных веществ широко применяются возможности цифровых устройств и самой сети «Интернет». При этом при их использовании на самом устройстве и (или) в сети «Интернет» все же остается след от производимого действия, получив и проанализировав который, можно установить само производимое действие, а также идентифицировать лицо, его осуществившее. В связи с этим для правоохранительной системы возникает необходимость в обязательном собирании цифровых следов как в целях идентификации личности предполагаемого преступника, так и в установлении причастности лица к преступлению.

Непосредственная деятельность по фиксации цифрового следа может быть осуществлена как самим субъектом, то есть сотрудником оперативного или следственного подразделения, так и по его запросу, поручению, назначению экспертизы или проведения совместного осмотра иным лицом, обладающим специальными знаниями (сотрудниками экспертно-криминалистического центра, бюро специальных технических мероприятий, сторонних организаций (сотовых, транспортных, интернет-компаний,

Росфинмониторинга и т. п.). К примеру, экспертно-криминалистические центры МВД России, используя специальные познания и различные специальные методы и техники, позволяющие найти, структурировать и сформировать интересующую информацию, находящуюся на электронном устройстве, применяя специальное программное обеспечение с возможностями контент-анализа (*UFED, XRY, U2*, мобильный криминалист, *OSForensics*) [6], могут получить дополнительные доказательства, которые невозможно получить простым осмотром цифрового устройства. При этом могут быть установлены файлы-*cookies*, сохраненные страницы с посещением сайтов, удаленные фотоизображения, удаленные поисковые запросы в интернет-поисковиках и т. п.

Процесс идентификации личности в основном связан с установлением его паспортных данных, к которым относятся фамилия, имя, отчество, год рождения, место рождения, место жительства и иные данные, которые необходимы для однозначного установления человека. Рассмотрим некоторые из возможных способов идентификации личности посредством цифровых следов:

— анализ социальных сетей по имеющимся данным. Так, используя возможности социальных сетей «Вконтакте» и «Одноклассники», можно найти дополнительные данные о личности подозреваемого лица, указанные им при регистрации в социальной сети;

— анализ данных из служб доставки («Деливери», «ЯндексДоставка»), служб такси (Яндекс*Go*) или аренды автомобиля позволяют установить место жительства, образ жизни, время и способы перемещения, а также иную значимую информацию;

— анализ личных цифровых данных (электронный почтовый ящик, абонентский номер, домашний интернет, электронные банковские счета и т. п.), где при регистрации лицо обычно указывает свои личные установочные данные. Например, при наличии установленного абонентского номера можно установить фамилию и инициалы при использовании приложения «СбербанкОнлайн», а при дальнейшем направлении запросов и судебных решений получить паспортные данные, указанные при регистрации абонентского номера, установить *imei* номера устройства и получить биллинг за интересующий период времени.

При установлении причастности лица к преступным деяниям посредством собирания цифровых следов, то есть документального подтверждения того, что лицо использовало цифровое устройство и (или) сеть «Интернет» для совершения преступления применяется также довольно большой спектр различных способов. Рассмотрим некоторые из них:

— установление *IP*-адреса, с которого были загружены или просмотрены фотоизображения с местами тайников-закладок с подконтрольными веществами;

— установление посредством биллинга местонахождения конкретного устройства в конкретный момент времени;

— установление метаданных по имеющимся файлам;

— установление финансовых транзакций, связанных с преступной деятельностью лиц (вывод денежных средств, оплата заработной платы закладчикам, совершение иных покупок и т. п.);

• установление индивидуальных данных лиц (ники в мессенджерах, ники в преступных интернет-магазинах и т. п.);

— при непосредственном осмотре технических цифровых устройств у задержанного лица в обязательном порядке с целью обнаружений цифрового следа, подтверждающего причастность к преступлению, устанавливаются ники в интересующих программах и мессенджерах, фотоизображения с получением метаданных, *IP*-адрес устройства, факты выходов в сеть «Интернет» и т. п. [7].

Обычно идентификация личности подозреваемого лица и установление его причастности к преступлению представляют собой единый процесс. Сначала по имеющимся данным устанавливается личность лица, а позже проверяется его причастность к преступной деятельности или же устанавливается причастность неустановленного лица к преступлению, а в последующем проводятся мероприятия, направленные на его идентификацию.

В большинстве своем направления собирания доказательственной базы связаны с бесконтактным способом идентификации лица и установлением его причастности к преступлению, то есть до его непосредственного задержания. При этом в обязательном порядке уже после задержания лица необходимо также собрать цифровой след при осмотре принадлежащих ему технических средств. К примеру, в сотовом телефоне зачастую указан адрес электронной почты, другие используемые абонентские номера, посещенные интернет-ресурсы в браузере. Могут находиться фотографии самого лица, его личные документы и иная информация, которую можно использовать в качестве идентификации

Legal Science and Practice: Journal of Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia, 2024, no. 3 (67)

человека и подтверждения причастности к совершению преступления. В данной связи нельзя не согласиться с венгерской исследовательницей Каталин Фехер [8], которая, размышляя в своей статье на тему цифровых следов, оставленных людьми, писала, что человек в сети «Интернет» оставляет их. При этом он может о них и не помнить, но цифровые устройства сохраняют в памяти очень многие из его действий.

В настоящее время информационно-телекоммуникационные технологии интенсивно развиваются. Создается новое программное обеспечение, улучшающее способы шифрования, скорости взаимодействия и анонимности пользователей при использовании цифровых устройств и сети «Интернет». Одновременно растет и количество преступлений, совершенных с их использованием, в том числе в области незаконного оборота лекарственных средств, содержащих в своем составе наркотические средства, психотропные, сильнодействующие вещества. В связи с этим деятельность правоохранительной системы в обязательном порядке должна подстраиваться к цифровизации мира; оснащаться более современным оборудованием, позволяющим отследить цифровой след и «распутать его»; совершенствовать способы и средства его обнаружения, фиксации и анализа; дополнить методики и рекомендации по выявлению, раскрытию и расследованию преступлений, совершенных с использованием цифровых устройств и сети «Интернет», и, соответственно, подготавливать кадры, имеющие должный уровень компетенции, необходимый для сбора и анализа цифрового следа.

Активизация деятельности в данном направлении крайне важна, так как для всестороннего документирования преступной деятельности и расследования уголовного дела на должном уровне оперативным и следственным подразделениям необходимо самостоятельно иметь представление о возможных источниках получения цифрового следа, законном, грамотном его получении и закреплении, а также активно использовать силы и средства специальных подразделений системы МВД России и иных организаций, специализирующихся на определении и сборе цифрового следа.

Список источников

1. Бертовский Л. В., Сембекова Б. Р. Высокотехнологичные преступления как угроза национальной безопасности // Новеллы материального и процессуального права: материалы Всероссийской (нац.) научно-практической конференции (май – октябрь 2020 г., г. Красноярск). Красноярск: Красноярский государственный аграрный университет, 2020. С. 127–130.

2. Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2023 года. URL: https://мвд.рф/reports/item/47055751/ (дата обращения 25.04.2024).

3. Ростовцев А. В. Особенности судебно-экспертного исследования «Цифровых следов» // Академическая мысль. 2019. № 3 (8).

4. Меняйло Д. В., Малыхина Е. А. Цифровые следы в сфере незаконного оборота наркотических средств // Проблемы правоохранительной деятельности. 2022. № 4. С. 29–32

5. Земцова С. И. Бесконтактный сбыт наркотических средств с использованием интернет-магазинов: актуальные вопросы // Наркоконтроль. 2019. № 3. С. 17–22.

6. Сборник статей о деятельности криминалистических подразделений следственных органов Следственного комитета Российской Федерации / Следственный комитет Российской Федерации. Москва: 2018. 240 с.

7. Большая Российская Энциклопедия. URL: https://bigenc.ru/c/metadannye-0b2c68 (дата обращения 12.12.2023).

8. Fehér K. Digital identity and the online self: Footprint strategies – An exploratory and comparative research study // Journal of Information Science, 2019.

References

1. Bertovsky L. V., Sembekova B. R. High-tech crimes as a threat to national security // Novels of substantive and procedural law: materials of the All-Russian. (national) scientific and practical conference (May-October 2020, Krasnoyarsk). Krasnoyarsk: Krasnoyar. state Agrarian University. Univ., 2020. pp. 127–130. (In Russ.)

2. Brief description of the state of crime in the Russian Federation in January – December 2023. URL: https://мвд.рф/reports/item/47055751 / (accessed 25.04.2024). (In Russ.)

3. Rostovtsev A. V. Features of forensic research of "Digital traces". *Academic thought*, 2019, no. 3 (8). (In Russ.)

4. Menyailo D. V., Malykhina E. A. Digital traces in the field of illicit drug trafficking. *Problems of law enforcement*, 2022, no. 4, pp. 29–32. (In Russ.)

5. Zemtsova S. I. Contactless sale of narcotic drugs using online stores: topical issues. *Drug control*, 2019, no. 3, pp. 17–22. (In Russ.)

6. Collection of articles on the activities of forensic units of investigative bodies of the Investigative Committee of the Russian Federation. Investigative Committee of the Russian Federation. Moscow: 2018. 240 p. (In Russ.)

7. The Great Russian Encyclopedia. URL: https://bigenc.ru/c/metadannye-0b2c68 (accessed 12.12.2023). (In Russ.)

8. Scheer K. Research Identity and Online Identity: a Tracking strategy — Research and Comparative Research. *Journal of Informatics*, 2019. (In Russ.)