УДК 343.985.2

ИСПОЛЬЗОВАНИЕ СЕТИ ИНТЕРНЕТ ПРИ УСТАНОВЛЕНИИ ЛИЦА, СОВЕРШИВШЕГО ПРЕСТУПЛЕНИЕ

Кулаевский Андрей Витальевич

Алтайский государственный университет, г. Барнаул
e-mail: andrei8888.98@mail.ru

USING THE INTERNET TO IDENTIFY THE PERSON WHO COMMITTED THE CRIME

Kulaevsky Andrey V.

Altai State University, Barnaul

Аннотация. В работе анализируются цифровые следы, оставленные лицом, совершившим преступление в сети Интернет, определяются цифровые следы, необходимые для установления лица, совершившего преступление, исследуются современные возможности фиксации цифровых следов в сети Интернет. В статье приводятся различные классификации цифровых следов, определяются их виды. Исследуются свойства личности преступника. В завершении указывается рациональный путь получения персональных данных лица, совершившего преступление.

Ключевые слова: цифровая криминалистика, цифровой след, установление преступника, персональные данные, цифровая тень.

Abstract. The paper analyzes the digital footprints left by a person who committed a crime on the Internet, determines the digital footprints necessary to identify the person who committed the crime, and explores the modern possibilities of fixing digital footprints on the Internet. The article presents various classifications of digital traces and defines their types. The properties of the criminal's personality are being investigated. At the end, a rational way to obtain the personal data of the person who committed the crime is indicated.

Keywords: digital forensics, digital footprint, identification of the perpetrator, personal data, digital shadow.

Для цитирования: Кулаевский А.В. Использование сети Интернет при установлении лица, совершившего преступление // Проблемы правовой и технической защиты информации. 2023. №11. С. 83-86.

For citation: Kulaevsky A.V. Using the Internet to identify the person who committed the crime // Legal and Technical Problems Information Protection. 2023. No. 11. P. 83-86.

Современные способы совершения преступления усложняют процесс расследования преступлений. Выявление, постановка и решение проблем расследования преступлений являются необходимыми действиями для улучшения качества процесса расследования. Преступники, совершая преступления с использованием компьютерных средств, оставляют цифровые следы. Использование криминалистически значимой информации в виде цифрового следа является одним из главных путей, ведущих к лицу, совершившему преступление.

Правильное использование цифрового следа залог качественного расследования преступлений, совершенных с использованием сети Интернет. Данные, оставленные преступниками в сети Интернет зачастую являются единственным источником криминалистически значимой информации позволяющей установить лицо,

совершившие преступление. В рамках настоящей статьи будет предпринята попытка исследовать цифровой след лица, совершившего преступление, в качестве основного элемента, его установления.

Цифровые следы остаются и при совершении преступником дистанционного мошенничества. В таком виде мошенничества, средством информационного обеспечения преступной деятельности являются компьютерные устройства и технологии сотовой связи.

Цифровые следы не относятся к традиционной криминалистической классификации следов на материальные и идеальные. В криминалистической науке такие следы обознаются как цифровые, электронно-цифровые, виртуальные. Не вступая в дискуссию относительно определения рассматриваемых следов приведем определения «цифрового следа».

В.Б. Вехов предлагает ввести в криминалистический категориальный аппарат понятие «электронно-цифровой след», под которым понимает «любую криминалистически значимую компьютерную информацию, т.е. сведения (сообщения, данные), находящиеся в электронно-цифровой форме, зафиксированные на материальном носителе с помощью электромагнитных взаимодействий либо передающиеся по каналам связи посредством электромагнитных сигналов» [5].

Е.Р. Россинской и И.А. Рядовский определяют «цифровой след» как криминалистически значимую компьютерную информацию о событиях или действиях, отраженную в материальной среде, в процессе ее возникновения, обработки, хранения и передачи» [9].

В.А. Мещеряков под «виртуальными» следами понимает любые изменения состояния автоматизированной информационной системы (образованного ею «кибернетического пространства»), связанные с событием преступления и зафиксированные в виде компьютерной информации (т.е. информации в виде, пригодном для машинной обработки) на материальном носителе, в т.ч. на электронно-магнитном поле» [6].

В криминалистической литературе представлены две распространённые классификации цифрового следа. В зависимости от физического носителя цифрового следа [3], а также в зависимости от механизма следообразования [4].

В рамках настоящего исследования необходимо выделить цифровые следы, указывающие на лицо, совершившее преступление. При исследовании таких следов необходимо учитывать выделенные криминалистической наукой биологические, социальные и психологические свойства личности преступника.

В первую очередь необходимо обращать внимание на социальные свойства личности преступника. К социальным свойствам можно отнести персональные данные лица, совершившего преступление. Такой тезис объясняется тем, что персональные данные в соответствии с п.1 ст. 3 Федерального закона №152-ФЗ «О персональных данных» – это любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)[1]. Такая информация может содержать личные данные: ФИО, место регистрации, информация об образовании, о месте работы, номер телефона, e-mail.

С.В. Милюков определил социальные свойства как совокупность сфер: общегражданской, национальной, семейной, бытовой и производственной [7].

Таким образом, персональные данные по своему содержанию имеют социальную информацию о преступнике и могут быть определены как социальные. Вследствие указанного, данные лица, совершившего

[1] О персональных данных : Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 30.12.2020) (с изм. и доп., вступ. в силу с 01.03.2021). – Текст : электронный // Официальный интернет-портал правовой информации. – URL : http://www.pravo.gov.ru/ (дата обращения: 19.05.2021). Режим доступа: свободный.

преступление, могут именоваться персональными данными.

Для скорейшего установления лица, совершившего преступление, необходимо исследовать цифровые следы, содержащие идентифицирующую информацию о пользователях средства, с помощью которого было совершено преступление. Такая информация, как правило, выражается в виде персональных данных – ФИО, номера телефона, почты и др. При подключении пользователя к сети Интернет ему присваивается уникальный идентификатор – IP-адрес, позволяющий определить персональные данные лица, использующего IP-адрес.

Из изложенного выше следует, что наиболее рациональным путем установления лица, совершившего преступление, является получение его персональных данных.

Персональные данные лица, совершившего преступление, остаются на устройствах – средствах совершения преступления. Именно устройство, как отмечает М.С. Бисалиев может «указать» на лицо, совершившее противоправные действия, а характер совершенных им действий – свидетельствовать о наиболее важных признаках способа совершения посягательства в процессе криминалистического установления киберпреступления [2].

В.В. Поляков смоделировал 4 группы различных ситуаций, возникающих в процессе расследования компьютерных преступлений [8]. В рамках настоящего научного исследования заслуживает внимания первая группа ситуаций, имеющая варианты: 1. «личные устройства связи принадлежат пользователям на праве собственности и, как правило, содержат следы владельца устройства (характерные идентификационные признаки личности)»; 2. «публичные устройства связи позволяют ими воспользоваться на праве пользования при конкретных условиях и обстоятельствах, обычно они содержат следы общения разных личностей (наличие идентификационных признаков, принадлежащих разным лицам в конкретные периоды времени)».

При возникновении такой ситуации лицо, совершившее преступление, формируется как цифровая личность, оставляя цифровые следы.

В науке есть позиция о квалификации цифрового следа на активный и пассивный. Активный цифровой след пользователь сети Интернет оставляет осознано, регистрируясь в социальных сетях, совершая покупки в интернет-магазине [1]. Пассивный цифровой след оставляется пользователем непреднамеренно. Из пассивных цифровых следов, с помощью созданных коммерческими компаниями алгоритмами создается «цифровая личность» со своими интересами и предпочтениями, местоположением пользователя. Нередко в научных публикациях можно встретить синонимичный пассивному цифровому следу термин – цифровая тень. В любом случае алгоритмы обработки информации настроены для получения максимальной информации о пользователе, даже если он не самостоятельно вводил свои данные. Сервисы Google Maps, Yandex Maps, 2GIS и др. обрабатывая IP-адрес получают данные о местоположении пользователя. Получение такой информации существенно влияет на результативность действий следователя по установлению лица, совершившего преступление.

Перечислим основные виды цифровых следов, содержащихся в сети Интернет, и имеющих персональные данные лица, совершившего преступление: 1) данные пользователя интернет-ресурса; 2) данные пользователя, оставленные в средстве совершения преступления при его использовании; 3) данные социальных сетей и мессенджеров.

Все перечисленные цифровые следы остаются в сети Интернет посредством работы информационно-технологических идентификаторов, фиксирующих персональные данные лица, совершившего преступление, в учетной записи (аккаунте пользователя).

Таким образом, при установлении лица, совершившего преступление, органам

дознания и предварительного расследования необходимо определить учетные данные пользователя сети Интернет — физического лица. Такие действия целесообразно проводить в следующей последовательности: 1. определить идентификатор (IP-адрес) преступника; 2. определить наличие учетных записей, зарегистрированных с найденного IP-адреса; 3. Получить персональные данные, содержащиеся в учетных записях.

В завершении отметим, полученная в ходе расследования преступления информация о цифровом следе преступника, может является основным источником получения информации о лице, совершившем преступление. Такой тезис подтверждается содержанием информации неумышленно оставленная преступником в сети Интернет.

Библиографический список

1. *Бояркина Л.А., Бояркин В.В. Цифровой след и цифровая тень как производные персональных данных //Сборники конференций ниц социосфера. – Vedecko vydavatelske centrum Sociosfera-CZ sro, 2016. – №. 62. – С. 78-81.*
2. *Бисалиев М.С., Шакиров К.Н. Цифровые следы как фактор безопасности оборота персональных данных в сети Интернет //Вестник Евразийского национального университета имени ЛН Гумилева. Серия: Право. – 2023. – Т. 142. – №. 1. – С. 81-98.*
3. *Бычков В.В. Соблюдение прав граждан на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений при проверке сообщений о преступлениях и в ходе их расследования // Российский следователь. 2013. N 24. С. 12*
4. *Бычков В.В., Вехов В.Б. Специальные знания, обеспечивающие расследование преступлений, связанных с оборотом криптовалюты // Российский следователь. 2018. N 2. С. 8-11.*
5. *Вехов В.Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки: монография. Волгоград: ВА МВД России, 2008. С. 84.*
6. *Мещеряков В.А. Основы методики расследования преступлений в сфере компьютерной информации: дис. ... д-ра юрид. наук. Воронеж, 2001. С. 104.*
7. *Милюков С.В. Современные возможности использования свойств человека при установлении личности в раскрытии и расследовании преступлений: монография. - Москва: Юрлитинформ, 2013. – 188 с.*
8. *Поляков, В.В. Следственные ситуации начального этапа расследования компьютерных преступлений, совершаемых удаленным образом // Проблемы правовой и технической защиты информации. – 2018. – № 6. – С. 113-119. – EDN RTLHJB.*
9. *Россинская Е.Р., Рядовский И.А. Концепция цифровых следов в криминалистике // Аубакировские чтения: материалы международной научно-практической конференции (19 февраля 2019 г.). Алматы: Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының, 2019. С. 7.*