

Научная статья
УДК 343.98

ТАКТИКА ИСПОЛЬЗОВАНИЯ ДАННЫХ BIG DATA (ЦИФРОВЫХ ПРОФИЛЕЙ) В ДОКАЗЫВАНИИ ПРИ ОТСУТСТВИИ УСТАНОВЛЕННОГО СУБЪЕКТА ПРЕСТУПЛЕНИЯ

Софья Денисовна ПОРТНЫХ

Юридический институт
ФГАОУ ВО «Южно-Уральский государственный университет
(Национальный исследовательский университет)»
port.sofiy78@gmail.com

Научный руководитель: доцент кафедры уголовного процесса, криминалистики и судебной экспертизы Юридического института ФГАОУ ВО «Южно-Уральский государственный университет (Национальный исследовательский университет)», кандидат юридических наук, доцент
Елена Анатольевна БУГЛАЕВА, buglaevaea@susu.ru

Аннотация. Статья посвящена вопросу использования деперсонализированных цифровых профилей в качестве доказательства по уголовному делу. Автор акцентирует внимание на необходимости фиксации паттернов аномального поведения в сети с целью установления цифрового профиля, при этом отделяя его от личности субъекта преступления.

Ключевые слова: деперсонализированный цифровой профиль, аномальный паттерн поведения, транзакции.
Юридический институт

TACTICS FOR USING BIG DATA (DIGITAL PROFILES) IN PROVING A CRIME IN THE ABSENCE OF AN IDENTIFIED SUBJECT OF THE CRIME

Sofya D. PORTNYKH

Law Institute
South Ural State University (National Research University)
port.sofiy78@gmail.com

Scientific adviser. Associate Professor at the Department of Criminal Procedure, Criminalistics and Forensic Expertise, Law Institute, South Ural State University (National Research University), Candidate of Legal Sciences, Associate Professor, **Elena Anatolyevna BUGLAEVA**, buglaevaea@susu.ru

Abstract. The article is devoted to the issue of using depersonalized digital profiles as evidence in a criminal case. The author focuses on the need to record patterns of abnormal behavior online in order to establish a digital profile, while separating it from the identity of the subject of the crime.

Keywords: depersonalized digital profile, abnormal behavior pattern, transactions.

Scientific adviser — Professor at the Department of theory and history of state and law of St. Petersburg Law Institute (branch) of the University of the Prosecutor's Office of the Russian Federation, Doctor of Science (Law), Full Professor, **I. B. Lomakina**, lomakina7311@gmail.com

Abstract. The article is devoted to one of the classical types of legal understanding – the sociology of law. The author focuses on the historical and legal aspect of the sociological school, analyzes the main provisions. The current state is also touched upon, the relevance and importance, positive and negative sides are noted.

Keywords: law, type of legal understanding, sociological type of legal understanding, sociology of law, sociological concept

В современных условиях преступность, особенно – в сфере экономики, незаконного оборота наркотических средств, психотропных веществ и их прекурсоров, оружия, взрывных устройств и взрывчатых веществ, чаще стала носить децентрализованный характер. В связи с этим классическая для России оперативно-розыскная деятельность¹, направленная на установление личности субъекта преступления, сталкивается с серьёзными препятствиями в виде приватности даркнета, использования криптовалют, VPN-маршрутизаторов и синтетических личностей.

Преступник как физическое лицо может не проявляться до момента совершения транзакции, но его криминальная активность неизбежно оставит массивный цифровой след. В подобных случаях решением может стать переход от субъект-ориентированного подхода к объект-ориентированному: правоохранительным органам следует устанавливать не

¹ Агапов, П. В. Основы теории оперативно-розыскной деятельности органов внутренних дел : учебник – 133 с.

конкретного человека, а аномальный паттерн поведения и при помощи различных специализированных программных обеспечений фиксировать его². В таких случаях деперсонализированные данные (например, Digital Twins, цифровые профили) являются самостоятельным объектом оперативной заинтересованности и, потенциально, становятся доказательством по уголовному делу.

В оперативно-розыскной деятельности под деперсонализированным цифровым профилем следует понимать агрегированный набор индикаторов, который создаётся для описания поведения неустановленного узла сети, но при этом без привязки к паспортным данным владельца. В число таких индикаторов можно включить: геометрические и временные метаданные (обозначают паттерны перемещений некоторой группы абонентов), цифровой отпечаток устройства (device fingerprinting), граф социальных связей (показывает топологию взаимодействия в мессенджерах) и финансовый граф (отражает цепочки транзакций).

Основной тактической проблемой использования деперсонализированных данных является то, что в ст. 7 Федерального закона от 12.08.1995 №144-ФЗ «Об оперативно-розыскной деятельности» закреплён исчерпывающий перечень оснований для проведения оперативно-розыскных мероприятий, одним из основных пунктов которого является наличие сведений о подготавливаемом, совершаемом или совершённом противоправном деянии – несмотря на это, результат анализа сетей и фиксацию аномального паттерна поведения нельзя считать юридическим фактом из-за того, что алгоритм выдаёт лишь вероятность девиации. В таком случае основной задачей сотрудника оперативного подразделения того или иного правоохранительного органа заключается в переводе математической корреляции на «язык» уголовного процесса.

² Зуев, С. В. Уголовное судопроизводство в цифровую эпоху: доктрина и практика – 46 с.

Стоит отметить, что зарубежные правоохранительные органы столкнулись с проблемой использования деперсонализированных данных несколько раньше российских³, и наиболее показательной является практика Верховного суда США по делу Карпентера (V. Carpenter) (2018) и Суда Европейского Союза по делу «La Quadrature du Net» (2020). Рассмотрим подробнее оба дела.

По делу Карпентера суд рассматривал вопрос о законности получения сотрудниками полиции данных о местоположении мобильного телефона подозреваемого (CSLI) от провайдера без соответствующего ордера. Правительство США, представлявшее сторону обвинения, ссылалось на так называемую доктрину «третьей стороны» («Third-party doctrine»): передавая любые данные оператору связи, гражданин должен терять ожидание приватности. Однако суд не принял данные доводы и встал на сторону защиты, сославшись на то, что сотрудники полиции незаконным путём получили данные о геолокации мобильного устройства за 127 дней, что позволило составить детальный план его передвижения. По отдельности каждая точка такого плана незначима для дела, однако их совокупность даёт доступ к данным лица, ранее доступным только ему.

В приведённом примере следует обратить внимание на то, что при формировании цифрового профиля отсутствие установленного субъекта снимает вопрос нарушения права конкретного лица на тайну частной жизни, но лишь в том случае, когда полученный массив информации не позволяет установить привычки, состояние здоровья, религиозные убеждения и т.п. черты гипотетически анонимного пользователя – что требует контроля суда за процессом получения и обработки таких данных.

³ Багмет, А. М. Цифровая криминалистика: проблемы собирания и исследования электронных доказательств – 112 с.

В ходе рассмотрения дела «La Quadrature du Net and Others», C-470/21, Поводом стал спор вокруг французского механизма борьбы с нарушением авторских прав в интернете. Во Франции действовала независимая организация Hadopi. Когда правообладатели жаловались на пользователя, Hadopi по национальному законодательству (законы 2010 и 2017 годов) могла запросить у провайдеров данные: IP-адрес и информацию, позволяющую установить личность человека. Правозащитная организация La Quadrature du Net совместно с другими подала иск. Представители утверждали, что такое общее и неизбирательное хранение данных (когда провайдер вынужден хранить информацию обо всех пользователях, а власти потом по запросу получают доступ к личности) непропорционально нарушает фундаментальные права (право на неприкосновенность частной жизни, защиту данных, свободу выражения мнений). Суд ЕС рассматривал этот вопрос в два этапа.

В первом решении от 6 октября 2020 года суд подтвердил: национальное законодательство, которое обязывает поставщиков электронных услуг связи к общему и неизбирательному хранению данных о трафике и местоположении пользователей в целях борьбы с преступностью в целом или для защиты национальной безопасности, противоречит праву нормам права Европейского Союза. Во втором решении от 30 апреля 2024 суд уточнил подход. Он допустил целевое и ограниченное по времени хранение IP-адресов — например, для расследования особо тяжких онлайн-преступлений (таких как торговля людьми, жестокое обращение с детьми). При этом Суд провёл разграничение и зафиксировал, что хранение самих IP-адресов (которые лишь идентифицируют устройство, а не раскрывают содержание переписки) допустимо в более широком формате, чем хранение данных о трафике и местоположении (которые дают гораздо более глубокую картину частной жизни). Также суд подчеркнул, что любое подобное вмешательство должно сопровождаться эффективными

гарантиями и проходить под контролем судов или какого-либо независимого административного органа.

Таким образом, можно заметить, что СЕС признаёт формирование каких—либо универсальных баз данных, содержащих в себе цифровые профили, незаконным, а доказательственное значение для дела может иметь только профиль, который был сформирован ретроспективно по конкретному событию (например, профиль создан и зафиксирован в месте обнаружения лаборатории по изготовлению наркотических средств).

Стоит отметить, что в российских судебных решениях термин «цифровой профиль» не используется, заменяясь чаще всего на «совокупность доказательств» или «совокупность цифровых данных». Правоохранительные органы РФ столкнулись с проблемой использования деперсонализированных данных на несколько лет позже, но, несмотря на это, вектор для наделения их доказательственным значением всё же был задан Судебной коллегией по уголовным делам Верховного Суда РФ.

Так, в 2019 году ВС РФ вынес Определение №5-АПУ19-66 по делу о незаконном сбыте наркотических средств бесконтактным способом с применением криптовалюты. Тогда органам следствия не удалось установить личность владельца интернет-магазина по продаже наркотических средств в теневом сегменте интернета, в связи с чем обвинение строилось на юридически подтверждённом факте изъятия вещества и анализе переписки с заказчиком. Верховный Суд оставил приговор суда первой инстанции и при этом подчеркнул важность анализа движения денежных средств по криптокошелькам и IP-адресов используемых серверов. По данному делу в качестве цифрового профиля использовалась связка: «IP-адрес сервера – кошелек А – кошелек В – QIWI-терминал». Субъект преступления (владелец кошелька В) не установлен, но судом была признана устойчивой цепочка, созданная для передачи оплаты.

Такое решение суда показывает, что первые шаги к легализации цифрового профиля в качестве доказательства по уголовному делу были сделаны.

В 2023 году были внесены изменения в Постановление Пленума Верховного Суда РФ от 30 ноября 2017 года № 48, в которых указывается, что местом совершения киберпреступления является не только место нахождения виновного лица, но и место наступления общественного опасных последствий. Для формирования цифрового профиля потерпевшего (с целью выявления мошенников-фродстеров) правоохранительные органы принимают во внимание логи авторизации, ID рекламных кабинетов и технические заголовки писем. Отсутствие возможности установления личности отправителя не делает эти данные недопустимыми для использования в производстве по делу, так как они не противоречат нормам действующего уголовно-процессуального законодательства и позволяют установить группу тождественных эпизодов противоправных действий.

Чтобы деперсонализированные данные стало можно считать основанием для возбуждения уголовного дела (ст. 140 УПК РФ) при неустановленном субъекте, на наш взгляд, можно действовать по предложенному нами алгоритму, состоящему из пяти этапов. Рассмотрим каждый подробнее.

Первым этапом проводится триггирование. Производится выявление статистической аномалии при помощи автоматизированных систем (например, отслеживание всплеска транзакций через один и тот же POS-терминал в ночное время или синхронное перемещение 15-20 мобильных устройств по промышленной зоне).

Затем следует сформировать легендированный объект. Вместо внесения в материалы дела оперативного учёта записи: «анализ профиля неустановленного пользователя», - нужно провести проверку юридического

лица или мониторинг конкретно определённой территории. Подобным образом можно легализовать сбор первичных данных.

Проводим агрегацию, но без идентификации – для этого возможно использовать методы технического обезличивания, такие, как k-анонимизация. Приведём примеры: сотрудник оперативного подразделения фиксирует не MAC-адрес, а хэш-сумму; не номер телефона, а внутренний ID аналитической системы.

После этого осуществляется создание искусственной точки контакта. С целью превращения некоего абстрактного профиля в установленный субъект производится следующая тактическая комбинация: на выявленный узел графа (например, аккаунт-дроповод) направляется контролируемая передача (например, закладка или перевод криптовалюты). В момент принятия этого контакта анонимным пользователем происходит его физическая или техническая идентификация.

Заключительным этапом будет легализация полученной информации через заключение специалиста (ст. 58 УПК РФ). Согласно действующему законодательству, результаты работы нейросети или аналитического ПО, работающего с Big Data, могут быть закреплены в материалах дела исключительно через заключение специалиста. При этом в заключении специалиста должна быть подтверждена методология получения этих данных и содержаться объяснение, почему полученный набор метрик относится именно к искомой преступной группе, а не является ошибкой системы или случайным совпадением.

Использование деперсонализированных данных меняет философию доказывания, мы уходим от того времени, когда факты, которые невозможно связать с конкретным субъектом, исключаются из уголовного дела, и переходим к тому, когда обнаруженный вредоносный паттерн становится основанием для проведения расследования.

Для сотрудников оперативных подразделений это значит, что возникает необходимость овладения навыками криминологического программирования и понимания границ допустимости его применения, также навыками работы со специализированными программными обеспечениями.

Проведённый анализ судебной практики показал, что доказательственное значение имеет не «сырые» сведения из базы данных мобильного оператора, а верифицированный цифровой профиль, локализованный по времени, привязанный к конкретному эпизоду и подтверждённый процессуальным способом – осмотром, экспертизой и последующим установлением лица.

Список источников

1. Агапов, П. В. Основы теории оперативно-розыскной деятельности органов внутренних дел : учебник / П. В. Агапов, Д. В. Вагин. — Москва : Проспект, 2023. — 488 с.

2. Багмет, А. М. Цифровая криминалистика: проблемы собирания и исследования электронных доказательств / А. М. Багмет, В. В. Польшаный. — Москва : Юрлитинформ, 2024. — 296 с.

3. Гаврилов, Б. Я. Искусственный интеллект в правоохранительной деятельности: мифы и реальность правового регулирования / Б. Я. Гаврилов, А. Н. Ильяшенко // Труды Академии управления МВД России. — 2024. — № 3 (69). — С. 12–21.

4. Зуев, С. В. Уголовное судопроизводство в цифровую эпоху: доктрина и практика / С. В. Зуев // Lex russica. — 2023. — № 11. — С. 45–58.

5. Иванов, Н. А. Тактические особенности использования систем биометрической идентификации при установлении личности

неустановленного преступника / Н. А. Иванов // Эксперт-криминалист. — 2025. — № 2. — С. 2–5.

6. Смирнов, А. В. Уголовный процесс : учебник / А. В. Смирнов, К. Б. Калиновский ; под общ. ред. А. В. Смирнова. — 9-е изд., перераб. — Москва : Норма : ИНФРА-М, 2024. — 784 с.

7. Association of Large Data Operators. Annual Report on the use of depersonalized data in law enforcement. — Moscow, 2025. — 45 p.

8. Kerr, O. S. Computer Crime Law (4th Edition). — St. Paul : West Academic Publishing, 2023. — 912 p.

9. Solove, D. J. Digital Persona and the Fourth Amendment // The Yale Law Journal. — 2023. — Vol. 132. — P. 1500–1560.

Информация об авторах

С.Д. ПОРТНЫХ — студент 4 курса.

Information about authors

S.D. PORTNYKH — 4st year student.