УДК 343.98

Колотовкина А.А.
магистрант 3 курса
Красноярский государственный аграрный университет
(г. Красноярск, Россия)

КРИМИНАЛИСТИЧЕСКОЕ ЗНАЧЕНИЕ СОЦИАЛЬНЫХ СЕТЕЙ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ ЭКСТРЕМИСТСКОЙ НАПРАВЛЕННОСТИ

Аннотация: *в статье рассматривается криминалистическое значение социальных сетей при расследовании преступлений экстремистской направленности. Раскрываются особенности социальной сети как цифровой среды, систематизируются основные группы размещаемых в ней сведений и цифровых следов, анализируется их значение для выдвижения и проверки следственных версий. Особое внимание уделяется установлению принадлежности учетной записи, авторства публикаций, содержания и контекста высказываний, а также разграничению цифровой активности и юридически значимого поведения. Обосновывается необходимость комплексной оценки содержательных, технических, временных и контекстуальных данных.*

Ключевые слова: *социальная сеть, преступление экстремистской направленности, криминалистическое значение, цифровой след, учетная запись, авторство публикации, доказывание, контекст публикации.*

Расширение цифровых коммуникаций существенно изменило информационную среду, в которой подготавливаются, совершаются и обсуждаются противоправные деяния. Социальные сети обеспечивают возможность быстрого распространения текстов, изображений, аудио- и видеоматериалов, поддержания групповых коммуникаций и взаимодействия пользователей независимо от их фактического местонахождения. Поэтому для расследования преступлений экстремистской направленности они имеют двойное значение: могут выступать средой совершения отдельных действий и

одновременно источником сведений об обстоятельствах события, участниках и связях между ними [2, с. 41, 3, с. 54].

Актуальность криминалистического исследования обусловлена не только объемом доступного контента, но и его изменчивостью. Публикации редактируются и удаляются, псевдонимы и сведения профиля изменяются, доступ к странице ограничивается, а материалы могут автоматически исчезать. В цифровой среде пользовательские действия сопровождаются техническими записями, которые не всегда видны при обычном просмотре страницы. Несвоевременное выявление и сохранение таких данных способно привести к утрате сведений, необходимых для проверки версии или восстановления последовательности действий.

Цель настоящей статьи состоит в определении основных криминалистически значимых групп информации, размещенной в социальных сетях, и раскрытии условий, при которых такая информация может быть использована при расследовании преступлений экстремистской направленности. Методологическую основу составляют анализ и синтез, формально-логический и сравнительно-правовой методы, а также обобщение положений научной литературы и материалов правоприменительной практики.

Социальную сеть целесообразно рассматривать не только как интернет-страницу или мобильное приложение, предназначенное для общения. В криминалистическом аспекте это сложная цифровая экосистема, включающая учетные записи, публичные страницы, сообщества, средства личной и групповой коммуникации, механизмы размещения и распространения контента, системы хранения данных и алгоритмы рекомендаций. Ее содержание создается как пользователями, так и программными средствами платформы. Такое понимание позволяет исследовать одновременно видимый материал и сведения о действиях, которые сопровождали его создание, изменение, передачу и распространение [7, с. 246–253].

Структура социальной сети может быть представлена в виде совокупности узлов и связей. Узлами выступают учетные записи, сообщества,

отдельные публикации и иные цифровые объекты. Связи образуются посредством подписок, переписки, упоминаний, комментариев, реакций, пересылок и совместного участия в группах. Их анализ помогает установить круг контактов, последовательность коммуникаций и устойчивые модели взаимодействия. Вместе с тем наличие связи между двумя аккаунтами само по себе не подтверждает преступный характер отношений: она может объясняться общими интересами, учебой, работой, родственными или иными социальными контактами.

Содержащуюся в социальной сети информацию можно условно разделить на несколько взаимосвязанных групп. Первая группа — сведения профиля: имя или псевдоним, фотография, описание, заявленные место проживания, образование, работа и контактные данные. Они могут использоваться для выдвижения версии о личности пользователя и поиска связанных учетных записей. Однако сведения профиля, как правило, формируются самим пользователем, могут быть неполными, вымышленными или скопированными. Совпадение имени, фотографии и иных открытых характеристик поэтому не является достаточным основанием для категоричного вывода о принадлежности аккаунта конкретному человеку [1, с. 35–37].

Вторая группа включает пользовательский контент: публикации, комментарии, личные и групповые сообщения, фотографии, видеозаписи и прямые трансляции. Содержание таких объектов может отражать мотивы поведения, осведомленность о конкретных обстоятельствах, подготовительные действия, взаимодействие с другими лицами либо поведение после события. Для правильной интерпретации необходимо исследовать не только отдельную фразу или изображение, но и весь материал, последовательность сообщений, предшествующие и последующие публикации, адресатов и условия распространения.

Третью группу составляют метаданные и технические сведения: дата и время размещения, история редактирования, параметры файла, данные о загрузке, авторизации и используемом устройстве, если такие сведения

доступны и получены законным способом. Их значение заключается в возможности восстановить временную последовательность действий, сопоставить публикации с другими событиями и выявить признаки изменения материала. При этом отображаемое платформой время может зависеть от часового пояса, а преобразование изображения или видео при загрузке может изменять исходные свойства файла. Следовательно, технические данные должны оцениваться с учетом архитектуры и правил работы конкретного сервиса.

Четвертая группа — сведения о цифровой активности и сетевых связях: подписки, реакции, репосты, упоминания, участие в сообществах, история взаимодействия с публикациями и контакты. Анализ их последовательности может выявить повторяющиеся модели поведения или согласованное распространение материалов. Однако алгоритмы платформы самостоятельно рекомендуют контент и контакты, поэтому появление публикации в ленте, автоматическое уведомление или рекомендация не доказывают, что пользователь целенаправленно искал материал либо ознакомился с ним. Значение такого признака возможно определить только в совокупности с другими сведениями.

Социальная сеть может иметь значение на различных этапах расследования. На первоначальном этапе открытые сведения позволяют обнаружить публикации, уточнить данные о проверяемом лице, выявить возможных свидетелей, установить круг общения и определить цифровые объекты, подлежащие дальнейшей проверке. На последующих этапах исследуются связи между учетными записями, содержание коммуникаций, хронология публикаций и технические характеристики файлов. Полученные данные помогают формулировать следственные версии, планировать следственные действия, сопоставлять показания с другими доказательствами и определять необходимость экспертного исследования [1, с. 35–37, 11, с. 250–262].

Для преступлений экстремистской направленности особое значение приобретает исследование содержания и направленности распространенных

материалов, обстоятельств их размещения, доступности для других пользователей, действий по повторному распространению и фактической роли каждого участника. Исследование не должно ограничиваться наличием публикации на странице. Необходимо установить, кем и при каких обстоятельствах создан материал, каков его полный контекст, кому он был адресован, какие действия совершались с ним и какие сведения подтверждают связь пользователя с конкретным действием. Данный подход соответствует выводу о необходимости комплексного анализа содержания публикаций, личности пользователя и его сетевых связей [2, с. 41–45].

С криминалистической точки зрения важно различать различные формы поведения в сети. Создание и размещение материала, его пересылка, комментарий, реакция, подписка на сообщество и простое отображение публикации в рекомендательной ленте имеют разную фактическую природу. Их нельзя автоматически приравнивать друг к другу. В частности, критическое высказывание, участие в дискуссии, подписка на страницу или техническое появление материала в ленте сами по себе не устанавливают наличие умысла на совершение преступления. Правовая оценка должна учитывать содержание и контекст высказывания, направленность действий, осознание пользователем характера размещаемой информации и совокупность иных обстоятельств, а также соответствующие разъяснения судебной практики [5].

Важной проблемой остается разграничение авторства публикации и формальной принадлежности учетной записи. Аккаунт может быть создан с использованием недостоверных сведений, взломан, передан другому лицу или использоваться несколькими пользователями. Поэтому при установлении лица, совершившего определенное действие, следует сопоставлять сведения профиля с характером переписки, устройствами и подключениями, временем активности, языковыми особенностями текста и обстоятельствами реальной жизни, отраженными в цифровой коммуникации. Ни один из перечисленных признаков не должен рассматриваться изолированно.

Самостоятельное значение имеет проверка подлинности цифрового контента. Текст может быть отредактирован, изображение — обработано, видеозапись — смонтирована, а дата публикации — изменена при копировании или повторной загрузке. Развитие инструментов генерации контента дополнительно усложняет разграничение оригинальных и искусственно созданных материалов. Поэтому криминалистическая оценка должна включать исследование происхождения файла, его метаданных, признаков редактирования, согласованности временных отметок и соответствия другим установленным обстоятельствам. Внешняя убедительность фотографии или видеозаписи не является самостоятельным подтверждением места, времени и обстоятельств съемки.

Материал, обнаруженный в социальной сети, и доказательство в уголовно-процессуальном смысле не являются тождественными категориями. Информация приобретает значение доказательства не вследствие самого факта ее размещения в Интернете, а при получении и закреплении в установленном законом порядке. При этом должны быть проверяемы источник материала, способ доступа, обстоятельства обнаружения, целостность и связь с расследуемым событием. Обычный снимок экрана может отражать лишь видимую часть страницы и не содержать сведений, достаточных для установления происхождения объекта, его целесообразно сопоставлять с осмотром устройства, исходными файлами, перепиской и иными данными [11, с. 250–262].

При исследовании сведений из социальных сетей следует разграничивать открытые данные, персональные данные и информацию, охраняемую тайной переписки и иных сообщений. Публичная доступность страницы не означает неограниченного права на получение любых связанных с ней сведений. Доступ к открытому контенту и получение закрытой переписки различаются по фактическому способу и правовым основаниям. Действия по сбору информации должны соответствовать требованиям уголовно-процессуального

законодательства, законодательства об оперативно-розыскной деятельности и противодействии экстремистской деятельности [4, 8–10].

Практическое значение комплексного подхода проявляется и при оценке доказательственной совокупности. Например, публикация может содержать определенное сообщение, а технические сведения — подтверждать время его размещения, история переписки — раскрывать контекст, информация о входах и устройствах — помогать проверить версию об авторстве, показания и результаты иных следственных действий — подтвердить или опровергнуть связь лица с соответствующим действием. Только сопоставление разнородных источников позволяет избежать подмены доказывания единичным цифровым совпадением.

Социальные сети представляют собой самостоятельную криминалистически значимую цифровую среду, в которой сочетаются пользовательский контент, технические данные и сведения о сетевых взаимодействиях. Их значение для расследования преступлений экстремистской направленности определяется возможностью получить сведения о содержании коммуникаций, последовательности действий, участниках и связях между ними.

Криминалистическая оценка информации из социальных сетей должна строиться на комплексном исследовании профиля, публикаций, метаданных, цифровой активности и контекста. Принадлежность учетной записи не равнозначна доказанному авторству конкретного сообщения, а подписка, реакция, рекомендация алгоритма или присутствие публикации в ленте не подтверждают сами по себе наличие преступного умысла.

В качестве практических ориентиров предлагается использовать совокупную проверку содержательных, технических, временных и контекстуальных признаков, фиксировать источник и условия получения цифрового объекта, отдельно оценивать его происхождение и целостность, разграничивать предварительную аналитическую информацию и процессуально закрепленные доказательства. Такой подход способствует повышению обоснованности следственных версий и снижает риск ошибочного толкования цифровой активности.

СПИСОК ЛИТЕРАТУРЫ:

1. Афанасьев Е.А. О некоторых возможностях использования в расследовании преступлений данных, полученных из социальных сетей // Научный Лидер. 2021. № 36 (38). С. 35–37
2. Болвачев М.А. Использование социальных сетей при расследовании преступлений экстремистской направленности: дис. ... канд. юрид. наук. Калининград, 2022. 202 с.
3. Дремлюга Р.И. Интернет-преступность: монография. Владивосток: Изд-во Дальневосточного университета, 2018. 165 с.
4. Конституция Российской Федерации (с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 г., с изменениями, внесенными ФКЗ от 04.10.2022 № 8-ФКЗ) // Официальный интернет-портал правовой информации. 06.10.2022. Ст. 0001202210060013
5. Постановление Пленума Верховного Суда Российской Федерации от 28.06.2011 № 11 «О судебной практике по уголовным делам о преступлениях экстремистской направленности» // Бюллетень Верховного Суда РФ. 2011. № 8
6. Русскевич Е.А. Уголовное право и «цифровая преступность»: проблемы и решения: монография. Москва: НИЦ ИНФРА-М, 2023. 133 с.
7. Смушкин А.Б. Криминалистическое исследование страницы в социальных сетях // Вестник Томского государственного университета. 2024. № 505. С. 246–253 https://doi.org/10.17223/15617793/505/27
8. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ // Собрание законодательства РФ. 24.12.2001. № 52
9. Федеральный закон от 25.07.2002 № 114-ФЗ «О противодействии экстремистской деятельности» // Собрание законодательства РФ. 29.07.2002. № 30. Ст. 3031
10. Федеральный закон от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности» // Российская газета. 18.08.1995. № 160
11. Чич Ю.А., Романов А.В. Процессуальные особенности собирания электронных доказательств в социальных сетях // Эпомен. 2026. № 113. С. 250–262

Kolotovkina A.A.
master's degree student of 3rd year
Krasnoyarsk State Agrarian University
(Krasnoyarsk, Russia)

FORENSIC SIGNIFICANCE OF SOCIAL NETWORKS IN INVESTIGATING EXTREMIST CRIMES

Abstract: *the article examines the forensic significance of social networks in investigating extremist crimes. It describes the characteristics of social networks as a digital environment, categorizes the main types of information posted on them and digital traces left there, and analyzes their value for developing and testing investigative hypotheses. Particular attention is paid to establishing account ownership, authorship of posts, and the content and context of statements, as well as distinguishing digital activity from legally significant conduct. The article argues for a comprehensive assessment of content, technical, temporal, and contextual data.*

Keywords: *social network, extremist crime, forensic significance, digital trace, user account, post authorship, proof, post context.*