

УДК 343.1

DOI: 10.34670/AR.2026.12.21.058

**Предмет доказывания и цифровые следы по уголовным делам о
распространении экстремистских материалов, созданных с
использованием технологий искусственного интеллекта**

Парфёнов Константин Иванович

Старший преподаватель,
кафедра информационного обеспечения органов внутренних дел,
Уральский юридический институт МВД России,
620057, Российская Федерация, Екатеринбург, ул. Корепина, 66;
e-mail: russia.pki@gmail.com

Аннотация

В статье исследуются особенности предмета и пределов доказывания, а также системы цифровых следов по уголовным делам о распространении экстремистских материалов, созданных с использованием технологий искусственного интеллекта. Обосновывается тезис о том, что предмет доказывания по делам данной категории расширяется за счёт включения обстоятельств, характеризующих происхождение материала, степень участия лица в его создании и характер взаимодействия лица с генеративной нейросетью. Анализируется специфика установления субъективной стороны как центрального и наиболее сложного элемента предмета доказывания, а также рассматривается дискуссия о допустимых пределах вывода о форме вины на основании объективных цифровых данных. Раскрывается понятие цифрового следа применительно к нейросетевому контенту, анализируются доктринальные разногласия относительно содержания понятия электронного доказательства, предлагается классификация цифровых следов на следы взаимодействия пользователя с нейросетью, следы самого процесса генерации и следы распространения материала. Особое внимание уделяется доказательственному значению промта как зафиксированного выражения воли пользователя, а также метаданных, журналов обращений к сервису и иных производных данных. Рассматриваются процессуальные формы закрепления цифровых следов и проблемы, обусловленные нахождением значительной части таких следов под контролем третьих лиц — операторов нейросетевых сервисов, в том числе иностранных, а также трансграничным характером хранения данных. Формулируется вывод о том, что специфика предмета доказывания и системы цифровых следов по делам рассматриваемой категории требует выработки самостоятельных методических подходов к собиранию и проверке доказательств.

Для цитирования в научных исследованиях

Парфёнов К.И. Предмет доказывания и цифровые следы по уголовным делам о распространении экстремистских материалов, созданных с использованием технологий искусственного интеллекта // Вопросы российского и международного права. 2026. Том 16. № 7А. С. 564-575. DOI: 10.34670/AR.2026.12.21.058

Ключевые слова

Предмет доказывания, пределы доказывания, цифровые следы, электронные доказательства, экстремистские материалы, генеративные нейросети, искусственный интеллект, промт, метаданные, трансграничный доступ к данным.

Введение

Уголовно-правовая характеристика деяний, связанных с распространением экстремистских материалов, созданных с использованием технологий искусственного интеллекта, образует лишь исходную основу для решения главной практической задачи - доказывания обстоятельств таких деяний в ходе предварительного расследования и судебного разбирательства. Если материально-правовая оценка позволяет ответить на вопрос о том, какие признаки деяния подлежат установлению, то именно процессуальная плоскость определяет, каким образом эти признаки могут быть установлены при помощи допустимых, относимых и достоверных доказательств. Применительно к рассматриваемой категории уголовных дел эта задача приобретает особую остроту, поскольку появление между волей человека и противоправным результатом промежуточного звена в виде генеративной нейросети меняет как состав обстоятельств, подлежащих доказыванию, так и саму природу следов, в которых отражается событие преступления.

Проблематика доказывания по уголовным делам, сопряженным с использованием информационно-телекоммуникационных технологий, в последние годы привлекает устойчивое внимание исследователей. Общие вопросы теории доказывания разработаны в трудах В.А. Лазаревой, С.А. Шейфера и многих других процессуалистов. Криминалистические аспекты работы с электронной информацией исследуются в работах В.Б. Вехова, Е.Р. Россинской и иных представителей криминалистической науки [Лазарева, 2018; Шейфер, 2014; Вехов, 2016; Россинская, Рябцев, 2019]. Вместе с тем вопрос о специфике предмета доказывания и системы цифровых следов применительно к деяниям, при которых противоправный материал создается не человеком непосредственно, а генеративной нейросетью по инициативе человека, в процессуальной и криминалистической литературе самостоятельно не рассматривался. Настоящая статья представляет собой попытку восполнить этот пробел в той части, которая относится к материально-процессуальной основе доказывания, то есть к определению круга подлежащих установлению обстоятельств и характеристике отражающих их следов.

Материалы и методы исследования

Необходимо сразу оговорить методологические ограничения исследования. Самостоятельная судебная практика по уголовным делам о распространении экстремистских материалов, созданных именно с использованием генеративных нейросетей, в Российской Федерации на момент подготовки работы фактически отсутствует, что объясняется новизной технологии и кратким периодом ее массового распространения. По этой причине выводы статьи опираются, во-первых, на сложившуюся практику доказывания по делам о распространении экстремистских материалов в информационно-телекоммуникационной сети «Интернет», взятую в качестве отправной точки, и, во-вторых, на метод юридического моделирования типовых следственных ситуаций, посредством которого выявляются обстоятельства, не находящие аналога в практике расследования «традиционных» преступлений данной группы.

Такой подход не позволяет претендовать на исчерпывающие эмпирически подтвержденные обобщения, однако дает возможность заблаговременно обозначить проблемы, с которыми правоприменитель неизбежно столкнется по мере распространения соответствующих деяний.

Результаты и обсуждение

Предмет доказывания по уголовному делу определяется ст. 73 Уголовно-процессуального кодекса Российской Федерации [Уголовно-процессуальный кодекс РФ, 2001] и включает в себя событие преступления, виновность лица, форму его вины и мотивы, обстоятельства, характеризующие личность обвиняемого, а также иные обстоятельства, перечисленные в данной норме. Этот перечень носит общий характер и подлежит конкретизации применительно к отдельным категориям уголовных дел с учетом особенностей соответствующих составов преступлений. В теории уголовного процесса прочно утвердилось представление о том, что предмет доказывания, оставаясь единым в своей нормативной основе, наполняется специфическим содержанием в зависимости от вида расследуемого преступления [Лазарева, 2018; Шейфер, 2014]. Распространение экстремистских материалов, созданных нейросетью, представляет собой именно такую категорию, при расследовании которой общие положения о предмете доказывания требуют существенной конкретизации.

Прежде всего необходимо отметить, что событие преступления по делам рассматриваемой категории приобретает усложненную структуру. При распространении «традиционного» экстремистского материала событие преступления охватывает создание материала и его доведение до сведения третьих лиц, причем оба эти действия совершаются непосредственно человеком. При использовании генеративной нейросети в структуре события появляется дополнительный элемент - процесс машинной генерации контента, опосредующий связь между действиями лица и возникновением материала. Установлению, таким образом, подлежит не только факт распространения материала, но и факт его создания именно посредством нейросети, а также характер участия лица в этом процессе. Без выяснения этих обстоятельств невозможно дать правильную уголовно-правовую оценку деянию, в частности разграничить создание и распространение материала, о чем подробно говорилось нами в предшествующем исследовании.

Из сказанного следует, что предмет доказывания по делам данной категории расширяется за счет включения в него ряда специфических обстоятельств, не свойственных делам о распространении экстремистских материалов, созданных без использования технологий искусственного интеллекта. К числу таких обстоятельств мы относим прежде всего факт создания распространенного материала с использованием генеративной нейросети, что само по себе нуждается в доказывании и не может презюмироваться. Не менее важна идентификация конкретной нейросети, то есть программного средства или сервиса, посредством которого был создан материал. Подлежит установлению и содержание запроса (промта), на основании которого был сгенерирован материал, поскольку именно запрос отражает направленность воли пользователя. Наконец, доказыванию подлежит степень содержательного контроля лица над результатом генерации, позволяющая определить, выступает ли лицо создателем материала или только его распространителем. Каждое из перечисленных обстоятельств обладает самостоятельным доказательственным значением и требует установления при помощи определенной совокупности доказательств.

Расширение предмета доказывания затрагивает не только событие преступления, но и иные

элементы, перечисленные в ст. 73 УПК РФ. Так, обстоятельства, характеризующие личность обвиняемого, по делам данной категории включают в себя сведения о его навыках работы с технологиями искусственного интеллекта, об опыте использования конкретных нейросетевых сервисов, о наличии или отсутствии у него специальных познаний, позволяющих целенаправленно обходить установленные в нейросетях ограничения на генерацию противоправного контента. Эти сведения значимы не только для индивидуализации ответственности, но и для оценки достоверности доводов лица о случайном или непреднамеренном характере полученного результата. Лицо, систематически и со знанием дела взаимодействующее с нейросетью, и лицо, впервые обратившееся к подобному сервису, находятся в принципиально разном положении с точки зрения возможности предвидеть характер генерируемого контента.

Особое место в предмете доказывания по делам рассматриваемой категории занимает субъективная сторона преступления. Как было показано ранее, психическое отношение лица к экстремистскому характеру распространяемого материала является решающим для квалификации, а возможные варианты этого отношения варьируются от прямого умысла до невиновного распространения. Доказывание субъективной стороны по делам данной категории осложняется тем обстоятельством, что подозреваемый или обвиняемый получает удобную линию защиты, ссылаясь на отсутствие осознания экстремистского характера материала, сгенерированного нейросетью, либо на то, что экстремистский результат явился неожиданным и нежелательным для него следствием нейтрального запроса. Опровержение или подтверждение подобных доводов невозможно без обращения к объективным данным, отражающим реальный характер взаимодействия лица с нейросетью. Именно здесь предмет доказывания смыкается с проблематикой цифровых следов, поскольку только зафиксированные следы такого взаимодействия способны дать объективную картину направленности умысла лица.

Здесь уместно обозначить и более общее теоретическое затруднение, относительно которого в науке нет единства. Речь идет о допустимых пределах использования объективных данных для вывода о субъективной стороне деяния. Одни исследователи исходят из того, что содержание запросов и характер действий лица позволяют с достаточной надежностью реконструировать направленность его умысла, тогда как другие предостерегают от подмены доказывания вины формальной оценкой внешней стороны поведения. Мы разделяем ту позицию, согласно которой объективные цифровые следы являются необходимым, но не самодостаточным средством доказывания субъективной стороны: они подлежат оценке в совокупности с иными доказательствами, характеризующими личность лица, его осведомленность и реальные намерения. Абсолютизация любого отдельно взятого следа, будь то текст запроса или факт многократного обращения к нейросети, способна привести к ошибочным выводам о форме вины. Особую осторожность следует проявлять в ситуациях, когда содержание запроса допускает несколько толкований, а характер последующего распространения материала не позволяет однозначно судить о том, осознавал ли пользователь экстремистский смысл сгенерированного контента.

Пределы доказывания, под которыми в теории уголовного процесса понимается необходимая и достаточная совокупность доказательств, обеспечивающая достоверное установление обстоятельств предмета доказывания, по делам рассматриваемой категории также обладают известной спецификой. С одной стороны, расширение предмета доказывания за счет специфических обстоятельств влечет за собой и расширение круга доказательств, подлежащих

собираению. С другой стороны, значительная часть относимых доказательств имеет цифровую природу и сосредоточена в инфраструктуре, находящейся вне непосредственного контроля органов предварительного расследования, что объективно затрудняет достижение необходимой полноты доказывания. Определение момента, когда совокупность собранных доказательств может считаться достаточной, по делам данной категории осложняется тем, что отсутствие отдельных цифровых следов далеко не всегда свидетельствует об их изначальном отсутствии и может быть результатом их уничтожения, недоступности либо нахождения на серверах, расположенных за пределами юрисдикции Российской Федерации. Следовательно, таким образом, нередко вынужден формировать вывод о доказанности обстоятельств дела в условиях заведомо неполного доступа к существующим, но недостижимым следам, что предъявляет повышенные требования к надежности тех доказательств, которые объективно доступны.

Переходя к рассмотрению цифровых следов как элемента доказательственной базы, необходимо прежде всего определить содержание самого этого понятия применительно к рассматриваемой категории дел. Следует отметить, что в теории уголовного процесса и криминалистике до настоящего времени не сложилось единого понимания природы доказательств, имеющих электронную форму. В литературе используются различные обозначения - «электронные доказательства», «цифровые доказательства», «электронные следы», «цифровые следы», - причем за терминологическими расхождениями стоят и содержательные разногласия. Часть исследователей рассматривает электронную информацию как самостоятельный вид доказательств, не укладывающийся в существующую систему источников доказательств, закрепленную в ст. 74 УПК РФ, и предлагает дополнить эту систему соответствующим самостоятельным видом. Другие авторы исходят из того, что электронная информация не образует нового вида доказательств, а лишь приобретает значение доказательства, будучи облеченной в одну из предусмотренных законом процессуальных форм - чаще всего в форму вещественного доказательства или иного документа. Этот спор имеет не только теоретическое, но и сугубо практическое значение, поскольку от его разрешения зависит порядок собирания, проверки и оценки соответствующих сведений.

Не вступая в развернутую полемику, выходящую за рамки темы, отметим, что, на наш взгляд, более убедительной является позиция, согласно которой цифровые следы как таковые не образуют самостоятельного вида доказательств, а служат материальным субстратом, из которого доказательство формируется в результате его процессуального закрепления. В этом смысле понятие цифрового следа является скорее криминалистическим, нежели строго процессуальным: оно описывает объективно существующую информацию до и независимо от того, придана ли ей процессуальная форма. Применительно к настоящему исследованию мы используем понятие цифрового следа в указанном криминалистическом значении, понимая под ним имеющую значение для дела информацию, зафиксированную в электронно-цифровой форме на материальном носителе и образующуюся в результате действий с использованием электронных устройств и информационно-телекоммуникационных технологий [Вехов, 2016; Россинская, Рябцев, 2019]. Применительно к распространению нейросетевого экстремистского контента понятие цифрового следа охватывает совокупность данных, отражающих как процесс создания материала посредством нейросети, так и процесс его последующего распространения.

Специфика цифровых следов по делам рассматриваемой категории состоит в том, что они образуются на нескольких относительно самостоятельных стадиях и в нескольких местах одновременно. Это обстоятельство, на наш взгляд, обуславливает необходимость их классификации, которая имела бы не только теоретическое, но и прикладное значение,

ориентируя следователя на поиск следов в каждой из соответствующих точек их образования. Мы предлагаем классифицировать цифровые следы по делам рассматриваемой категории на три основные группы в зависимости от стадии, на которой они образуются.

Первую группу составляют следы взаимодействия пользователя с нейросетью. К ним относятся прежде всего запросы (промты), которые пользователь направлял нейросети, а также полученные от нее ответы. Сюда же следует отнести историю диалога с нейросетью, сохраняемую как на устройстве пользователя, так и на стороне сервиса, данные об учетной записи, использованной для доступа к сервису, а также сведения о времени и продолжительности сеансов взаимодействия. Эта группа следов имеет ключевое значение для установления направленности воли пользователя и степени его участия в создании материала.

Вторую группу образуют следы самого процесса генерации, формирующиеся на стороне нейросетевого сервиса. К ним относятся технические записи (журналы, логи) об обращениях к модели, параметры генерации, идентификаторы запросов, а в ряде случаев и сведения о версии модели, использованной для создания контента. Доступ к этой группе следов, как правило, наиболее затруднен, поскольку они находятся под исключительным контролем оператора сервиса. Между тем именно эти следы способны подтвердить или опровергнуть факт создания конкретного материала конкретной моделью в конкретный момент времени, а потому их доказательственная ценность весьма высока.

Третью группу составляют следы распространения материала. Они образуются в момент и в результате доведения сгенерированного материала до сведения третьих лиц и включают в себя данные о публикации материала в социальной сети, мессенджере или ином сетевом ресурсе, сведения об аккаунте, с которого осуществлено распространение, данные о просмотрах и иных формах взаимодействия аудитории с материалом, а также метаданные распространенного файла. Эта группа следов в наибольшей степени сходна с цифровыми следами по «обычным» делам о распространении экстремистских материалов в сети и устанавливается по сравнительно отработанным методикам.

Предложенная классификация позволяет наглядно увидеть принципиальное отличие дел рассматриваемой категории от «традиционных». При распространении созданного человеком материала первые две группы следов попросту отсутствуют, поскольку отсутствует и сам этап машинной генерации; доказательственная деятельность сосредотачивается на следах распространения. При использовании же нейросети центр тяжести смещается к первым двум группам, и именно они, как правило, оказываются решающими для правильной квалификации деяния и установления формы вины. Тем самым классификация не только описывает структуру следовой картины, но и указывает следователю направления поиска доказательств, которые в практике расследования «обычных» дел этой группы вообще не возникали.

Центральное место среди всех перечисленных цифровых следов занимает, по нашему убеждению, промт - текстовый запрос, посредством которого пользователь инициировал генерацию материала. Доказательственное значение промта определяется тем, что он представляет собой зафиксированное в цифровой форме выражение воли пользователя, непосредственно предшествующее возникновению материала и определяющее его содержание. Если содержание сгенерированного материала отражает результат работы нейросети, то содержание промта отражает намерение человека. Именно поэтому промт способен выступать важнейшим источником сведений о субъективной стороне деяния. Запрос, прямо требующий создания контента экстремистского содержания, свидетельствует о целенаправленности действий лица; нейтральный запрос, повлекший неожиданную генерацию экстремистского

материала, может, напротив, указывать на отсутствие соответствующего умысла. Анализ совокупности запросов, направленных пользователем, позволяет проследить динамику его взаимодействия с нейросетью и выявить, например, целенаправленные попытки обойти установленные в нейросети ограничения путем последовательного переформулирования запросов.

Особую доказательственную ценность приобретает именно последовательность запросов, рассматриваемая как единое целое. Если разработчики нейросети предусмотрели ограничения, препятствующие генерации противоправного контента, то получение такого контента нередко требует от пользователя неоднократных попыток, направленных на обход этих ограничений. Зафиксированная история подобных попыток, в которой видно, как пользователь шаг за шагом переформулирует запрос, добиваясь нужного результата, способна служить весомым доказательством целенаправленности его действий и, следовательно, наличия умысла. И напротив, единичный нейтральный запрос, повлекший непредвиденный результат, подкрепляет версию о невиновном характере действий лица. Таким образом, доказательственное значение имеет не только содержание отдельного промта, но и вся структура диалога пользователя с нейросетью.

Вместе с тем доказательственное использование промта сопряжено с рядом проблем, которые требуют осмысления. Первая из них состоит в том, что промт далеко не всегда сохраняется в доступном для органов расследования виде. Если пользователь взаимодействовал с нейросетью через веб-интерфейс без сохранения истории либо целенаправленно удалил историю диалога, восстановление содержания запросов на стороне пользовательского устройства может оказаться невозможным. В подобных случаях единственным источником сведений о содержании промта остаются данные на стороне оператора сервиса, доступ к которым, как уже отмечалось, существенно затруднен. Вторая проблема связана с установлением достоверной связи между конкретным промтом и конкретным сгенерированным материалом. Сам по себе факт обнаружения на устройстве пользователя некоторого запроса экстремистского содержания еще не доказывает, что именно этот запрос повлек создание именно того материала, который был впоследствии распространен. Установление такой связи требует сопоставления содержания запроса и результата генерации, что в силу стохастической природы нейросетей далеко не всегда может быть осуществлено с категорической достоверностью. Указанная проблема имеет преимущественно экспертный характер и подробно рассматривается нами в рамках самостоятельного исследования, посвященного судебным экспертизам по делам данной категории.

Существенное доказательственное значение наряду с промтом имеют метаданные сгенерированного материала. Под метаданными понимаются сведения, описывающие характеристики файла и сопутствующие обстоятельства его создания. Применительно к нейросетевому контенту метаданные могут содержать указание на программное средство, при помощи которого создан файл, дату и время его создания, а в отдельных случаях - специальные маркеры, предоставляемые некоторыми сервисами при генерации контента. В последние годы ряд разработчиков внедряет технологии нанесения на сгенерированный контент скрытых либо явных признаков машинного происхождения, в том числе посредством цифровых водяных знаков. Обнаружение подобных маркеров способно служить весомым доказательством машинного происхождения распространенного материала. Следует, однако, учитывать, что метаданные сравнительно легко поддаются изменению или удалению, а отсутствие маркеров машинного происхождения само по себе не свидетельствует о том, что материал создан

человеком. Поэтому метаданные, при всей их значимости, не могут рассматриваться как самостоятельное доказательство и подлежат оценке в совокупности с иными данными.

Помимо содержания самих цифровых следов, самостоятельного рассмотрения заслуживает вопрос о процессуальных формах их закрепления. Объективно существующая цифровая информация приобретает значение доказательства лишь тогда, когда она зафиксирована в установленном законом порядке и облечена в одну из предусмотренных процессуальных форм. Применительно к цифровым следам по делам рассматриваемой категории основными процессуальными способами их закрепления выступают осмотр электронных носителей информации и интернет-страниц, выемка и изъятие электронных носителей, получение информации у владельцев информационных ресурсов, а также назначение судебных экспертиз. Каждый из этих способов имеет свои особенности применительно к нейросетевому контенту. Так, осмотр интернет-страницы, на которой размещен распространенный материал, фиксирует лишь следы распространения, но не следы создания материала; для закрепления последних требуется доступ к устройству пользователя либо к данным оператора сервиса. Это означает, что полнота закрепления следовой картины напрямую зависит от того, насколько своевременно и тактически грамотно органы расследования получили доступ к соответствующим носителям, поскольку цифровые следы отличаются повышенной уязвимостью и могут быть уничтожены или изменены в короткие сроки.

Особое внимание следует обратить на необходимость обеспечения неизменности цифровых следов с момента их обнаружения и до момента исследования. Доказательственная ценность цифрового следа напрямую зависит от того, может ли быть подтверждена его аутентичность, то есть тождество исследуемой информации той, что была обнаружена при производстве следственного действия. Применительно к нейросетевому контенту это требование приобретает дополнительное измерение, поскольку защита может ставить под сомнение не только подлинность распространенного материала, но и подлинность зафиксированных запросов и истории взаимодействия с нейросетью. Обеспечение проверяемости и неизменности этих данных, в том числе посредством фиксации их контрольных сумм и подробного документирования процесса изъятия, становится необходимым условием признания соответствующих доказательств допустимыми. Подробное рассмотрение тактических приемов, обеспечивающих решение этой задачи, выходит за пределы настоящей статьи и относится к области криминалистической тактики.

Отдельного внимания заслуживает проблема, которая, как нам представляется, является ключевой для всей системы доказывания по делам рассматриваемой категории. Речь идет о том, что значительная, а зачастую и наиболее важная часть цифровых следов находится не под контролем лица, привлекаемого к ответственности, и не в распоряжении органов расследования, а под контролем третьих лиц - операторов нейросетевых сервисов. В отличие от «традиционного» создания экстремистского материала, при котором весь процесс протекает в пределах устройств, доступных для изъятия и исследования, создание материала посредством нейросетевого сервиса предполагает, что существенная часть процесса протекает на удаленных серверах оператора. Следы взаимодействия пользователя с нейросетью и следы самого процесса генерации формируются и хранятся в инфраструктуре оператора, доступ к которой возможен лишь при условии его содействия либо в порядке, предусмотренном для получения сведений у владельцев информационных ресурсов.

Эта проблема многократно усугубляется в тех случаях, когда оператором нейросетевого сервиса выступает иностранное юридическое лицо, а серверы расположены за пределами территории Российской Федерации. Получение цифровых следов, хранящихся в иностранной

юрисдикции, требует обращения к механизмам международного сотрудничества в сфере уголовного судопроизводства, предусмотренным частью пятой УПК РФ и соответствующими международными договорами. Эффективность этих механизмов применительно к данным операторов искусственного интеллекта на сегодняшний день остается невысокой. Сроки исполнения запросов о правовой помощи несопоставимы со сроками предварительного расследования, а в ряде случаев операторы, находящиеся в недружественных юрисдикциях, попросту отказывают в предоставлении сведений либо такие запросы остаются без ответа. Складывается ситуация, при которой доказательства, объективно существующие и имеющие решающее значение для установления обстоятельств дела, фактически оказываются недоступными для органов расследования.

Данное обстоятельство, по нашему мнению, представляет собой одну из наиболее серьезных проблем доказывания по делам рассматриваемой категории, и ее разрешение лежит сразу в нескольких плоскостях. С одной стороны, оно связано с совершенствованием процессуальных механизмов получения данных, хранящихся за рубежом, и развитием международного сотрудничества, что в современных условиях представляется задачей долгосрочной и не всегда выполнимой. С другой стороны, и это, на наш взгляд, более перспективное направление, разрешение проблемы связано с развитием национальной инфраструктуры искусственного интеллекта, операторы которой находились бы в пределах российской юрисдикции и были бы обязаны хранить соответствующие данные на территории Российской Федерации и предоставлять их по запросам органов расследования в установленном порядке. По мере того как отечественные нейросетевые сервисы будут занимать все большую долю на внутреннем рынке, доля цифровых следов, доступных для органов расследования, будет соответственно возрастать.

Из сказанного следует важный для практики вывод: в условиях затрудненного доступа к цифровым следам, хранящимся на стороне оператора, особое значение приобретают цифровые следы, обнаруживаемые на устройствах самого пользователя. История взаимодействия с нейросетью, сохраненная в памяти устройства, кэшированные данные веб-браузера, сохраненные файлы сгенерированного контента, сведения приложений-клиентов нейросетевых сервисов нередко становятся единственным реально доступным источником сведений о процессе создания материала. Это обстоятельство, в свою очередь, предъявляет повышенные требования к своевременности и тактической грамотности изъятия и исследования устройств пользователя, что составляет предмет криминалистической тактики и выходит за рамки настоящей статьи.

Заключение

Подводя итог проведенному анализу, мы можем сформулировать следующие выводы.

Предмет доказывания по уголовным делам о распространении экстремистских материалов, созданных с использованием технологий искусственного интеллекта, расширяется по сравнению с делами о распространении материалов, созданных без использования таких технологий. В него дополнительно включаются обстоятельства, характеризующие факт создания материала посредством нейросети, идентификацию конкретной нейросети, содержание запроса пользователя и степень его содержательного контроля над результатом генерации, а также сведения о навыках и опыте лица в работе с технологиями искусственного интеллекта.

Центральным и наиболее сложным элементом предмета доказывания по делам данной

категории остается субъективная сторона деяния, установление которой невозможно без обращения к объективным цифровым следам взаимодействия лица с нейросетью. При этом цифровые следы являются необходимым, но не самодостаточным средством доказывания субъективной стороны и подлежат оценке в совокупности с иными доказательствами.

Цифровые следы по делам рассматриваемой категории целесообразно классифицировать на следы взаимодействия пользователя с нейросетью, следы процесса генерации и следы распространения материала, что имеет прикладное значение, ориентируя следователя на поиск следов в каждой из соответствующих точек их образования и наглядно демонстрируя отличие следовой картины этих дел от следовой картины «традиционных» преступлений данной группы.

Ключевое доказательственное значение среди цифровых следов имеет промт как зафиксированное в цифровой форме выражение воли пользователя, непосредственно предшествующее возникновению материала. При этом доказательственную ценность представляет не только содержание отдельного запроса, но и вся последовательность запросов, отражающая динамику взаимодействия пользователя с нейросетью. Доказательственное использование промта осложняется проблемами его сохранности и установления достоверной связи между конкретным запросом и конкретным результатом генерации.

Наиболее серьезной проблемой доказывания по делам данной категории является нахождение значительной части цифровых следов под контролем третьих лиц - операторов нейросетевых сервисов, в том числе иностранных, а также трансграничный характер хранения таких данных. В этих условиях возрастает доказательственное значение цифровых следов, обнаруживаемых на устройствах самого пользователя, а перспективным направлением разрешения проблемы выступает развитие национальной инфраструктуры искусственного интеллекта.

В целом проведенное исследование показывает, что специфика предмета доказывания и системы цифровых следов по делам о распространении экстремистских материалов, созданных с использованием технологий искусственного интеллекта, носит качественный, а не только количественный характер и не сводится к простому добавлению новых обстоятельств к традиционному предмету доказывания. Появление генеративной нейросети как промежуточного звена между волей человека и противоправным результатом меняет саму структуру доказательственной деятельности, перемещая ее центр тяжести в цифровую среду и ставя ее в зависимость от доступности данных, контролируемых третьими лицами. Сформулированные положения о предмете доказывания и системе цифровых следов образуют теоретическую основу для последующей разработки процессуальных и криминалистических особенностей собирания и проверки доказательств по делам рассматриваемой категории, в том числе тактики производства следственных действий и назначения судебных экспертиз, что составляет предмет дальнейшего исследования.

Библиография

1. Вехов В.Б. Электронные доказательства: проблемы теории и практики // Правопорядок: история, теория, практика. 2016. № 4 (11). С. 46–50.
2. Лазарева В.А. Доказывание в уголовном процессе: учебно-практическое пособие. 6-е изд., перераб. и доп. Москва: Юрайт, 2018. 359 с.
3. Россинская Е.Р., Рябцев И.А. Концептуальные основы теории информационно-компьютерного обеспечения криминалистической деятельности // Вестник Санкт-Петербургского университета. Право. 2019. Т. 10, вып. 2. С. 224–239.
4. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ // Собрание законодательства Российской Федерации. 2001. № 52 (ч. I). Ст. 4921.

5. Шейфер С.А. Доказательства и доказывание по уголовным делам: проблемы теории и правового регулирования: монография. Москва: Норма: ИНФРА-М, 2014. 240 с.

The Subject of Proof and Digital Traces in Criminal Cases on the Distribution of Extremist Materials Created Using Artificial Intelligence Technologies

Konstantin I. Parfenov

Senior Lecturer,
Department of Information Support of Internal Affairs Bodies,
Ural Law Institute of the Ministry of Internal Affairs of Russia,
620057, 66, Korepina str., Yekaterinburg, Russian Federation;
e-mail: russia.pki@gmail.com

Abstract

The article examines the specific features of the subject and limits of proof, as well as the system of digital traces in criminal cases on the distribution of extremist materials created using artificial intelligence technologies. The thesis is substantiated that the subject of proof in cases of this category is expanded by including circumstances characterizing the origin of the material, the degree of the person's participation in its creation, and the nature of the person's interaction with the generative neural network. The specificity of establishing the subjective element as the central and most complex element of the subject of proof is analyzed, and the discussion on the permissible limits of inferring the form of guilt on the basis of objective digital data is examined. The concept of a digital trace is revealed in relation to neural network content, doctrinal disagreements regarding the content of the concept of electronic evidence are analyzed, and a classification of digital traces is proposed into traces of the user's interaction with the neural network, traces of the generation process itself, and traces of the distribution of the material. Particular attention is paid to the evidentiary significance of the prompt as a recorded expression of the user's will, as well as metadata, service access logs, and other derivative data. The procedural forms of securing digital traces and the problems caused by the fact that a significant part of such traces is under the control of third parties — operators of neural network services, including foreign ones — as well as the transborder nature of data storage, are examined. A conclusion is formulated that the specificity of the subject of proof and the system of digital traces in cases of the category under consideration requires the development of independent methodological approaches to the collection and verification of evidence.

For citation

Parfenov K.I. (2026) *Predmet dokazyvaniya i tsifrovye sledy po ugovolnym delam o rasprostranении ekstremistskikh materialov, sozdannykh s ispol'zovaniem tekhnologiy iskusstvennogo intellekta* [The Subject of Proof and Digital Traces in Criminal Cases on the Distribution of Extremist Materials Created Using Artificial Intelligence Technologies]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 16 (7A), pp. 564-575. DOI: 10.34670/AR.2026.12.21.058

Keywords

Subject of proof, limits of proof, digital traces, electronic evidence, extremist materials, generative neural networks, artificial intelligence, prompt, metadata, transborder access to data.

References

1. Criminal Procedure Code of the Russian Federation of December 18, 2001 No. 174-FZ. (2001). Collection of Legislation of the Russian Federation, (52(1)), Art. 4921.
2. Lazareva, V.A. (2018). Dokazyvanie v ugovnom protsesse [Proving in criminal proceedings] (6th ed.). Moscow: Yurayt.
3. Rossinskaya, E.R., & Ryabtsev, I.A. (2019). Kontseptual'nye osnovy teorii informatsionno-komp'yuternogo obespecheniya kriminalisticheskoy deyatelnosti [Conceptual foundations of the theory of information and computer support of forensic activity]. Vestnik Sankt-Peterburgskogo universiteta. Pravo, 10(2), 224–239.
4. Sheifer, S.A. (2014). Dokazatel'stva i dokazyvanie po ugovnym delam: problemy teorii i pravovogo regulirovaniya [Evidence and proving in criminal cases: problems of theory and legal regulation]. Moscow: Norma: INFRA-M.
5. Vekhov, V.B. (2016). Elektronnye dokazatel'stva: problemy teorii i praktiki [Electronic evidence: problems of theory and practice]. Pravoporyadok: istoriya, teoriya, praktika, (4(11)), 46–50.