

УДК 343

Цифровые следы и искусственный интеллект в уголовном судопроизводстве: проблемы трансформации доказательственного права¹

Большакова Ксения Борисовна, студент, Владимирский государственный университет имени А. Г. и Н. Г. Столетовых, xeniabolshakova@yandex.ru

Грачева Александра Ивановна, студент, Владимирский государственный университет имени А. Г. и Н. Г. Столетовых, alekssndra_g@mail.ru

Статья посвящена анализу актуальных проблем, возникающих при интеграции цифровых следов и технологий искусственного интеллекта в уголовное судопроизводство. Рассматривается влияние цифровых данных и алгоритмов искусственного интеллекта на традиционные институты доказательственного права. Выявляются ключевые сложности, связанные со сбором, проверкой и оценкой цифровых доказательств, а также с использованием результатов работы алгоритмических систем. Формулируются предложения по совершенствованию уголовно-процессуального законодательства с целью его адаптации к условиям цифровой среды.

Ключевые слова: цифровые следы, искусственный интеллект, уголовный процесс, доказательства, доказывание, допустимость доказательств, цифровая криминалистика.

Стремительная цифровизация всех сфер общественной жизни детерминирует трансформацию преступности, порождая новые формы противоправных деяний и видоизменяя традиционные. В этих условиях закономерным является обращение правоприменителя к современным технологиям, таким как искусственный интеллект (ИИ), для противодействия преступным угрозам. Однако внедрение технологий в уголовный процесс, в особенности в его доказательственную сферу, сопряжено с рядом системных проблем, требующих осмысления и законодательного разрешения. Актуальность темы обусловлена нарастающим разрывом между технологическими возможностями и нормативной регламентацией их использования. Целью настоящего исследования является комплексный анализ проблем, возникающих в доказательственном праве в связи с использованием цифровых следов и технологий ИИ, и выработка на его основе предложений по совершенствованию уголовно-процессуального законодательства [1, с. 227].

Как верно отмечается в научной литературе, цифровые технологии породили новый вид следов — цифровые следы, которые представляют собой информацию в электронной форме, хранящуюся на технических устройствах или передающуюся по каналам связи. К ним относятся данные с мобильных устройств, электронная переписка, записи с камер видеонаблюдения и многое другое. В ст. 74 УПК РФ [2] не содержится специального упоминания о «цифровых доказательствах», однако они находят свою нишу в существующей системе средств доказывания, прежде всего в качестве вещественных доказательств или иных документов, если получены и представлены в порядке, предусмотренном ст. 86 УПК РФ.

Основная проблема на стадии собирания таких следов заключается в обеспечении их допустимости. Действующий УПК РФ регламентирует традиционные следственные действия, которые зачастую оказываются недостаточно адаптированными для работы с цифровой информацией. Процедура изъятия электронного носителя, его исследования без надлежащего процессуального оформления, например без применения криптографических методов проверки целостности данных, может привести к утрате доказатель-

ственного значения изъятой информации. В этой связи требуется развитие таких процессуальных форм, как осмотр электронных носителей и выемка электронной информации, с детальной фиксацией применяемых криминалистических методик и программно-аппаратных средств. На стадии проверки цифровых следов возникает проблема их аутентификации и установления подлинности. В отличие от традиционного документа, цифровая информация может быть легко изменена без видимых следов, что требует от следователя и суда специальных знаний или привлечения эксперта для подтверждения неизменности представленных данных [3, с. 308].

Использование ИИ в уголовном процессе носит многогранный характер. Современные исследования справедливо указывают на его применение для криминалистического прогнозирования и анализа больших данных с целью выявления латентной преступности, для автоматизации рутинных операций, таких как распознавание лиц и анализ видеозаписей, а также для формирования результатов, имеющих доказательственное значение, например заключений экспертных систем. Именно этот аспект порождает наиболее сложные правовые проблемы [4, с. 256].

В первую очередь это проблема объяснимости решений, принимаемых алгоритмами машинного обучения, которые зачастую представляют собой «черный ящик». Даже разработчики не всегда могут детально объяснить логику, по которой система пришла к тому или иному выводу. Это вступает в прямое противоречие с принципом оценки доказательств по внутреннему убеждению, основанному на всестороннем, полном и объективном рассмотрении всех обстоятельств дела. Суд, а также стороны обвинения и защиты лишаются возможности проверить логику и достоверность вывода, сформированного ИИ.

Во-вторых, остро стоит вопрос о допустимости таких результатов. Действующий УПК РФ не дает прямого ответа на вопрос, можно ли рассматривать протокол, сгенерированный системой распознавания лиц, или заключение экспертной системы в качестве самостоятельного доказательства [5, с. 22]. Результаты работы ИИ, не подкрепленные заключением специалиста или экс-

¹ Научный руководитель: Ткачук Татьяна Алексеевна — профессор кафедры уголовно-правовых дисциплин, Владимирский государственный университет имени А. Г. и Н. Г. Столетовых, доктор юридических наук, профессор.

перта, несущего персональную ответственность за данное заключение, вряд ли могут соответствовать критерию допустимости, сформулированному в ст. 75 УПК РФ. Кроме того, использование «сырых» данных ИИ без их интерпретации человеком нарушает право обвиняемого на очную ставку и право на проверку доказательств, т. к. оспаривать алгоритм фактически невозможно. Наконец, существует серьезный риск системных ошибок и предвзятости алгоритмов, которые обучаются на определенных массивах данных, содержащих латентные социальные или расовые предубеждения, что может привести к дискриминационным последствиям в уголовном преследовании.

Для преодоления указанных проблем необходима комплексная модернизация уголовно-процессуального законодательства. Первоочередной мерой видится легализация понятия «цифровые доказательства» путем внесения изменений в ст. 74 и 81 УПК РФ, где можно закрепить цифровые следы в качестве самостоятельного вида доказательств или детализировать их статус в рамках вещественных доказательств и иных документов. Параллельно требуется разработка детальных процессуальных стандартов, регламентирующих в УПК РФ процедуры изъятия, осмотра, исследования и хранения цифровых следов, включая требования к программному обеспечению и методам обеспечения целостности данных.

Крайне важна четкая регламентация использования ИИ. Целесообразно закрепить на законодательном уровне, что результаты работы систем ИИ, направленные на установление обстоятельств, имеющих значение для дела, не могут являться самостоятельным

доказательством. Они могут служить лишь вспомогательным материалом или ориентирующей информацией для формирования профессионального убеждения следователя, дознавателя, эксперта или суда. Любой такой результат должен подлежать обязательной проверке и оценке человеком, несущим ответственность за принятое процессуальное решение. В этой связи также необходимо активное внедрение института цифрового специалиста/эксперта путем расширения трактовки ст. 58 и 80 УПК РФ, что стимулировало бы участие специалистов в области информационных технологий и цифровой криминалистики на всех стадиях работы с цифровыми следами.

Таким образом, проникновение цифровых следов и технологий ИИ в уголовное судопроизводство объективно и неизбежно. Однако этот процесс требует взвешенного и осторожного подхода, т. к. затрагивает фундаментальные принципы уголовного процесса: состязательность, допустимость доказательств, право на защиту и оценку доказательств по внутреннему убеждению. Существующее доказательственное право, основанное на аналоговой парадигме, испытывает значительные трудности в адаптации к цифровой среде. Преодоление возникающих проблем видится не в точечных изменениях, а в системной трансформации соответствующих норм УПК РФ. Ключевым вектором такой трансформации должен стать принцип человеческого волеизъявления, согласно которому любое технологически опосредованное доказательство подлежит окончательной оценке и интерпретации субъектом доказывания, несущим полную ответственность за свои решения.

Примечания

1. Русскевич Е. А. Уголовное право и «цифровая преступность»: проблемы и решения. 2-е изд., перераб. и доп. М., 2022.
2. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 N 174-ФЗ // Собрание законодательства РФ. 2001. N 52 (ч. 1). Ст. 4921.
3. Гриненко А. В. Уголовный процесс: учебник для вузов. 10-е изд., перераб. и доп. М., 2025.
4. Тарасов А. В., Темзоков А. Р. Криминалистические аспекты использования искусственного интеллекта в раскрытии и расследовании преступлений // Теория и практика общественного развития. 2023. N 10.
5. Россинская Е. Р. Нейросети в судебной экспертиологии и экспертной практике: проблемы и перспективы // Вестник Университета имени О. Е. Кутафина (МГЮА). 2024. N 3.

English version

Digital traces and artificial intelligence in criminal proceedings: challenges in the transformation of evidence law

Bolshakova Kseniya Borisovna, student, Vladimir State University named after A. G. and N. G. Stoletovs

Gracheva Aleksandra Ivanovna, student, Vladimir State University named after A. G. and N. G. Stoletovs

This article analyzes current issues arising from the integration of digital traces and artificial intelligence technologies into criminal proceedings. It examines the impact of digital data and AI algorithms on traditional institutions of evidence law. The study identifies key challenges related to the collection, verification, and evaluation of digital evidence, as well as the use of outcomes generated by algorithmic systems. The authors propose measures to improve criminal procedure legislation in order to adapt it to the conditions of the digital environment.

Keywords: digital traces, artificial intelligence, criminal procedure, evidence, evidentiary process, admissibility of evidence, digital forensics.