

УДК 343.1; 343.34
МРНТИ 10.77.51

DOI: <https://doi.org/10.37788/2026-2/155-163>

О.С. Коновалов^{1*}, Д.Н. Бекежанов¹

¹Инновационный Евразийский университет, Казахстан

*(e-mail: konovalovo042@gmail.com)

Проблемы допустимости и верификации доказательств, полученных с применением технологий искусственного интеллекта в уголовном процессе: сравнительно-правовое исследование

Аннотация

Основная проблема: Стремительное внедрение искусственного интеллекта в уголовный процесс и массовое распространение технологии «дипфейк» разрушают традиционные парадигмы доказывания. Возникает острая необходимость верификации машинных выводов и защиты правосудия от цифровых фальсификаций, что усугубляется процессуальным отставанием законодательства.

Цель: Формирование комплексного доктринального понимания механизмов верификации и условий допустимости ИИ-доказательств на основе сравнительно-правового анализа зарубежного опыта и оценки законодательных новелл Республики Казахстан.

Методы: В исследовании применялся комплексный подход, включающий сравнительно-правовой (анализ систем США, Великобритании, Германии, ЕС), формально-юридический, формально-логический и системно-структурный методы.

Результаты и их значимость: Выявлен эпистемологический дуализм ИИ-доказательств («заявленные» алгоритмические решения и «незаявленные» дипфейки). Установлено, что зарубежный опыт (EU AI Act, практика США и ЕСПЧ) доказывает острую необходимость жесткого процессуального аудита алгоритмов для предотвращения судебных ошибок (феномен «дивиденд лжеца»). Доказано, что отечественный УПК РК объективно отстает от норм нового Закона РК «Об искусственном интеллекте» и требует адаптации.

Обоснована критическая потребность в модернизации доктринального концепта «специальных научных знаний». Внедрение обязательных механизмов алгоритмического аудита интеллектуальных систем позволит исключить монополию ИИ-разработчиков на установление истины, обеспечив идеальный баланс между технологической эффективностью расследования преступлений и строгим соблюдением конституционных прав граждан.

Ключевые слова: уголовный процесс, искусственный интеллект, свобода оценки доказательств, допустимость доказательств, дипфейки, машинные доказательства, сравнительно-правовое исследование, цифровая криминалистика, прозрачность алгоритмов, верификация данных, Закон об искусственном интеллекте.

Введение

Современная система уголовного правосудия переживает глубокий эпистемологический и парадигмальный сдвиг, обусловленный беспрецедентным внедрением технологий искусственного интеллекта (ИИ) в деятельность органов досудебного расследования, прокуратуры и суда [1]. В последние годы применение интеллектуальных систем перестало быть предметом научной фантастики и превратилось в рутинную правоприменительную практику: от алгоритмов автономного роботизированного патрулирования и предиктивной аналитики мест совершения преступлений до систем биометрической идентификации лиц и автоматизированного анализа колоссальных массивов цифровых следов [2]. Этот технологический скачок открывает широкие горизонты для повышения эффективности раскрытия и расследования уголовных правонарушений, однако он же порождает критические вызовы для устоявшихся принципов уголовно-процессуального права [3].

Проблематика усугубляется взрывным развитием генеративного искусственного интеллекта, который окончательно стер демаркационную линию между объективной физической реальностью и синтетической цифровой фальсификацией. Эпоха, когда фотография, видео- и аудиозапись считались неоспоримым, объективным отражением

действительности, завершилась с массовым распространением технологии «дипфейк» (deepfake) [4]. В мировой судебной практике уже фиксируются прецеденты, когда сторона защиты обоснованно или сугубо спекулятивно ставит под сомнение подлинность ключевых мультимедийных улик, ссылаясь на техническую доступность их искусственной генерации [5].

Целью настоящего исследования является формирование комплексного, научно обоснованного доктринального понимания механизмов верификации и условий допустимости доказательств, полученных с применением ИИ, на основе сравнительно-правового анализа передового зарубежного опыта и критической оценки недавних законодательных новелл Республики Казахстан.

Материалы и методы

Методологическую основу исследования составил комплексный инструментарий, включающий общенаучные и частнонаучные методы познания. Базовым методом выступил сравнительно-правовой подход, позволивший сопоставить концептуальные основы доказательственного права различных правовых семей в условиях цифровизации. В рамках англосаксонской правовой семьи были проанализированы Федеральные правила доказывания США (Federal Rules of Evidence) и новейшие законодательные инициативы отдельных штатов по их адаптации к угрозам дипфейков [6]; прецедентное право, а также аналитические отчеты Правовой комиссии Великобритании (Law Commission) за 2025 год, касающиеся отмены презумпции надежности компьютеров [7].

В рамках романо-германской правовой семьи детальному изучению подверглись положения Уголовно-процессуального кодекса Германии (Strafprozessordnung – StPO) и доктринальные подходы к свободной оценке машинных доказательств [8]. Важным элементом исследования стал формально-юридический анализ наднационального регулирования Европейского Союза, в первую очередь фундаментального Закона ЕС об искусственном интеллекте (EU AI Act) и Директивы о защите данных в правоохранительной сфере (LED) [9].

Особый акцент сделан на отечественной нормативной базе: нормах Уголовно-процессуального кодекса Республики Казахстан (УПК РК) и положениях концептуального Закона РК от 17 ноября 2025 года № 230-VIII «Об искусственном интеллекте». Использование формально-логического и системно-структурного методов позволило выявить нормативные пробелы в действующем законодательстве и смоделировать последствия внедрения алгоритмических систем в механизм доказывания по уголовным делам.

Результаты

1. Эпистемологическая и теоретико-правовая природа доказательств, связанных с искусственным интеллектом. Внедрение искусственного интеллекта в уголовный процесс требует кардинального пересмотра традиционных криминалистических классификаций. Как справедливо отмечается в современной юридической литературе, новейшие интеллектуальные системы представляют собой не просто усовершенствованные технические инструменты фиксации (подобно фотокамере, лупе или диктофону), а выступают в роли квазисубъектов, способных автономно регистрировать, анализировать, коррелировать и интерпретировать многомерные массивы данных [10].

Вопрос о сущности ИИ в криминалистике выходит далеко за рамки технической проблематики. Прежде всего, речь идет о переосмыслении подходов к восприятию и оценке цифровых следов [11]. В американской и европейской уголовно-процессуальной доктрине намечилось четкое разделение ИИ-доказательств на две фундаментальные категории, каждая из которых порождает свой уникальный спектр правовых проблем: «заявленные» (acknowledged) и «незаявленные» (unacknowledged) ИИ-доказательства [12].

Фундаментальная проблема заявленных ИИ-доказательств заключается в доказательстве их валидности и надежности в суде [13]. Понятие валидности (validity) подразумевает, что алгоритм действительно измеряет или предсказывает именно тот феномен, для которого он был концептуально создан (например, алгоритм точно идентифицирует конкретное лицо, а не выдает ложное совпадение из-за особенностей освещения или расовой принадлежности). Понятие надежности (reliability) означает стабильность и воспроизводимость результатов при повторном применении инструмента в схожих условиях [14].

2. Кризис аутентичности: феномен дипфейков и «дивиденд лжеца». Вектор угрозы, исходящий от «незаявленных» ИИ-доказательств, в первую очередь связан с развитием генеративных сетей (GAN). Дипфейки, массово появившиеся в публичном цифровом пространстве около 2017 года, стремительно эволюционировали от сатирических роликов до

мощнейшего криминального инструмента мошенничества, шантажа и целенаправленной фабрикации уголовных улик [10]. Легкость, с которой в настоящее время могут быть созданы сверхреалистичные сфабрикованные видео- и аудиозаписи, наносит колоссальный удар по процессу доказывания.

Как справедливо отмечал судья Верховного суда округа Колумбия Герберт Б. Диксон-младший, из-за внедрения дипфейков, которые спроектированы специально для того, чтобы осуществлять «газлайтинг» наблюдателя, древний постулат «увидеть – значит поверить» может навсегда исчезнуть из нашего правового и культурного этоса.

Процессуальная опасность этого явления носит глубоко двойственный характер. Во-первых, существует очевидный риск неправомерного осуждения невиновных лиц на основании мастерски сфабрикованных улик. Во-вторых, возникает сложный психологический и правовой феномен, получивший в доктрине название «дивиденд лжеца» (liar's dividend) [15]. Суть данного феномена заключается в том, что реально виновный субъект может вполне обоснованно заявить в суде, что подлинная видеозапись совершения им преступления является дипфейком, сгенерированным его недоброжелателями или коррумпированными полицейскими. Учитывая общеизвестность технологии, такое заявление неизбежно зароняет зерно разумного сомнения у судьи или присяжных заседателей. В результате судебные органы сталкиваются с беспрецедентным скептицизмом присяжных в отношении абсолютно любых цифровых доказательств, даже тех, достоверность которых не вызывает сомнений у экспертов.

3. Англосаксонская правовая модель: вызовы и реакция в США и Великобритании

3.1. Подход Соединенных Штатов Америки В правовой системе США допуск доказательств к судебному следствию жестко регламентируется Федеральными правилами доказывания (Federal Rules of Evidence – FRE). Исторически американская модель устанавливала достаточно низкий порог для первоначальной допустимости релевантных доказательств (правила 401 и 402), ограничивая их представление присяжным лишь в том случае, если риск несправедливого предубеждения, путаницы или затягивания процесса существенно перевешивает их доказательственную ценность (правило 403).

Оценка научных экспертных заключений (правило 702) проходит через строгие фильтры прецедентных стандартов Дауберта (Daubert) или Фрая (Frye), требующих доказывания того, что теория или метод были проверены, подвергнуты рецензированию, имеют известный уровень ошибок и общепризнаны в научном сообществе. Однако действующие нормы базовой аутентификации доказательств (правило 901) формировались задолго до появления генеративного ИИ. Согласно классическому правилу 901, для аутентификации документа или видеозаписи стороне достаточно предоставить минимальный объем информации, на основе которой разумное жюри присяжных могло бы сделать логический вывод о том, что предмет с большей долей вероятности является тем, за что его выдают. В эпоху дипфейков этот барьер оказался катастрофически низким.

Помимо борьбы с дипфейками, американские суды пытаются регламентировать и заявленные ИИ-доказательства. В частности, в законодательное собрание штата Нью-Йорк был внесен передовой законопроект, добавляющий параграф § 60.80 в Уголовно-процессуальный закон (CPL). Данная норма содержит жесткое требование: доказательства, созданные с участием ИИ, не могут быть приняты судом в уголовном процессе, если они существенно не подкреплены иными независимыми и допустимыми уликами, а сторона, представляющая их, не установила надежность и точность конкретного способа использования алгоритма.

3.2. Эволюция подходов в Великобритании Правовая система Англии и Уэльса демонстрирует совершенно иную историческую траекторию, которая привела юрисдикцию к одной из крупнейших судебных катастроф современности. Как отмечается в английской доктрине, с 1999 года в уголовном и гражданском судопроизводстве Великобритании действует презумпция общего права, согласно которой компьютер, создавший доказательственную запись, работал исправно в соответствующее время, пока не доказано обратное.

До 1999 года действовала статья 69 Закона о полиции и доказательствах по уголовным делам (PACE), которая жестко требовала от стороны обвинения позитивно доказывать, что компьютер функционировал правильно, прежде чем распечатки признавались допустимыми. Однако Правовая комиссия (Law Commission) рекомендовала отменить эту норму как «громоздкую и непрактичную», опираясь на мнение профессора Колина Таппера, высказанное

в 1991 году, о том, что большинство компьютерных ошибок легко обнаружимы и возникают исключительно из-за неверного ввода данных человеком [16].

Отмена презумпции необходимости независимой проверки систем обернулась делом Post Office / Horizon — величайшей системной судебной ошибкой в истории британского правосудия. Сотни невинных руководителей почтовых отделений были неправомерно осуждены за хищения исключительно на основе данных автоматизированной бухгалтерской системы Horizon. Лишь спустя годы выяснилось, что система содержала критические архитектурные ошибки, которые плодили несуществующие недостатки. Суды годами отказывались верить подсудимым, опираясь на презумпцию исправности машины.

4. Романо-германская правовая модель и наднациональное регулирование Европейского Союза

4.1. Доктрина и практика Германии Германия представляет собой классический, исторически устоявшийся пример смешанного (с преобладанием следственных или инквизиционных элементов) типа уголовного процесса. В отличие от состязательной англо-американской модели, где суд выступает пассивным арбитром, в Германии бремя установления объективной (материальной) истины возложено на самого судью. Уголовно-процессуальный кодекс Германии (Strafprozessordnung – StPO) содержит крайне мало формальных правил априорного исключения доказательств. Допустимость и достоверность улик в немецком суде определяется фундаментальным принципом свободной оценки доказательств (§ 261 StPO), согласно которому суд принимает решение по своему внутреннему убеждению, сформированному на основе всестороннего исследования всего хода судебного разбирательства.

В отношении сбора и изъятия цифровых данных StPO устанавливает строгие материальные и процессуальные гарантии. Так, параграфы 100a и 100b детально регламентируют негласное прослушивание и удаленный доступ к информационно-техническим системам, защищая так называемое «ядро частной жизни» (Kernbereich privater Lebensgestaltung). Правила исключения незаконно полученных доказательств (Beweisverwertungsverbot) в последнее время были дополнительно усилены прецедентами Европейского суда справедливости (ECJ). В частности, суд постановил, что доказательства, собранные государством посредством неизбирательного и массового удержания данных граждан, должны безусловно исключаться из процесса, если обвиняемый не имеет эффективной возможности оспорить их техническую природу.

4.2. Наднациональное регулирование: AI Act Европейского Союза Европейский Союз предпринял самую масштабную в современной истории попытку кодификации правил разработки и эксплуатации ИИ, приняв EU Artificial Intelligence Act (AI Act). Данный беспрецедентный акт базируется на риск-ориентированном подходе. Системы ИИ, используемые правоохранительными органами для оценки достоверности доказательств в ходе расследования, профилирования подозреваемых, прогнозирования преступлений (Predictive Policing) или полиграфирования, жестко классифицируются законом как высокорисковые (high-risk).

Однако с точки зрения защиты прав личности в уголовном процессе AI Act содержит весьма тревожные компромиссы. Статьи 49 и 71 акта устанавливают строгие требования прозрачности, ведения технической документации и регистрационные обязательства для операторов высокорисковых систем. Но для правоохранительных органов эти обязательства существенно смягчены: публичные органы (полиция, спецслужбы) получили законное право скрывать данные о работе алгоритма от общественности и обвиняемых под предлогом оперативной необходимости и защиты тайны следствия.

Как аргументированно отмечают европейские исследователи из Центра ИТ и IP-права (CiTiP) Лёвенского католического университета (KU Leuven), такой подход создает прямую коллизию со статьей 6 Европейской конвенции по правам человека (ЕКПЧ), гарантирующей право на справедливое судебное разбирательство. Право на справедливый суд имплицитно включает право обвиняемого иметь достаточное время и возможности для подготовки защиты (ст. 6(3)(b) ЕКПЧ) и право допрашивать показывающих против него свидетелей (ст. 6(3)(d) ЕКПЧ).

5. Имплементация технологий ИИ в правовую систему Республики Казахстан: текущее состояние и векторы развития Республика Казахстан демонстрирует высокую динамику интеграции в глобальные процессы цифровизации государственного управления и

судопроизводства. Важнейшей вехой в формировании национальной цифровой среды стало принятие Закона Республики Казахстан от 17 ноября 2025 года № 230-VIII «Об искусственном интеллекте». Данный нормативный правовой акт закладывает базовые этические и юридические принципы функционирования ИИ в стране и вводит в юридический оборот критически важную правовую конструкцию — «алгоритмическое решение с юридическим значением», а также закрепляет требования прозрачности применяемых алгоритмов.

Обсуждение

Вместе с тем, как справедливо отмечается в новейшей отечественной правовой литературе, вопросы процессуальной формы, допустимости, верификации и пределов использования доказательств, полученных с использованием ИИ в рамках уголовного судопроизводства, остались за рамками регулирования профильного закона об ИИ. Эти вопросы требуют глубокой, органичной интеграции в ткань Уголовно-процессуального кодекса РК.

Согласно статье 1 УПК РК, порядок уголовного судопроизводства на территории страны определяется Конституцией Республики Казахстан, конституционными законами и Уголовно-процессуальным кодексом. Фундаментальные задачи уголовного процесса (статья 8 УПК РК) предписывают не только быстрое и полное раскрытие преступлений, но и обеспечение надежной защиты граждан от необоснованного обвинения и осуждения, от незаконного ограничения прав и свобод человека. Принцип равенства граждан перед законом (статья 16 УПК РК) исключает любую дискриминацию, в том числе ту, которая может быть алгоритмически заложена в предвзятые системы предиктивной юстиции.

Специфика казахстанского уголовного процесса состоит в том, что применение сложных научно-технических и алгоритмических инструментов правоохранными органами должно проходить строгую, формализованную оценку через институт судебной экспертизы. УПК РК (в частности, статья 114 и смежные нормы) оперирует фундаментальным понятием «специальные научные знания» — это области специальных знаний, содержание которых составляют научные достижения, реализованные в валидированных методиках судебно-экспертного исследования.

В научной доктрине Казахстана и стран СНГ уже активно поднимаются смежные вопросы. Например, в монографии И.Н. Мосечкина (2020 г.) исследуются перспективы уголовной ответственности самого ИИ как нового вида субъекта преступления и пределы невменяемости (соотнесение с разделом 15 УПК РК и ст. 16 УК). Однако для практической криминалистики куда более актуален процессуальный аспект: как оценивать вину и умысел разработчика, оператора или следователя, если алгоритмическая ошибка («галлюцинация» системы распознавания лиц) привела к незаконному аресту или конфискации имущества (ст. 118 УПК РК).

Заключение

Проведенное глубокое сравнительно-правовое исследование со всей очевидностью свидетельствует о том, что интеграция технологий искусственного интеллекта в уголовный процесс является не просто рутинным вопросом внедрения новых эффективных аппаратно-программных комплексов. Это глобальный вызов, требующий фундаментального концептуального переосмысления базовых институтов доказательственного права.

Мировая правоприменительная практика столкнулась с острой дуалистической проблемой. С одной стороны, правоохранным органам жизненно необходимо процессуально легализовать и верифицировать «заявленные» решения легитимных нейросетей, преодолев гносеологическую проблему «черного ящика» и катастрофический дефицит воспроизводимости машинных выводов. С другой стороны — налицо экзистенциальная необходимость выстроить надежные барьеры для защиты самой системы правосудия от «незаявленных» алгоритмических манипуляций в виде дипфейков и синтетических улик, разрушающих вековое доверие общества к объективным визуальным и аудиальным фактам.

Республика Казахстан, сделав значительный, исторически важный шаг вперед путем разработки и принятия профильного Закона «Об искусственном интеллекте» в ноябре 2025 года, заложила прочный этико-правовой и административный фундамент для цифрового рывка. Однако уголовно-процессуальное законодательство (в частности, нормы УПК РК, регламентирующие процесс доказывания и назначения экспертиз) пока объективно отстает от стремительно меняющихся технологических реалий.

Для обеспечения идеального баланса между необходимостью повышения эффективности раскрытия преступлений новыми методами и конституционной обязанностью государства по защите фундаментальных прав и свобод личности, представляется критически важным срочно модернизировать доктринальный и законодательный концепт «специальных научных знаний». Внедрение в отечественную криминалистику обязательных механизмов алгоритмического аудита интеллектуальных систем и создание жестких процессуальных гарантий проверки так называемых «машинных доказательств» позволит исключить опасную монополию разработчиков программного обеспечения на установление истины по уголовным делам. Только гармоничный симбиоз технологической прозрачности (Explainable AI) и неукоснительного соблюдения классических уголовно-процессуальных гарантий позволит национальному и международному правосудию сохранить свою легитимность, авторитет и справедливость в наступающую эпоху искусственного интеллекта.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

- 1 Уголовный процесс, свобода оценки доказательств, искусственный интеллект, цифровизация уголовного судопроизводства // Вестник Академии Права и Управления [Электронный ресурс]. – URL: <https://elibrary.ru/item.asp?id=82462787> (дата обращения: 07.04.2026).
- 2 Singh S. et al. Reliability and Admissibility of AI-Generated Forensic Evidence in Criminal Trials // National Seminar on Criminal Law and Justice Reforms [Electronic resource]. – 2025. – P. 45-53. – URL: <https://arxiv.org/abs/2601.06048> (date of access: 07.04.2026).
- 3 Gless S. AI in the Courtroom: A Comparative Analysis of Machine Evidence in Criminal Trials // Georgetown Journal of International Law [Electronic resource]. – 2020. – Vol. 51. – P. 195-253. – URL: https://ius.unibas.ch/fileadmin/user_upload/ius/09_Upload_Personenprofile/01_Professuren/Gless_Sabine/AI_in_the_courtroom_GT-GJIL2020.pdf (date of access: 07.04.2026).
- 4 Gless S., Silverman E., Weigend T. If Robots Cause Harm, Who Is to Blame? Self-Driving Cars and Criminal Liability // New Criminal Law Review [Electronic resource]. – 2016. – Vol. 19, № 3. – P. 412-436. – URL: <https://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=3206&context=facpubs> (date of access: 07.04.2026).
- 5 Grimm P. W., Grossman M. R., Cormack G. V. Artificial Intelligence as Evidence // Northwestern Journal of Technology and Intellectual Property [Electronic resource]. – 2021. – Vol. 19, № 1. – P. 9-106. – URL: <https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1349&context=njtip> (date of access: 07.04.2026).
- 6 Quezada-Tavárez K., Vogiatzoglou P., Royer S. Artificial Intelligence in Criminal Justice: Fair Trial Challenges // KU Leuven Centre for IT and IP Law [Electronic resource]. – 2021. – URL: <https://lirias.kuleuven.be/retrieve/638528> (date of access: 07.04.2026).
- 7 A Deepfake Evidentiary Rule - Just in Case // UIC Law News [Electronic resource]. – 2024. – URL: <https://library.law.uic.edu/news-stories/a-deepfake-evidentiary-rule-just-in-case/> (date of access: 07.04.2026).
- 8 Delfino R. A Suggestion for Amending Rule 901 regarding Deepfakes // US Courts Publications [Electronic resource]. – 2025. – URL: https://www.uscourts.gov/sites/default/files/2025-04/25-ev-a_suggestion_from_prof.rebecca_delfino_rule_901.pdf (date of access: 07.04.2026).
- 9 Deepfakes in the Courtroom: Problems and Solutions // ISBA Bench Newsletter [Electronic resource]. – 2025. – № 3. – URL: <https://www.isba.org/sections/bench/newsletter/2025/03/deepfakesinthecourtroomproblemsandsolutions> (date of access: 07.04.2026).
- 10 Deepfakes and Evidence Authentication in Courts // Thomson Reuters Institute [Electronic resource]. – 2024. – URL: <https://www.thomsonreuters.com/en-us/posts/ai-in-courts/deepfakes-evidence-authentication/> (date of access: 07.04.2026).
- 11 Imwinkelried E.J. Deepfakes in Court: How Judges Can Proactively Manage Alleged AI-Generated Material // University of Chicago Legal Forum [Electronic resource]. – 2024. – URL: <https://legalforum.uchicago.edu/print-archive/deepfakes-court-how-judges-can-proactively-manage-alleged-ai-generated-material> (date of access: 07.04.2026).
- 12 Мосечкин И.Н. Искусственный интеллект в уголовном праве: перспективы совершенствования охраны и регулирования : монография / И. Н. Мосечкин. – Киров: ВятГУ, 2020. [Электронный ресурс]. – URL: <https://vestnik43.ru/assets/mgr/docs/Монографии/2020/mosechkin-maket-itog.pdf> (дата обращения: 07.04.2026).

- 13 Калиев А. Искусственный интеллект в уголовном процессе Республики Казахстан // Maqsut Narikbayev University [Электронный ресурс]. – URL: <https://km.mnu.kz/pdf/release/7%20статья%20-%20Калиев%20А..pdf> (дата обращения: 07.04.2026).
- 14 EU Artificial Intelligence Act: Law Enforcement Exceptions and Transparency Obligations // Open Research Europe [Electronic resource]. – 2025. – URL: <https://open-research-europe.ec.europa.eu/articles/5-361> (date of access: 07.04.2026).
- 15 The EU AI Act and Criminal Procedure: Protecting Fundamental Rights [Electronic resource]. – 2024. – URL: <https://www.hpnlu.ac.in/PDF/c609c1a4-81ce-47ea-839b-5a5eb3fc2724.pdf> (date of access: 07.04.2026).
- 16 How the AI Act Enhances the Need for EU Regulation on Evidence in Criminal Proceedings // Maastricht Student Law Review [Electronic resource]. – 2024. – URL: <https://www.maastrichtstudentlawreview.com/post/how-the-ai-act-enhances-the-need-for-eu-regulation-on-evidence-in-criminal-proceedings> (date of access: 07.04.2026).
- 17 Adapting the Rules of Evidence for the Age of AI // Quinn Emanuel Publications [Electronic resource]. – URL: <https://www.quinnemanuel.com/the-firm/publications/adapting-the-rules-of-evidence-for-the-age-of-ai/> (date of access: 07.04.2026).

REFERENCES

- 1 Ugolovnyi protsess, svoboda otsenki dokazatelstv, iskusstvennyi intellekt, tsifrovizatsiya ugolovnogo sudoproizvodstva [Criminal process, freedom of evaluation of evidence, artificial intelligence, digitalization of criminal proceedings]. (2023). Vestnik Akademii Prava i Upravleniya. Available at: <https://elibrary.ru/item.asp?id=82462787> (Accessed: 07.04.2026). [in Russian]
- 2 Singh, S. et al. (2025). Reliability and Admissibility of AI-Generated Forensic Evidence in Criminal Trials. National Seminar on Criminal Law and Justice Reforms, 45-53. Available at: <https://arxiv.org/abs/2601.06048> (Accessed: 07.04.2026).
- 3 Gless, S. (2020). AI in the Courtroom: A Comparative Analysis of Machine Evidence in Criminal Trials. Georgetown Journal of International Law, 51, 195-253. Available at: https://ius.unibas.ch/fileadmin/user_upload/ius/09_Upload_Personenprofile/01_Professuren/Gless_Sabine/AI_in_the_courtroom_GT-GJIL2020.pdf (Accessed: 07.04.2026).
- 4 Gless, S., Silverman, E., Weigend, T. (2016). If Robots Cause Harm, Who Is to Blame? Self-Driving Cars and Criminal Liability. New Criminal Law Review, 19(3), 412-436. Available at: <https://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=3206&context=facpubs> (Accessed: 07.04.2026).
- 5 Grimm, P. W., Grossman, M. R., Cormack, G. V. (2021). Artificial Intelligence as Evidence. Northwestern Journal of Technology and Intellectual Property, 19(1), 9-106. Available at: <https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1349&context=njtip> (Accessed: 07.04.2026).
- 6 Quezada-Tavárez, K., Vogiatzoglou, P., Royer, S. (2021). Artificial Intelligence in Criminal Justice: Fair Trial Challenges. KU Leuven Centre for IT and IP Law. Available at: <https://lirias.kuleuven.be/retrieve/638528> (Accessed: 07.04.2026).
- 7 A Deepfake Evidentiary Rule - Just in Case. (2024). UIC Law News. Available at: <https://library.law.uic.edu/news-stories/a-deepfake-evidentiary-rule-just-in-case/> (Accessed: 07.04.2026).
- 8 Delfino, R. (2025). A Suggestion for Amending Rule 901 regarding Deepfakes. US Courts Publications. Available at: https://www.uscourts.gov/sites/default/files/2025-04/25-ev-a_suggestion_from_prof.rebecca_delfino-_rule_901.pdf (Accessed: 07.04.2026).
- 8 Deepfakes in the Courtroom: Problems and Solutions. (2025). ISBA Bench Newsletter, (3). Available at: <https://www.isba.org/sections/bench/newsletter/2025/03/deepfakesinthecourtroomproblemsandsolutions> (Accessed: 07.04.2026).
- 9 Deepfakes and Evidence Authentication in Courts. (2024). Thomson Reuters Institute. Available at: <https://www.thomsonreuters.com/en-us/posts/ai-in-courts/deepfakes-evidence-authentication/> (Accessed: 07.04.2026).
- 10 Imwinkelried, E. J. (2024). Deepfakes in Court: How Judges Can Proactively Manage Alleged AI-Generated Material. University of Chicago Legal Forum. Available at: <https://legal->

forum.uchicago.edu/print-archive/deepfakes-court-how-judges-can-proactively-manage-alleged-ai-generated-material (Accessed: 07.04.2026).

11 Mosechkin, I.N. (2020). *Iskusstvennyi intellekt v ugovnom prave: perspektivy sovershenstvovaniya okhrany i regulirovaniya* [Artificial intelligence in criminal law: prospects for improving protection and regulation]. Kirov: VyatGU. Available at: <https://vestnik43.ru/assets/mgr/docs/Монографии/2020/mosechkin-maket-itog.pdf> (Accessed: 07.04.2026). [in Russian]

12 Kaliev, A. (2024). *Iskusstvennyi intellekt v ugovnom protsesse Respubliki Kazakhstan* [Artificial intelligence in the criminal process of the Republic of Kazakhstan]. Maqsut Narikbayev University. Available at: <https://km.mnu.kz/pdf/release/7%20статья%20-%20Калиев%20А..pdf> (Accessed: 07.04.2026). [in Russian]

13 EU Artificial Intelligence Act: Law Enforcement Exceptions and Transparency Obligations. (2025). Open Research Europe. Available at: <https://open-research-europe.ec.europa.eu/articles/5-361> (Accessed: 07.04.2026).

14 The EU AI Act and Criminal Procedure: Protecting Fundamental Rights. (2024). Available at: <https://www.hpnlu.ac.in/PDF/c609c1a4-81ce-47ea-839b-5a5eb3fc2724.pdf> (Accessed: 07.04.2026).

15 How the AI Act Enhances the Need for EU Regulation on Evidence in Criminal Proceedings. (2024). Maastricht Student Law Review. Available at: <https://www.maastrichtstudentlawreview.com/post/how-the-ai-act-enhances-the-need-for-eu-regulation-on-evidence-in-criminal-proceedings> (Accessed: 07.04.2026).

16 Adapting the Rules of Evidence for the Age of AI. Quinn Emanuel Publications. Available at: <https://www.quinnemanuel.com/the-firm/publications/adapting-the-rules-of-evidence-for-the-age-of-ai/> (Accessed: 07.04.2026).

О.С. Коновалов¹, Д.Н. Бекежанов¹

¹Инновациялық Еуразиялық университеті, Қазақстан

Қылмыстық процесте жасанды интеллект технологияларын қолдану арқылы алынған дәлелдемелердің жарамдылығы мен верификациясы мәселелері: салыстырмалы-құқықтық зерттеу

Жасанды интеллектіні қылмыстық процеске қарқынды енгізу және «дипфейк» технологиясының жаппай таралуы дәлелдеудің дәстүрлі парадигмаларын бұзады. Машиналық тұжырымдарды верификациялау және сот төрелігін цифрлық қолдан жасаудан қорғаудың өткір қажеттілігі туындайды, бұл заңнаманың процестік тұрғыдан артта қалуымен ушыға түседі.

Шетелдік тәжірибені салыстырмалы-құқықтық талдау және Қазақстан Республикасының заңнамалық жаңашылдықтарын бағалау негізінде ЖИ-дәлелдемелерін верификациялау тетіктері мен рұқсат етілу шарттарын кешенді доктриналық түсінуді қалыптастыру.

Зерттеуде салыстырмалы-құқықтық (АҚШ, Ұлыбритания, Германия, ЕО жүйелерін талдау), формальды-заңдық, формальды-логикалық және жүйелі-құрылымдық әдістерді қамтитын кешенді тәсіл қолданылды.

ЖИ-дәлелдемелерінің эпистемологиялық дуализмі («мәлімделген» алгоритмдік шешімдер және «мәлімделмеген» дипфейктер) анықталды. Шетелдік тәжірибе (ЕУ AI Акт, АҚШ пен АҚЕС практикасы) сот қателіктерін («өтірікші дивиденді» феномені) болдырмау үшін алгоритмдерге қатаң процестік аудит жүргізудің өткір қажеттілігін дәлелдейтіні анықталды. Отандық ҚР ҚДЖК жаңа «Жасанды интеллект туралы» ҚР Заңының нормаларынан объективті түрде артта қалатыны және бейімдеуді қажет ететіні дәлелденді.

«Арнайы ғылыми білім» доктриналық тұжырымдамасын жаңғыртудың сыни қажеттілігі негізделді. Зияткерлік жүйелерге алгоритмдік аудит жүргізудің міндетті тетіктерін енгізу қылмыстарды тергеп-тексерудің технологиялық тиімділігі мен азаматтардың конституциялық құқықтарын қатаң сақтау арасындағы мінсіз теңгерімді қамтамасыз ете отырып, ЖИ-әзірлеушілердің ақиқатты анықтаудағы монополиясын жоюға мүмкіндік береді.

Түйінді сөздер: қылмыстық процесс, жасанды интеллект, дәлелдемелерді бағалау еркіндігі, дәлелдемелердің жарамдылығы, дипфейктер, машиналық дәлелдемелер,

салыстырмалы-құқықтық зерттеу, цифрлық криминалистика, алгоритмдердің ашықтығы, деректерді верификациялау, Жасанды интеллект туралы заң.

O.S. Konovalov¹, D.N. Bekezhanov¹

¹Innovative University of Eurasia, Kazakhstan

Problems of admissibility and verification of evidence obtained using artificial intelligence technologies in criminal proceedings: a comparative legal study

The rapid introduction of artificial intelligence into the criminal process and the mass proliferation of "deepfake" technology are destroying traditional paradigms of proof. There is an acute need to verify machine conclusions and protect justice from digital falsifications, which is exacerbated by the procedural lag of legislation.

The formation of a comprehensive doctrinal understanding of the mechanisms of verification and the conditions for the admissibility of AI evidence based on a comparative legal analysis of foreign experience and an assessment of the legislative novelties of the Republic of Kazakhstan.

The study applied a comprehensive approach, including comparative-legal (analysis of the systems of the USA, UK, Germany, EU), formal-legal, formal-logical, and systemic-structural methods.

The epistemological dualism of AI evidence ("acknowledged" algorithmic decisions and "unacknowledged" deepfakes) was revealed. It has been established that foreign experience (EU AI Act, US and ECtHR practice) proves the acute need for a strict procedural audit of algorithms to prevent miscarriages of justice (the "liar's dividend" phenomenon). It is proven that the domestic Criminal Procedure Code of the RK objectively lags behind the norms of the new Law of the RK "On Artificial Intelligence" and requires adaptation.

The critical need to modernize the doctrinal concept of "special scientific knowledge" is substantiated. The introduction of mandatory mechanisms for the algorithmic audit of intellectual systems will make it possible to eliminate the monopoly of AI developers on establishing the truth, ensuring an ideal balance between the technological efficiency of investigating crimes and strict compliance with the constitutional rights of citizens.

Keywords: criminal proceedings, artificial intelligence, freedom of evidence evaluation, admissibility of evidence, deepfakes, machine evidence, comparative legal study, digital forensics, algorithmic transparency, data verification, Artificial Intelligence Act.

Дата поступления рукописи в редакцию: 07.04.2026 г.