

АКИМОВ Сергей Владимирович,
Старший научный сотрудник НИЦ № 3 ВНИИ МВД
России, подполковник полиции,
e-mail: yan.sahatoff@gmail.com

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И БИОМЕТРИЧЕСКИЕ ТЕХНОЛОГИИ В РОЗЫСКЕ ЛИЦ, СКРЫВАЮЩИХСЯ ОТ ОРГАНОВ ПРЕДВАРИТЕЛЬНОГО РАССЛЕДОВАНИЯ И СУДА

Аннотация. Настоящая статья посвящена исследованию возможностей, пределов и правовых условий применения технологий искусственного интеллекта и биометрической идентификации в деятельности по розыску лиц, скрывающихся от органов предварительного расследования и суда. В статье отмечено, что с ростом мобильности населения, цифровизацией коммуникаций, распространением трансграничной преступности и увеличением объема разнородной информации, подлежащей анализу правоохранительными органами, традиционные способы розыска, основанные преимущественно на оперативной проверке адресов, опросах, ориентировках и межведомственном обмене сведениями, сохраняют значение, однако недостаточно эффективны при обработке больших массивов цифровых данных. Искусственный интеллект способен автоматизировать поиск закономерностей, ранжировать розыскные версии, сопоставлять сведения из ведомственных баз данных, выявлять связи между лицами, событиями, транспортными средствами и геолокационными данными. Биометрические технологии, включающие распознавание лица, дактилоскопическую идентификацию, анализ голоса, радужной оболочки глаза и иных устойчивых физиологических признаков, создают основу для установления личности разыскиваемого лица в условиях изменения им внешности, документов либо места пребывания. Вместе с тем их применение связано с рисками ошибочной идентификации, дискриминационных алгоритмических решений, неправомерного вмешательства в частную жизнь и расширения практик массового наблюдения. Обосновывается вывод о том, что результаты работы интеллектуальных и биометрических систем должны иметь ориентирующее, а не предрешающее доказательственное значение. Эффективное внедрение рассматриваемых технологий требует нормативной определенности, человеческого контроля, аудита алгоритмов, защиты персональных данных и процессуальной проверяемости получаемой информации.

Ключевые слова: искусственный интеллект, биометрия, розыск, идентификация личности, предварительное расследование, судебное производство, персональные данные, распознавание лица, цифровые доказательства, алгоритмический контроль.

AKIMOV Sergey Vladimirovich,
Senior researcher of the Research Center No. 3 of
the All-Russian Research Institute of the Ministry of
Internal Affairs of Russia, police lieutenant colonel

ARTIFICIAL INTELLIGENCE AND BIOMETRIC TECHNOLOGIES IN THE SEARCH FOR PERSONS HIDING FROM PRELIMINARY INVESTIGATION AUTHORITIES AND THE COURT

Annotation. This article explores the potential, limits, and legal conditions for using artificial intelligence and biometric identification technologies in the search for individuals absconding from pretrial investigation and prosecution authorities. The article notes that with the increasing mobility of the population, the digitalization of communications, the spread of cross-border crime, and the growing volume of heterogeneous information that must be analyzed by law enforcement agencies, traditional search methods based primarily on prompt address verification, interviews, alerts, and interagency information exchange remain valuable,

but are insufficiently effective when processing large amounts of digital data. Artificial intelligence can automate the search for patterns, rank search leads, compare information from departmental databases, and identify connections between individuals, events, vehicles, and geolocation data. Biometric technologies, including facial recognition, fingerprint identification, voice analysis, iris analysis, and other stable physiological characteristics, provide the basis for establishing the identity of a wanted person even if their appearance, documents, or location changes. However, their use is associated with risks of misidentification, discriminatory algorithmic decisions, unlawful interference with privacy, and the expansion of mass surveillance practices. It is concluded that the results of intelligent and biometric systems should have indicative, rather than prejudicial, evidentiary value. Effective implementation of these technologies requires regulatory certainty, human oversight, algorithm auditing, personal data protection, and procedural verifiability of the information obtained.

Key words: artificial intelligence, biometrics, search, personal identification, preliminary investigation, legal proceedings, personal data, facial recognition, digital evidence, algorithmic control.

Розыск лиц, скрывающихся от органов предварительного расследования и суда, представляет собой одно из важных направлений правоохранительной деятельности. Его эффективность непосредственно влияет на реализацию принципа неотвратимости уголовной ответственности, соблюдение разумных сроков уголовного судопроизводства, обеспечение прав потерпевших, а также на возможность исполнения судебных решений. Лицо, уклоняющееся от следствия или суда, как правило, предпринимает меры к сокрытию своего местонахождения: изменяет внешность, использует чужие либо поддельные документы, меняет номера телефонов, ограничивает контакты с родственниками, перемещается между регионами и государствами.

В этих условиях возрастают возможности цифровых технологий. Современная информационная среда формирует значительный массив данных о перемещениях, коммуникациях, финансовых операциях и визуальном образе человека. Системы видеонаблюдения, государственные информационные ресурсы, базы дактилоскопического учёта, сведения о пересечении границы, цифровые следы в телекоммуникационных сетях и открытых источниках способны существенно расширить поисковые возможности правоохранительных органов. Однако получение полезной информации из таких массивов невозможно без автоматизированной аналитики и механизмов быстрого сопоставления данных.

Искусственный интеллект в правоохранительной сфере следует рассматривать не как самостоятельного субъекта принятия решения, а как комплекс технологий обработки данных, прогнозирования, классификации, распознавания образов и поиска статистических взаимосвязей. Его использование в розыске предполагает автоматизацию рутинных операций, сокращение времени анализа информации и повышение вероятности обнаружения значимых связей, которые трудно установить исключительно традиционными средствами.

В российской правовой политике развитие

искусственного интеллекта связывается с необходимостью сочетать технологическое развитие с обеспечением безопасности и защитой прав граждан. Концепция развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники ориентирована на формирование условий для безопасного и ответственного применения соответствующих технологий, включая работу с данными при соблюдении интересов субъектов персональных данных. Вместе с тем внедрение подобных решений в уголовно-процессуальную и оперативно-розыскную практику требует особой осторожности, поскольку последствия ошибочного алгоритмического вывода могут затрагивать конституционные права личности [2].

Биометрическая идентификация основывается на сравнении уникальных физиологических либо поведенческих характеристик человека с эталонными данными. Для розыскной деятельности наибольшее значение имеют следующие виды биометрии:

- дактилоскопическая идентификация по отпечаткам пальцев и ладоней;
- распознавание лица по фотографии, видеозаписи или кадрам камер наблюдения;
- идентификация по радужной оболочке глаза;
- распознавание голоса;
- анализ походки, динамики движений и иных поведенческих характеристик;
- сопоставление профилей ДНК при наличии предусмотренных законом оснований [1].

Наиболее распространённой является технология распознавания лиц. Она предполагает преобразование изображения лица в цифровой шаблон, включающий набор математически описываемых признаков, после чего этот шаблон сопоставляется с массивом ранее сформированных биометрических образцов. Результатом работы системы обычно является не категорический вывод о тождестве лиц, а перечень наиболее вероятных совпадений. Следовательно, алгоритм создаёт основание для дальнейшей проверки, но

не заменяет процессуально значимую процедуру установления личности.

Международная практика демонстрирует востребованность таких механизмов. Система распознавания лиц Интерпола формирует список кандидатов путём алгоритмического сравнения введённого изображения с биометрическими шаблонами, содержащимися в международной базе данных. При этом окончательное решение предполагает последующую оценку полученного совпадения компетентными специалистами. Биометрический центр Интерпола объединяет возможности поиска по отпечаткам пальцев, изображениям лиц и иным биометрическим данным; система была введена в эксплуатацию в октябре 2023 года и рассчитана на проведение до одного миллиона криминалистических поисковых запросов в сутки [5].

Для российской практики особое значение имеет интеграция различных учётов и информационных ресурсов. Эффективность биометрического поиска возрастает, если изображение, отпечаток либо иной идентификатор сопоставляется не с изолированной базой, а с совокупностью данных о гражданах, подозреваемых, обвиняемых, осуждённых, лицах без вести пропавших, неопознанных трупах, пересечении государственной границы, регистрации транспортных средств и иных юридически значимых обстоятельствах.

Искусственный интеллект может применяться в розыске по нескольким направлениям [4].

Во-первых, он позволяет автоматически обрабатывать большие объёмы визуальной информации. При наличии законных оснований система способна выделять из видеопотока изображения, схожие с биометрическим шаблоном разыскиваемого лица, фиксировать место и время предполагаемого обнаружения, а также передавать информацию сотруднику для проверки.

Во-вторых, интеллектуальные методы применимы для выявления связей между людьми, событиями и объектами. Анализ телефонных соединений, данных о маршрутах, финансовых операциях, цифровых профилях и контактах может указывать на лиц, способных поддерживать разыскиваемого, предоставлять ему жильё, денежные средства или средства связи. При этом сам факт статистической связи не означает участия лица в преступлении и не может подменять доказывание.

В-третьих, алгоритмы могут использоваться для приоритизации розыскных мероприятий. Например, система способна ранжировать версии о возможном местонахождении лица по степени соответствия имеющимся сведениям: наличию родственников в определённом регионе, преж-

ним адресам, частоте контактов, данным о поездках или использовании банковских продуктов, что позволяет рациональнее распределять ресурсы, но не освобождает должностное лицо от обязанности самостоятельно оценивать фактические данные.

В-четвертых, искусственный интеллект применим в анализе неструктурированных документов. Большие массивы протоколов, ориентировок, судебных актов, сообщений граждан и иных текстовых материалов могут обрабатываться средствами семантического поиска. Такая технология помогает выявлять повторяющиеся адреса, псевдонимы, номера документов, транспортные средства, географические точки и связанные уголовные производства.

Следственный комитет Российской Федерации заявлял о намерении развивать нейросетевые инструменты и биометрическую идентификацию при розыске лиц, скрывающихся от следствия, в том числе через подключение к базам МВД России. Данное направление отражает общий переход от фрагментарного использования цифровых ресурсов к построению более взаимосвязанной аналитической инфраструктуры [6].

Применение биометрических технологий связано с обработкой персональных данных повышенной чувствительности. Биометрические персональные данные позволяют установить личность человека на основе его физиологических или биологических особенностей, вследствие чего их сбор, хранение, передача и использование требуют специальных организационных и правовых гарантий.

Федеральный закон от 29 декабря 2022 года № 572-ФЗ регулирует отношения, связанные с идентификацией и аутентификацией физических лиц с использованием биометрических персональных данных, а также функционирование соответствующей государственной информационной системы [7]. Однако механизмы биометрической идентификации в сфере публичной безопасности и уголовного преследования должны оцениваться не только через призму законодательства о персональных данных, но и с учётом норм уголовно-процессуального законодательства, законодательства об оперативно-розыскной деятельности, конституционных гарантий неприкосновенности частной жизни и принципа соразмерности ограничений прав личности.

Правовая допустимость применения искусственного интеллекта в розыске предполагает соблюдение ряда условий:

наличие нормативного основания для получения и обработки конкретной категории сведений;

определённость целей обработки данных и запрет их использования вне пределов постав-

ленной розыскной задачи;

соразмерность применяемого средства степени общественной опасности расследуемого деяния и характеру имеющихся оснований для розыска;

ограничение круга должностных лиц, имеющих доступ к биометрическим и аналитическим системам;

документирование действий по формированию запроса, получению результата и его последующей проверке;

обеспечение информационной безопасности, предотвращение утечек и несанкционированного доступа;

возможность ведомственного, прокурорского, судебного и общественного контроля в пределах, совместимых с охраняемой законом тайной [3].

Особое значение имеет различие между ориентирующей и доказательственной информацией. Результат автоматического сопоставления изображения с базой данных не должен автоматически признаваться доказательством тождества личности. Алгоритм может ошибиться из-за низкого качества изображения, недостаточного освещения, изменения ракурса, возрастных изменений внешности, ношения головного убора, маски, очков или намеренного изменения внешности. Поэтому совпадение, установленное программным комплексом, требует подтверждения посредством процессуальных действий: предъявления для опознания при соблюдении установленных требований, экспертного исследования, проверки документов, допросов, осмотра, получения образцов для сравнительного исследования и иных предусмотренных законом процедур.

Следует также разграничивать идентификацию и аутентификацию. Идентификация отвечает на вопрос о том, кем является неизвестное лицо, сопоставляя его признаки с множеством записей. Аутентификация подтверждает, соответствует ли предъявляемый человек уже заявленной личности. В розыскной деятельности преимущественно используется идентификационный подход, поскольку задача состоит в обнаружении лица, местонахождение которого неизвестно или которое использует иную персональную информацию.

Оптимальная модель использования искусственного интеллекта и биометрических технологий в розыске должна строиться на принципе «человек принимает решение, технология помогает его обосновать». Алгоритм может быстро обработать информацию и сформировать перечень вероятных совпадений, но юридически значимая оценка должна производиться сотрудником, обладающим соответствующими полномочиями и несущим ответственность за принятое решение.

Представляется целесообразным закрепить

многоступенчатый порядок использования биометрического поиска. На первом этапе формируется законный запрос, содержащий сведения о разыскиваемом лице и основание для проведения розыскного мероприятия. На втором этапе система выполняет автоматизированное сопоставление и формирует список вероятных кандидатов. На третьем этапе сотрудник оценивает качество исходных данных, вероятность совпадения и наличие иных подтверждающих сведений. На четвертом этапе проводится проверка через процессуальные или оперативно-розыскные средства. На пятом этапе результаты проверки документируются и при необходимости получают надлежащую процессуальную форму.

Для обеспечения законности представляется необходимым внедрение следующих механизмов:

обязательная валидация используемых алгоритмов на репрезентативных наборах данных;

периодическая оценка точности, числа ложных совпадений и причин технических ошибок;

независимый аудит программных решений, применяемых в наиболее чувствительных сферах;

закрепление регламентов участия человека в принятии решений;

ведение журналов обращений к биометрическим базам данных;

установление сроков хранения полученной информации и процедур её уничтожения при отсутствии законных оснований;

подготовка сотрудников, способных критически оценивать результаты автоматизированного анализа;

разработка процессуальных правил проверки и использования сведений, полученных с применением искусственного интеллекта.

Таким образом, искусственный интеллект и биометрические технологии способны существенно повысить результативность розыска лиц, скрывающихся от органов предварительного расследования и суда. Их основное преимущество заключается в ускорении поиска по крупным массивам данных, автоматизации сравнения биометрических признаков, выявлении связей и формировании обоснованных версий о возможном местонахождении разыскиваемого лица.

Вместе с тем технологическая эффективность не может рассматриваться как самостоятельная ценность, превосходящая требования законности, необходимости и соразмерности. Биометрическое совпадение и алгоритмический прогноз должны служить ориентиром для дальнейшей проверки, но не подменять процессуальные гарантии и оценку доказательств уполномоченным лицом.

Дальнейшее развитие данного направления

требует специальной нормативной регламентации, единых стандартов качества алгоритмов, технической защищённости баз данных, прозрачности процедур и постоянного контроля со стороны компетентных органов.

Список литературы:

[1] Кузнецова С.С., Мочалов А.Н. Цифровые следы человека, цифровое профилирование и скоринг: правовое регулирование в России и за рубежом. – Екатеринбург: Издательство УМЦ УПИ, 2025. – 300 с.

[2] Кутейников Д. Л., Ижаев О. А., Лебедев В. А., Зенин С. С. Неприкосновенность частной жизни в условиях использования систем искусственного интеллекта для удаленной биометрической идентификации личности // Lex russica. — 2022. — Т. 75, № 2. — С. 121 – 131.

[3] Надежина И.В., Пшеничных С.Н. Использование возможностей искусственного интеллекта по розыску лиц // Вестник экономики, права и социологии. - 2025. - № 3. - С. 367 – 371.

[4] Хамидуллин Р. С. Криминалистическое обеспечение использования технологии искусственного интеллекта в раскрытии и расследовании преступлений // Электронное приложение к «Российскому юридическому журналу». - 2024. - № 2. - С. 19 – 29.

[5] Биометрический центр Интерпола [Электронный ресурс]/ INTERPOL : официальный сайт. — URL: <https://www.interpol.int/How-we-work/Forensics/Biometric-Hub> (дата обращения: 21.08.2026).

[6] Бастрыкин: в процесс розыска скрывшихся от следствия лиц внедряют нейросеть [Электронный ресурс]. Тасс, 2025. - URL: <https://tass.ru/obschestvo/22880321> (дата обращения: 21.08.2026).

[7] Федеральный закон от 29.12.2022 г. № 572-ФЗ [Электронный ресурс] // Официальный сайт Президента Российской Федерации. - URL: <http://www.kremlin.ru/acts/bank/48740> (дата обращения: 21.08.2026).

References:

[1] Kuznetsova S.S., Mochalov A.N. Digital human traces, digital profiling and scoring: legal regulation in Russia and abroad. - Yekaterinburg: Publishing House UMC UPI, 2025. - 300 s.

[2] Kuteinikov D. L., Izhaev O. A., Lebedev V. A., Zenin S. S. Privacy in the conditions of using artificial intelligence systems for remote biometric personality identification // Lex russica. — 2022. - T. 75, NO. 2. - S. 121-131.

[3] Nadezhina I.V., Pshenichnykh S.N. Using the capabilities of artificial intelligence to search for persons // Bulletin of Economics, Law and Sociology. - 2025. - № 3. - S. 367-371.

[4] Khamidullin R. S. Forensic support for the use of artificial intelligence technology in the disclosure and investigation of crimes // Electronic Appendix to the Russian Legal Journal. - 2024. - № 2. - S. 19-29.

[5] Interpol Biometric Center [Electronic Resource]/INTERPOL: official website. — URL: <https://www.interpol.int/How-we-work/Forensics/Biometric-Hub> (дата обращения: 21.08.2026).

[6] Bastrykin: a neural network [Electronic resource] will be introduced into the process of searching for persons hiding from the investigation. Tass, 2025. - URL: <https://tass.ru/obschestvo/22880321> (access date: 21.08.2026).

[7] Federal Law of 29.12.2022 No. 572-FZ [Electronic Resource] // Official Website of the President of the Russian Federation. - URL: <http://www.kremlin.ru/acts/bank/48740> (access date: 21.08.2026).