

УДК 342.95:004.93'1
МРНТИ 10.19.00

DOI: <https://doi.org/10.37788/2026-2/149--154>

С.С. Каримова^{1*}

¹Учебный центр МВД РК, Казахстан

*(e-mail: saltanat_karimova01@mail.ru)

**Использование систем распознавания лиц административной полицией:
обеспечение баланса между общественной безопасностью и правом на частную жизнь**

Аннотация

Основная проблема: Стремительное внедрение технологий алгоритмического распознавания лиц (FRT) в деятельность административной полиции порождает глубокий институциональный дисбаланс. Формирование инфраструктуры тотального видеонаблюдения создает прямую угрозу конституционным правам граждан на неприкосновенность частной жизни и свободу передвижения, усугубляемую отсутствием четкого профильного законодательства и рисками машинной предвзятости.

Цель: Комплексный концептуальный анализ существующих правовых моделей применения биометрических технологий полицией для выработки научно обоснованных рекомендаций по достижению баланса между общественной безопасностью и информационной автономией личности.

Методы: В исследовании применен комплексный подход, включающий системный, формально-догматический и сравнительно-правовой (ЕС, США, Великобритания, РК) методы. Особый акцент сделан на анализе прецедентной практики ЕСПЧ (дело Glukhin v. Russia) и актуальной эмпирической статистики МВД РК за 2024–2025 годы.

Результаты и их значимость: Признана высокая криминалистическая эффективность FRT. Однако установлено, что в Казахстане применение систем распознавания регламентируется преимущественно подзаконными актами, что предоставляет силовым структурам чрезмерную дискрецию. Неизбирательное биометрическое сканирование населения де-факто стирает презумпцию невиновности.

Обоснована критическая необходимость реформирования национального законодательства путем имплементации международных риск-ориентированных стандартов (EU AI Act) и принципов ЕСПЧ (extrema ratio). Предложены конкретные шаги: обязательное судебное санкционирование алгоритмического розыска, закрепление исчерпывающего перечня преступлений для использования FRT и создание института независимого аудита Искусственный Интеллект.

Ключевые слова: распознавание лиц, административная полиция, общественная безопасность, право на частную жизнь, биометрические персональные данные, видеонаблюдение, права человека, искусственный интеллект, прецедентная практика, информационная автономия, Республика Казахстан.

Введение

Стремительное развитие технологий на стыке XX и XXI веков привело к фундаментальному и необратимому пересмотру подходов к осуществлению административно-полицейских функций. Взрывной рост IT-сферы бросает серьезный вызов классическим правовым институтам, вынуждая государство и общество непрерывно подстраиваться под новые технологические реалии. В богатом арсенале современных правоохранительных структур наиболее перспективным, но в то же время дискуссионным инструментом выступают алгоритмы распознавания лиц (Facial Recognition Technology – FRT), базирующиеся на технологиях искусственного интеллекта (ИИ) и глубоком машинном обучении.

Если рассматривать историческую ретроспективу, методы криминалистической идентификации эволюционировали от антропометрических измерений и дактилоскопии до высокоточного анализа ДНК. Тем не менее внедрение FRT знаменует собой переход на совершенно иной уровень. Этот формат алгоритмического контроля способен функционировать в плотном потоке людей, демонстрируя скорость и точность, многократно

превосходящие возможности человеческого восприятия. Для современной концепции «безопасного города» способность вычислительных мощностей мгновенно выявлять разыскиваемых лиц и пресекать правонарушения на этапе покушения стала критически важной. Тенденция к масштабированию таких интеллектуальных систем в целях охраны правопорядка будет только усиливаться.

Вместе с тем, тотальное внедрение «умных» камер в полицейскую практику генерирует пласт сложнейших социальных, правовых и этических дилемм. Перед мировой юстицией встает проблема защиты от формирования инфраструктуры абсолютного алгоритмического контроля. Наделяя административную полицию инструментами для непрерывной и автоматизированной обработки чувствительных биометрических данных неограниченного числа граждан, государство создает прямую угрозу конституционным правам: свободе передвижения, неприкосновенности частной жизни и свободе выражения мнений.

На глобальном уровне регулирование биометрических инноваций характеризуется крайней нестабильностью и фрагментарностью, граничащей с правовым вакуумом. Отсутствие единого подхода приводит к полярным решениям: от строгих запретов на использование FRT полицией в некоторых американских штатах до формирования тотальных государственных биометрических реестров в других юрисдикциях. Возникает острая потребность в академическом осмыслении механизмов сдержек и противовесов, способных сбалансировать публичный запрос на безопасность и персональное право на информационную независимость.

Ситуация осложняется феноменом «черного ящика» ИИ. Нейросети, натренированные на гигантских массивах данных, склонны перенимать и масштабировать скрытые социальные предубеждения, что повышает риск дискриминационного профилирования. В связи с этим разработка строгих регламентов, повышение стандартов доказывания соразмерности вмешательства и учреждение институтов независимого аудита алгоритмов становятся ключевыми задачами для правовой науки.

Данная работа посвящена всестороннему концептуальному анализу существующих парадигм применения FRT. Центральная гипотеза сводится к следующему: использование биометрических решений административной полицией может считаться легитимным и соответствующим международным правозащитным стандартам исключительно при соблюдении принципов *ultima ratio* (крайней необходимости), точечной обоснованности и при наличии многоуровневого независимого контроля.

Материалы и методы

Сложность, многомерность и междисциплинарный характер темы потребовали использования комплексного методологического аппарата, синтезирующего подходы юридической, технической и социологической наук. Исследование феноменов, находящихся на стыке IT и юриспруденции, обусловило применение широкого набора научных инструментов.

Фундаментальным общенаучным методом стал системный анализ. Он позволил исследовать внедрение FRT в полицейскую деятельность не просто как процесс технической модернизации, а как масштабный социально-правовой сдвиг, меняющий саму природу взаимодействия государственного аппарата принуждения и личности. Логико-дедуктивный метод применялся для формулирования выводов о влиянии цифровизации на правовую доктрину.

Для скрупулезного анализа нормативной базы использовался формально-догматический (юридико-технический) инструментарий. С его помощью были детально исследованы: Директива ЕС (LED), Регламент ЕС об искусственном интеллекте (EU AI Act), положения Конституции РК, а также национальные законы, регламентирующие работу с биометрией (включая Закон РК «О персональных данных и их защите» и нормы КоАП РК).

Учитывая глобальный характер развития ИИ, важнейшую роль сыграл сравнительно-правовой (компаративистский) метод. Сопоставление правоприменительных и регуляторных стратегий ЕС, США, Великобритании и Казахстана дало возможность выявить национальную специфику правовой адаптации к цифровым угрозам.

Существенный акцент сделан на методе анализа судебных прецедентов, в первую очередь – знаковых постановлений Европейского суда по правам человека (ЕСПЧ), касающихся пределов электронного наблюдения. Особое внимание уделено историческому решению по делу *Glukhin v. Russia*.

Эмпирический фундамент работы опирается на актуальную статистику МВД РК по раскрываемости преступлений, а также на отчетные данные о работе Национальной системы видеомониторинга (НСВМ) и аппаратно-программных комплексов в 2024–2025 годах.

Результаты

Технико-правовая природа систем распознавания лиц в полицейском контексте. Разработка качественного правового регулирования невозможна без понимания технической специфики объекта. Технология FRT работает путем обработки визуальной информации для алгоритмического подтверждения или установления личности. Базовый цикл включает: фиксацию лица в видеопотоке, пространственное выравнивание и захват узловых точек, после чего программа трансформирует эти данные в уникальный математический «шаблон» (вектор).

Далее этот вектор мгновенно сопоставляется с обширными базами данных, источниками которых выступают государственные реестры, криминалистические учеты, а в последнее время – открытые профили граждан в социальных сетях.

С точки зрения полицейской практики, выделяют три операционных режима FRT:

Верификация (1:1) – подтверждение личности конкретного человека.

Идентификация (1:N) – поиск неустановленного лица в базе данных путем сканирования толпы.

Категоризация – алгоритмический анализ демографии или эмоционального фона.

Для административной полиции ключевым является режим идентификации (1:N) в публичных местах. Он позволяет оперативно находить преступников и предотвращать угрозы. Однако переход к такой предиктивной (превентивной) модели контроля несет колоссальные риски. Технические искажения алгоритмов часто провоцируют ложноположительные срабатывания (False Positives), что на практике оборачивается незаконными задержаниями и грубым нарушением прав граждан.

Международный и зарубежный опыт правового регулирования. Европейский Союз демонстрирует наиболее проработанную парадигму защиты прав человека в цифровую эпоху. Директива LED наделяет биометрию статусом особо чувствительных данных. Принятие Регламента об ИИ (EU AI Act) утвердило риск-ориентированный подход, согласно которому использование полицией систем онлайн-идентификации в общественных местах признано источником неприемлемого риска и категорически запрещено (за исключением узких экстренных случаев).

В Соединенных Штатах федерального законодательства об ИИ пока нет. Регулирование децентрализовано: если ряд муниципалитетов ввел жесткие моратории на FRT для местной полиции, то федеральные службы активно сотрудничают с коммерческими вендорами вроде Clearview AI.

В Великобритании, опирающейся на прецедентное право, специального статутного закона о FRT не существует. Правоохранительные органы легитимизируют применение камер, ссылаясь на свои общие полномочия по поддержанию порядка [1].

Эволюция прецедентной практики Европейского суда по правам человека. Практика ЕСПЧ выступает золотым стандартом в вопросах определения границ полицейского биометрического вмешательства. Критерии соразмерности цифровой слежки поэтапно формировались в решениях *S. and Marper v. the United Kingdom*, *Uzun v. Germany* и *Roman Zakharov v. Russia*.

Обсуждение

Рубиконом стало постановление по делу *Glukhin v. Russia* от 4 июля 2023 года. В данном кейсе заявителя оштрафовали за одиночный мирный пикет после того, как его личность установила система распознавания лиц в метрополитене [2]. ЕСПЧ признал технологию тотального распознавания «крайне интрузивной» (highly intrusive). Исходя из позиции Суда, можно выделить три фундаментальных правовых принципа:

Принцип *extrema ratio*: технология применима лишь тогда, когда все менее радикальные методы исчерпали свою эффективность.

Принцип обоснованного подозрения: алгоритмы должны базироваться на конкретных фактах, тотальное сканирование населения (blanket use) недопустимо.

Принцип выборочной легитимности: использование FRT оправдано только для розыска строго лимитированного круга особо опасных лиц [3].

Правовое регулирование и правоприменительная практика в Республике Казахстан. В Казахстане внедрение алгоритмов компьютерного зрения в контур общественной безопасности

идет беспрецедентно быстрыми темпами, формируя новую архитектуру профилактики правонарушений и цифрового урбанизма [4].

На уровне закона оборот биометрии регулируется Законом РК «О персональных данных и их защите». Хотя закон требует согласия субъекта на обработку данных, он содержит широкие исключения для силовых структур, позволяя собирать информацию в целях национальной безопасности без ведома граждан [5].

Важнейшим инфраструктурным этапом стало внедрение Национальной системы видеомониторинга (НСВМ), утвержденной соответствующим приказом КНБ РК. НСВМ выступает централизованным хабом, агрегирующим видеопотоки с государственных и частных камер по всей республике [6].

Статистика МВД РК иллюстрирует масштаб происходящего: в 2024–2025 годах в стране функционирует более 1,4 млн камер. Интеграция систем «Сергек» и «TargetEYE» в работу полиции показала впечатляющие результаты: с помощью цифрового мониторинга раскрывается 56 % уголовных и 66 % административных деяний в публичных местах. Внедрение ИИ-камер и патрульных дронов позволило снизить общий уровень уголовной преступности на 10,9 %.

Законодатель также расширяет сферу алгоритмического контроля в КоАП РК, позволяя выписывать автоматические штрафы с помощью FRT за мелкие проступки (выброс мусора, переход дороги в неположенном месте) [7].

Однако такая повсеместная экспансия видеоаналитики вызывает критику экспертов. В Казахстане пока не принят узкопрофильный закон, который бы жестко ограничивал полицейское использование алгоритмов. Неизбирательный сбор биометрии несет угрозы конфиденциальности. На практике уже фиксировались инциденты, когда система TargetEYE в аэропортах ошибочно идентифицировала блогеров и активистов, что приводило к их необоснованным задержаниям [8]. Отсутствие строгих процессуальных фильтров, аналогичных европейскому AI Act, чревато трансформацией систем безопасности в механизм гипертротрофированного контроля, нарушающего конституционные свободы казахстанцев.

Заключение

Внедрение FRT и машинного обучения в рутинную работу административной полиции представляет собой тектонический сдвиг в развитии правоохранительных органов. Интеллектуальный видеомониторинг доказал свою феноменальную эффективность: статистика Республики Казахстан наглядно подтверждает успешность алгоритмов в профилактике преступлений и розыске правонарушителей.

Однако проведенное исследование выявило глубокий институциональный дисбаланс: технологический потенциал полицейского надзора развивается в геометрической прогрессии, тогда как правовые механизмы защиты частной жизни остаются консервативными. В силу своей технической интрузивности технология FRT при массовом применении де-факто стирает презумпцию невиновности, превращая любого горожанина в объект перманентного сканирования.

Анализ международной практики демонстрирует, что демократические страны двигаются в сторону жестких риск-ориентированных моделей, где эталоном выступает европейский AI Act. В Казахстане, при наличии базового Закона «О персональных данных», реальное применение FRT полицией регулируется в основном ведомственными приказами (как в случае с НСВМ). Подобный подход предоставляет исполнительной власти чрезмерно широкую дискрецию.

Для выстраивания конституционно сбалансированной системы необходимо кардинально реформировать национальное законодательство. Оптимальным решением станет имплементация принципов ЕСПЧ (extrema ratio, обоснованного подозрения и выборочной легитимности) в уголовно-процессуальное и административное право РК.

Рекомендуется предпринять следующие шаги: закрепить на уровне закона строгий и исчерпывающий перечень тяжких преступлений, допускающих использование FRT в реальном времени; ввести обязательное судебное санкционирование для загрузки профилей граждан в базы алгоритмического розыска; а также создать независимый контролирующий орган для аудита полицейских ИИ-систем на предмет предвзятости. Лишь перевод биометрического мониторинга в русло прозрачного и демократически контролируемого процесса позволит обществу безопасно пользоваться плодами цифровой революции.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

- 1 Bonsor K. How Facial Recognition Systems Work / K. Bonsor, R. Johnson // PCEINC. – 2019.
- 2 Studies on facial recognition technology use and racial disparities in policing / Johnson [et al.] // Tandfonline. – 2024.
- 3 Akbari Facial recognition technology categories and implications / Akbari, Lynch, Chen // MDPI. – 2024.
- 4 Perez S. H. The Impact of Facial Recognition Technology in Law Enforcement. A Leadership White Paper / S. H. Perez // LEMIT (The Bill Blackwood Law Enforcement Management Institute of Texas). – 2025.
- 5 Gültekin-Várkonyi G. Navigating data governance risks: Facial recognition / G. Gültekin-Várkonyi // Policy Review. – 2024.
- 6 Joldoshev J. Glukhin v. Russia: The European Court of Human Rights' First Step into the Age of AI Surveillance / J. Joldoshev // Federal Bar Association. – 2024.
- 7 Palmiotto F. Facial Recognition Before the European Court of Human Rights / F. Palmiotto // European Review of Digital Administration & Law (Erdal). – 2025. – Vol. 6, Issue 1.
- 8 Утеген Д. Защита биометрических данных: анализ законодательства Казахстана в контексте зарубежной практики / Д. Утеген // Maqsut Narikbayev University. – 2025.

REFERENCES

- 1 Bonsor K. How Facial Recognition Systems Work / K. Bonsor, R. Johnson // PCEINC. – 2019.
- 2 Studies on facial recognition technology use and racial disparities in policing / Johnson [et al.] // Tandfonline. – 2024.
- 3 Akbari Facial recognition technology categories and implications / Akbari, Lynch, Chen // MDPI. – 2024.
- 4 Perez S. H. The Impact of Facial Recognition Technology in Law Enforcement. A Leadership White Paper / S. H. Perez // LEMIT (The Bill Blackwood Law Enforcement Management Institute of Texas). – 2025.
- 5 Gültekin-Várkonyi G. Navigating data governance risks: Facial recognition / G. Gültekin-Várkonyi // Policy Review. – 2024.
- 6 Joldoshev J. Glukhin v. Russia: The European Court of Human Rights' First Step into the Age of AI Surveillance / J. Joldoshev // Federal Bar Association. – 2024.
- 7 Palmiotto F. Facial Recognition Before the European Court of Human Rights / F. Palmiotto // European Review of Digital Administration & Law (Erdal). – 2025. – Vol. 6, Issue 1.
- 8 Utegen D. Zashchita biometricheskikh dannyykh: analiz zakonodatelstva Kazakhstana v kontekste zarubezhnoy praktiki / D. Utegen // Maqsut Narikbayev University. – 2025. [in Russian].

С.С. Каримова¹

¹ҚР ИМ Оқу орталығы, Қазақстан

Әкімшілік полицияның адам жүзін тану жүйелерін пайдалануы: қоғамдық қауіпсіздік пен жеке өмірге қолсұғылмаушылық құқығы арасындағы теңгерімді қамтамасыз ету

Бет-әлпетті алгоритмдік тану (FRT) технологияларын әкімшілік полиция қызметіне қарқынды енгізу терең институционалдық теңгерімсіздікті тудырады. Жаппай бейнебақылау инфрақұрылымын қалыптастыру азаматтардың жеке өмірге қолсұғылмаушылық және жүріп-тұру бостандығына қатысты конституциялық құқықтарына тікелей қауіп төндіреді, бұл нақты бейінді заңнаманың жоқтығымен және машиналық біржақтылық (предвзятость) тәуекелдерімен ушыға түседі.

Қоғамдық қауіпсіздік пен жеке тұлғаның ақпараттық дербестігі арасындағы теңгерімге қол жеткізу бойынша ғылыми негізделген ұсынымдар әзірлеу үшін полицияның биометриялық технологияларды қолдануының қолданыстағы құқықтық модельдерін кешенді тұжырымдамалық талдау.

Зерттеуде жүйелік, формальды-догматикалық және салыстырмалы-құқықтық (ЕО, АҚШ, Ұлыбритания, ҚР) әдістерді қамтитын кешенді тәсіл қолданылды. Адам құқықтары жөніндегі Еуропалық соттың (АҚЕС/ЕСПЧ) прецеденттік практикасын (Glukhin v. Russia ісі)

және ҚР ІІМ-нің 2024–2025 жылдардағы өзекті эмпирикалық статистикасын талдауға ерекше назар аударылды.

FRT-тің жоғары криминалистикалық тиімділігі мойындалды. Алайда, Қазақстанда тану жүйелерін қолдану негізінен заңға тәуелді актілермен реттелетіні анықталды, бұл күштік құрылымдарға шамадан тыс дискреция (еркіндік) береді. Халықты талғамсыз биометриялық сканерлеу іс жүзінде кінәсіздік презумпциясын жоққа шығарады.

Халықаралық тәуекелге бағдарланған стандарттарды (EU AI Act) және Еуропалық соттың қағидаттарын (*extrema ratio*) имплементациялау арқылы ұлттық заңнаманы реформалаудың сыни қажеттілігі негізделді. Нақты қадамдар ұсынылды: алгоритмдік іздестіруді міндетті түрде соттың санкциялауы, FRT қолдану үшін қылмыстардың толық тізбесін бекіту және ЖІ тәуелсіз аудит институтын құру.

Түйінді сөздер: адам жүзін тану, әкімшілік полиция, қоғамдық қауіпсіздік, жеке өмірге қолсұғылмаушылық құқығы, биометриялық дербес деректер, бейнебақылау, адам құқықтары, жасанды интеллект, прецеденттік тәжірибе, ақпараттық дербестік, Қазақстан Республикасы.

S.S. Karimova¹

¹Training Center of the MIA of the RK, Kazakhstan

Use of Facial Recognition Systems by Administrative Police: Ensuring a Balance Between Public Safety and the Right to Privacy

The rapid integration of algorithmic facial recognition technologies (FRT) into the activities of the administrative police generates a deep institutional imbalance. The formation of a total video surveillance infrastructure poses a direct threat to citizens' constitutional rights to privacy and freedom of movement, exacerbated by the lack of clear specific legislation and the risks of machine bias.

A comprehensive conceptual analysis of existing legal models for the use of biometric technologies by the police to develop scientifically grounded recommendations for achieving a balance between public safety and the informational autonomy of the individual.

The research applies a comprehensive approach, including systemic, formal-dogmatic, and comparative-legal (EU, USA, UK, RK) methods. Special emphasis is placed on the analysis of the ECtHR case law (*Glukhin v. Russia*) and the relevant empirical statistics of the Ministry of Internal Affairs of the Republic of Kazakhstan for 2024–2025.

The high forensic effectiveness of FRT is recognized. However, it has been established that in Kazakhstan, the use of recognition systems is primarily regulated by subordinate acts, which provides law enforcement agencies with excessive discretion. Indiscriminate biometric scanning of the population *de facto* erases the presumption of innocence.

The critical need to reform national legislation by implementing international risk-oriented standards (EU AI Act) and ECtHR principles (*extrema ratio*) is substantiated. Specific steps are proposed: mandatory judicial authorization of algorithmic searches, establishment of an exhaustive list of crimes for FRT use, and the creation of an independent AI audit institution.

Keywords: facial recognition, administrative police, public safety, right to privacy, biometric personal data, video surveillance, human rights, artificial intelligence, case law, informational autonomy, Republic of Kazakhstan.

Дата поступления рукописи в редакцию: 07.04.2026 г.