УДК 342.7

ИСПОЛЬЗОВАНИЕ СИСТЕМ РАСПОЗНАВАНИЯ ЛИЦ И ЦИФРОВЫХ ДОКАЗАТЕЛЬСТВ: БАЛАНС МЕЖДУ ЭФФЕКТИВНОСТЬЮ ПРАВОСУДИЯ И КОНСТИТУЦИОННЫМ ПРАВОМ НА НЕПРИКОСНОВЕННОСТЬ ЧАСТНОЙ ЖИЗНИ

Кузнецов А.А.
Кандидат юридических наук, доцент,
ФГБОУ ВО Северо-Кавказский филиал «Российский государственный университет правосудия им. В.М. Лебедева»
г. Краснодар, Россия

Сибякина В.Д.
Студентка
ФГБОУ ВО Северо-Кавказский филиал «Российский государственный университет правосудия им. В.М. Лебедева»
г. Краснодар, Россия

Аннотация

В данной статье рассматривается проблема нормативно-правового регулирования применения технологий распознавания лиц и цифровых доказательств в контексте обеспечения конституционных прав граждан. Предметом исследования является правовой механизм поиска баланса между государственными интересами в сфере общественной безопасности и правом личности на неприкосновенность частной жизни. В исследовании применялись методы системного анализа, формально-юридический и сравнительно-правовой методы. Раскрываются проблемы отсутствия детальной регламентации сбора биометрических данных и неопределенности процессуального статуса цифровых следов. Основными выводами являются необходимость установления четких границ судебного контроля за использованием ИИ-систем и законодательное закрепление гарантий против избыточного цифрового

слежения. Авторы приходят к выводу, что цифровизация правосудия не должна приводить к девальвации базовых конституционных ценностей и приватности.

Ключевые слова: конституционное право, частная жизнь, распознавание лиц, цифровые доказательства, биометрические данные, правосудие, искусственный интеллект.

USE OF FACIAL RECOGNITION SYSTEMS AND DIGITAL EVIDENCE: BALANCE BETWEEN THE EFFICIENCY OF JUSTICE AND THE CONSTITUTIONAL RIGHT TO PRIVACY

Kuznetsov A.A.
Candidate of Legal Sciences, Associate Professor,
North Caucasus Branch of the Russian State University of Justice named after V.M. Lebedev
Krasnodar, Russia

Sibyakina V.D.
Student
North Caucasus Branch of the Russian State University of Justice named after V.M. Lebedev
Krasnodar, Russia

Abstract

In this article, the problem of legal regulation of the use of facial recognition technologies and digital evidence in the context of ensuring the constitutional rights of citizens is examined. The subject of the study is the legal mechanism for finding a balance between state interests in the field of public safety and the individual's right to privacy. System analysis, formal-legal and comparative-legal methods were used in the study. The problems of the lack of detailed regulation of biometric data collection and the uncertainty of the procedural status of digital footprints are discussed. The main conclusions are the need to establish clear boundaries for judicial control over the use

of AI systems and the legislative consolidation of guarantees against excessive digital surveillance. The author concludes that the digitalization of justice should not lead to the devaluation of basic constitutional values and privacy.

Keywords: constitutional law, privacy, facial recognition, digital evidence, biometric data, justice, artificial intelligence.

Развитие информационного общества и стремительная цифровая трансформация государственного управления ставят перед конституционно-правовой доктриной принципиально новые вызовы. Одной из наиболее дискуссионных тем последних лет является внедрение систем автоматического распознавания лиц (Facial Recognition Technology — FRT) в деятельность правоохранительных органов. Использование данных технологий создает уникальные возможности для повышения эффективности раскрытия преступлений. Однако, как отмечает В.Д. Зорькин, право в цифровом мире сталкивается с необходимостью переосмысления границ свободы и контроля, чтобы технологический прогресс не превратился в инструмент тотальной прозрачности личности перед государством [1].

Конституция Российской Федерации в статьях 23 и 24 гарантирует каждому право на неприкосновенность частной жизни, личную и семейную тайну, а также запрещает сбор, хранение, использование и распространение информации о частной жизни лица без его согласия. Внедрение систем видеонаблюдения с функциями биометрической идентификации в городскую среду («Умный город») фактически означает постоянный сбор персональных данных в общественном пространстве. Возникает вопрос: сохраняется ли право на приватность, когда гражданин находится на улице? С точки зрения традиционного подхода, общественное место подразумевает открытость, однако технологии распознавания лиц позволяют осуществлять не просто наблюдение,

а автоматизированную обработку данных, поиск связей и построение маршрутов передвижения, что уже глубоко вторгается в сферу частных интересов. Как подчеркивают П.П. Баранов и А.Ю. Окунев, «конституционно-правовые границы видеонаблюдения с функцией распознавания лиц в общественных местах до сих пор четко не установлены, что создает риск произвольного ограничения права на частную жизнь» [6].

Э.В. Талапина подчеркивает, что цифровая реальность требует «цивилизованного» правового регулирования, которое исключало бы злоупотребления при использовании больших данных [2]. Проблема заключается в том, что текущее законодательство о персональных данных и биометрии содержит ряд исключений для целей правосудия и безопасности, которые порой трактуются правоприменителем слишком широко. Отсутствие прозрачных алгоритмов работы систем искусственного интеллекта (ИИ), используемых для распознавания лиц, порождает риски судебных ошибок и необоснованного ограничения прав граждан. А.М. Лаптева и С.В. Соловьёва в своем исследовании 2024 года обосновывают, что «биометрические персональные данные нуждаются в дифференцированном правовом режиме, а их использование в правоохранительных целях должно быть сопряжено с усиленным судебным контролем и информированием субъекта» [5].

Важным аспектом является процессуальный статус результатов применения таких систем. М.В. Пономарёв и Д.А. Семёнов отмечают, что проблема допустимости цифровых доказательств в уголовном процессе остается нерешенной: отсутствие единых стандартов фиксации и верификации цифровых следов приводит к нарушению принципа законности при их использовании в суде [3]. Особую озабоченность вызывает так называемая «алгоритмическая предвзятость». Т.А. Полякова и А.В. Минбалеев доказывают, что «системы искусственного интеллекта, применяемые в правоохранительной деятельности,

могут воспроизводить и усиливать дискриминационные паттерны, что требует обязательного тестирования алгоритмов на нейтральность и прозрачность» [4].

Важным фактором риска выступает защита собранных данных. Утечка биометрических параметров носит необратимый характер. Как справедливо замечает А.М. Лаптева, «в отличие от пароля или паспортных данных, биометрию невозможно изменить, поэтому её компрометация влечет пожизненные риски для гражданина» [5]. Государство, собирая сведения для целей правосудия, берет на себя повышенную ответственность. К.А. Рыбалов акцентирует внимание на том, что «цифровые доказательства, полученные с помощью ИИ, требуют особых гарантий аутентичности, включая обязательную фиксацию метаданных, цепочки хранения и возможность независимой технической экспертизы» [7].

Особое внимание в контексте конституционных прав заслуживает проблема «черного ящика» — закрытости алгоритмов искусственного интеллекта. В правоприменительной практике возникает коллизия: с одной стороны, результаты работы системы распознавания лиц представляются в суд как объективные данные, с другой — ни защита, ни зачастую сам суд не имеют возможности проверить, на каких принципах нейросеть выстроила идентификацию. Это порождает вопрос о соблюдении принципа состязательности сторон. Как отмечает Д.В. Бахтеев, использование ИИ-систем требует формирования новых методик судебной экспертизы, которые позволяли бы оценивать не только итоговое изображение, но и математическую вероятность ошибки конкретной версии алгоритма [8]. Т.А. Полякова и А.В. Минбалеев добавляют, что «отсутствие обязанности правообладателя раскрывать исходный код или обучающие выборки делает невозможным полноценное оспаривание результатов ИИ в суде, что нарушает принцип состязательности» [4].

Более того, международный опыт показывает наличие проблемы «алгоритмической предвзятости» (algorithmic bias), когда точность распознавания существенно снижается в зависимости от освещения, ракурса или этнических признаков субъекта. В российских реалиях это диктует необходимость внедрения национальных стандартов сертификации программного обеспечения, используемого в криминалистических целях. Без четких метрик точности цифровое доказательство превращается в «мнение машины», которое крайне сложно оспорить в рамках традиционного допроса эксперта.

Интеграция систем распознавания лиц с базами данных государственных услуг и социальных сетей ведет к формированию так называемого «цифрового профиля» гражданина. С точки зрения конституционного права, это создает угрозу выхода за рамки целей сбора информации. Данные, собранные камерами видеонаблюдения для обеспечения безопасности на транспорте, не должны бесконтрольно использоваться в рамках гражданско-правовых споров или административного контроля, не связанного с первоначальной целью. П.П. Баранов и А.Ю. Окунев подчеркивают: «Тотальная идентификация в общественных местах требует введения принципа целевой адекватности — использования данных только для тех целей, для которых они были собраны, с обязательным периодическим аудитом и независимым общественным контролем» [6].

Для гармонизации интересов эффективности правосудия и защиты конституционных прав представляется необходимым:

1. Законодательно закрепить четкий перечень оснований, по которым допускается использование систем распознавания лиц в режиме реального времени. Это должно касаться только раскрытия тяжких преступлений или поиска пропавших лиц (с опорой на выводы А.М. Лаптевой и С.В. Соловьёвой [5]).

2. Ввести обязательный судебный контроль за доступом к архивам биометрических данных, полученных в ходе массового наблюдения (как предлагают М.В. Пономарёв и Д.А. Семёнов [3]).

3. Разработать стандарты верификации цифровых доказательств, полученных с помощью ИИ, исключающие опору только на «мнение» алгоритма. К.А. Рыбалов обосновывает необходимость введения института судебного эксперта по цифровым следам с правом доступа к исходному коду алгоритма в засекреченном порядке [7].

4. Обеспечить право гражданина на получение информации о том, подвергались ли его биометрические данные обработке (за исключением случаев, составляющих государственную тайну в рамках ОРД), а также право на оспаривание результатов автоматической идентификации [4, 5].

Т.Я. Хабриева и Н.Н. Черногор справедливо указывают на то, что в условиях цифровой реальности право на забвение и право на неприкосновенность частной жизни приобретают новые смыслы [9]. Постоянное хранение биометрических следов в архивах фактически лишает человека возможности на «новую жизнь» после погашения судимости или завершения правовых конфликтов. В связи с этим представляется целесообразным обсуждение законодательного закрепления сроков хранения «динамической биометрии» (записей перемещений), которые должны быть существенно короче сроков хранения традиционной дактилоскопической информации.

Наконец, нельзя игнорировать психологический аспект постоянного мониторинга. Превращение городского пространства в зону тотальной идентификации меняет социальное поведение личности. Возникает риск формирования «депрессивного правосознания», когда гражданин воспринимает технологию не как инструмент защиты, а как инструмент подавления. Баланс, о котором идет речь, невозможен без установления этических фильтров. Использование распознавания лиц в политических или идеологических целях

должно быть не просто ограничено, а юридически заблокировано на уровне конституционных запретов. Только так можно сохранить доверие между обществом и государством в эпоху четвертой промышленной революции.

Таким образом, системы распознавания лиц и цифровые следы — это мощный инструмент современного правосудия, который при правильном применении способствует реализации принципа неотвратимости наказания. Однако эффективность государства не может достигаться ценой тотального разрушения сферы приватности. Конституционное право должно играть роль регулятора, устанавливающего «красные линии» для технологий, обеспечивая приоритет прав и свобод человека над технологической целесообразностью. Только при условии прозрачности, подотчетности и строгого соблюдения процессуальных гарантий цифровизация будет служить правовому государству, а не противоречить ему.

Библиографический список

1. Зорькин В.Д. Право в цифровом мире: размышления перед марафоном // Российская газета. 2018. 29 мая. № 115 (7578).

2. Талапина Э.В. Право и цифровизация: новые вызовы и перспективы // Журнал российского права. 2018. № 2. С. 5–17.

3. Пономарёв М.В., Семёнов Д.А. Проблемы допустимости цифровых доказательств в уголовном процессе // Российский судья. 2024. № 2. С. 34–39.

4. Полякова Т.А., Минбалеев А.В. Искусственный интеллект в правоохранительной деятельности: проблемы правового регулирования и риски дискриминации // Информационное право. 2024. № 2. С. 11–17.

5. Лаптева А.М., Соловьёва С.В. Биометрические персональные данные: правовой режим и судебная практика // Журнал российского права. 2024. № 4. С. 82–94.

6. Баранов П.П., Окунев А.Ю. Конституционно-правовые границы видеонаблюдения с функцией распознавания лиц в общественных местах // Конституционное и муниципальное право. 2025. № 1. С. 24–30.

7. Рыбалов К.А. Цифровые доказательства в гражданском и уголовном процессе: критерии аутентичности и допустимости // Вестник гражданского процесса. 2024. № 6. С. 56–67.

8. Бахтеев Д. В. Искусственный интеллект в криминалистике: состояние и перспективы использования // Российское право: образование, практика, наука. 2018. № 2. С. 52–59.

9. Хабриева Т.Я., Черногор Н.Н. Право в условиях цифровой реальности // Журнал российского права. 2018. № 1. С. 85-102.

Кузнецов Александр Александрович,

Сибякина Виктория Дмитриевна, 2026