

Дата поступления рукописи в редакцию: 21.02.2026 г.

DOI: 10.24412/2782-3830-2026-2-296-300

Дата принятия рукописи в печать: 18.03.2026 г.

ЦАРЬКОВА Евгения Геннадьевна,кандидат физико-математических наук,
ведущий научный сотрудник ФКУ НИИ ФСИН России,
e-mail: university69@mail.ru

ПРАВОВЫЕ АСПЕКТЫ ФОРМИРОВАНИЯ И ИСПОЛЬЗОВАНИЯ «ЦИФРОВОГО СЛЕДА» ОСУЖДЕННОГО В УЧРЕЖДЕНИЯХ ФСИН РОССИИ

Аннотация. Современное внедрение цифровых технологий в учреждения уголовно-исполнительной системы Российской Федерации становится причиной возникновения феномена «цифрового следа» осужденных, представляющего собой совокупность данных биометрического, поведенческого и коммуникативного характера, формируемых непрерывно в процессе исполнения наказания. Исследование направлено на формирование доктринальной модели специального правового режима указанного феномена, учитывающего его двойственную природу как инструмента государственного надзора и ресурса индивидуальной ресоциализации. Анализируются правовые пробелы, идентифицируемые исходя из соотношения законодательства в сфере исполнения уголовных наказаний и защиты персональных данных, детально регулирующего физические условия изоляции, но оставляющего без достаточного правового внимания последствия дальнейшего обращения с цифровой информацией об осужденном. В работе осуществляется структурирование «цифрового следа» на отдельные компоненты, включая биометрические данные, поведенческие паттерны, коммуникативные данные и учетно-режимные сведения. Обосновывается целесообразность применения дифференцированного подхода к правовому режиму различных категорий данных (обязательное уничтожение поведенческих данных после освобождения, обезличивание биометрии для научных архивов, ограниченное хранение режимно-значимой информации по судебному решению и др.). Предлагаются законодательные изменения в ведомственные акты ФСИН России, закрепляющие сроки хранения, порядок доступа и право осужденного на ознакомление с цифровым профилем. Особое внимание уделяется проблеме «презумпции цифровой виновности», возникающей при использовании нейросетевых систем надзора без законодательных гарантий верификации алгоритмических выводов. Научная новизна исследования состоит в методологическом переходе от описания технологий цифровизации УИС к построению целостной системы видения доктрины правового регулирования данных, генерируемых в условиях пенитенциарных учреждений, с приоритетным балансом интересов государственной безопасности и фундаментальных прав человека.

Ключевые слова: цифровой след, уголовно-исполнительная система Российской Федерации, биометрические данные, видеоаналитика, персональные данные, ресоциализация, искусственный интеллект, правовой режим, ФСИН России.

TSARKOVA Evgeniya Gennadievna,Candidate of Physico-mathematical Sciences,
Senior Researcher of the Research Institute
of the Federal Penitentiary Service of Russia

LEGAL ASPECTS OF THE FORMATION AND USE OF THE «DIGITAL FOOTPRINT» OF CONVICTED PERSON IN INSTITUTIONS OF THE FEDERAL PENITENTIARY SERVICE OF RUSSIA

Annotation. The modern introduction of digital technologies into the institutions of the penal system of the Russian Federation is giving rise to the phenomenon of convicts' "digital footprint," which constitutes a set of biometric, behavioral, and communicative data generated continuously during the execution of the sentence. This research aims to formulate a doctrinal model for a special

legal regime for this phenomenon, considering its dual nature as both an instrument of state surveillance and a resource for individual re-socialization. The study analyzes legal gaps identified by comparing legislation in the field of criminal sentence execution and personal data protection, which meticulously regulates the physical conditions of isolation but leaves the consequences of the further handling of convicts' digital information without sufficient legal attention. The work structures the "digital footprint" into individual components, including biometric data, behavioral patterns, communication data, and records/regime information. The feasibility of applying a differentiated approach to the legal regime of various data categories is substantiated (e.g., mandatory destruction of behavioral data after release, depersonalization of biometrics for scientific archives, limited storage of regime-significant information by court order, etc.). Legislative amendments to the departmental acts of the Federal Penitentiary Service of Russia are proposed, establishing storage periods, access procedures, and the convict's right to review their digital profile. Special attention is paid to the issue of the "presumption of digital guilt" arising from the use of neural network surveillance systems without legislative guarantees for verifying algorithmic conclusions. The scientific novelty of the research lies in the methodological transition from describing digitalization technologies within the penal system to constructing a holistic vision for the doctrine of legal regulation of data generated in penitentiary institutions, prioritizing a balance between state security interests and fundamental human rights.

Key words: *digital footprint, penal system of the Russian Federation, biometric data, video analytics, personal data, re-socialization, artificial intelligence, legal regime, Federal Penitentiary Service of Russia.*

Введение

Масштабное внедрение искусственного интеллекта и цифровых технологий видеомониторинга, биометрической идентификации и аудиоконтроля в учреждениях уголовно-исполнительной системы Российской Федерации обусловило возникновение феномена «цифрового следа» осужденного, представляющего собой устойчивый массив данных, формируемого параллельно физическому исполнению наказания. Современные нормативные акты, включая Федеральный закон от 15.07.1995 № 103-ФЗ «О содержании под стражей подозреваемых и обвиняемых в совершении преступлений» и Уголовно-исполнительный кодекс Российской Федерации (УИК РФ), устанавливают исчерпывающие требования к материальным условиям изоляции в условиях пенитенциарных учреждений, от размеров камер до продолжительности прогулок и медицинского обеспечения. В то же время правовая судьба цифровых данных, непрерывно генерируемых вокруг каждого осужденного в результате работы систем интеллектуального мониторинга и других средств автоматизации, пока остается вне сферы системного регулирования [1, с.27]. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», применимый к деятельности ФСИН России, не учитывает специфику необходимости широкого цифрового контроля в условиях исправительного учреждения, где согласие субъекта данных отсутствует по определению, а объем собираемой информации многократно превышает традиционные учетно-режимные документы. Целью настоящего исследования является разработка концепции специального правового режима «цифрового следа» осужденного,

обеспечивающего баланс между публично-правовыми задачами надзора за исполнением наказания и частноправовым интересом лица на ресоциализацию без сохранения негативных последствий содержания в пенитенциарном учреждении, связанных с формированием массивов данных мониторинга.

Материалы и методы

В данном исследовании под «цифровым следом» осужденного в условиях содержания в учреждении УИС понимается совокупность биометрических, поведенческих, коммуникативных и учетно-режимных данных, формируемых автоматически с использованием информационных технологий и искусственного интеллекта в процессе исполнения наказания и продолжающих существовать независимо от физического нахождения лица в учреждении [2, с.47]. Данная конструкция принципиально отличается от традиционного понятия персональных данных тем, что предполагает непрерывную генерацию информации в контролируемой среде, высокую точность идентифицируемости субъекта и потенциальную возможность реконструкции истории поведения в период лишения свободы. При этом автором предлагается в структуре цифрового следа рассматривать четыре взаимосвязанных компонента: биометрические данные, поведенческие паттерны, коммуникативные и учетно-режимные данные.

Биометрические данные составляют идентификационную основу, включающую дактилоскопические формулы, цифровые шаблоны радужной оболочки глаза, геометрические модели лица и голосовые паттерны, получаемые

в системах распознавания речи [3, с.51]. Эти сведения обеспечивают непрерывную верификацию личности в условиях массового содержания и формируют неизменяемую цифровую идентичность осужденного на весь период исполнения наказания.

Поведенческие паттерны образуются посредством видеоаналитики и нейросетевых алгоритмов, фиксирующих маршруты перемещения по территории учреждения, динамику взаимодействия с другими осужденными, продолжительность пребывания в различных зонах, а также аномалии поведения, автоматически классифицируемые как потенциально опасные [4, с.57]. В отличие от разовых видеозаписей инцидентов, речь идет о систематическом профилировании поведения, которое реконструирует типовые модели действий конкретного лица в контролируемой среде.

Коммуникативные данные включают результаты аудиоаналитики телефонных переговоров осужденных, записи электронных сообщений при их наличии, а также лингвистический анализ речевых конструкций, выявляющий признаки планирования противоправных действий или передачи запрещенной информации [5, с.89].

Учетно-режимные данные представляют собой оцифрованные характеристики осужденного, сведения о поощрениях и взысканиях, медицинские заключения, данные об участии в программах исправления в виде традиционного массива информации, обретающего новое качество при интеграции в системы машинного обучения и возможности криминологического прогнозирования.

Переходя к публично-правовому аспекту использования «цифрового следа» в целях надзора, необходимо констатировать фрагментарность действующего регулирования [6, с.135]. Федеральный закон № 103-ФЗ допускает применение администрацией учреждений технических средств наблюдения и контроля, однако не раскрывает объема допустимого сбора данных, их классификации и последующего использования. Уголовно-исполнительный кодекс РФ в статье 77 закрепляет обязанность ведения личных дел осужденных и учетно-режимной документации, но не содержит норм о цифровых массивах, существенно превышающих по объему и информативности бумажные аналоги. Федеральный закон № 152-ФЗ «О персональных данных» допускает обработку информации без согласия субъекта при исполнении государственных функций, однако общие требования к уведомлению субъекта, ограничению целей обработки и принципам минимальности данных практически не реализуются в условиях тотального цифрового контроля. Федеральный закон № 144-ФЗ «Об оператив-

но-розыскной деятельности» оправдывает использование технических каналов получения информации, оставляя открытым вопрос о сроках хранения материалов после утраты оперативной ценности и возможности их трансформации в доказательства дисциплинарного либо уголовного производства.

Такая правовая конструкция порождает правовые пробелы. При этом отсутствует определение процессуального статуса видеоданных, изначально собранных для превентивных целей, является дискуссионным вопрос, могут ли автоматические метки «подозрительности», присвоенные нейросетью, служить основанием для взысканий или отказа в переводе на облегченные условия содержания [7, с.260]. В правовых актах не установлены сроки хранения биометрических шаблонов, видеопотоков, аудиозаписей, при этом в современных условиях падения стоимости цифрового хранения существует реальная перспектива бесконтрольного накопления таких массивов на неопределенный срок [8, с.111]. В настоящее время не регламентирован субъектный состав лиц, допущенных к цифровому профилю осужденного; помимо сотрудников режима и оперативных подразделений доступ могут получить информационные центры, аналитические службы, внешние подрядчики, что создает риски вторичного использования данных в несогласованных целях. Прокурорский надзор за законностью исполнения наказаний, осуществляемый в соответствии с Федеральным законом № 2202-1 «О прокуратуре Российской Федерации», традиционно ориентирован на проверку материальных условий содержания, однако механизмы контроля за цифровыми процессами остаются неразвитыми.

Особую правовую коллизию образует феномен «презумпции цифровой виновности», возникающий при доминировании алгоритмических выводов над человеческой оценкой. Нейросетевые системы надзора с учетом поступившей в систему информации способны в автоматическом режиме классифицировать поведенческие паттерны как отклоняющиеся от нормы, присваивая объектам наблюдения цифровые метки риска без обязательной верификации оператором или независимым экспертом. В условиях отсутствия законодательных запретов на автоматизированное принятие решений подобные оценки могут стать основанием для ограничения прав осужденного, включая перевод в штрафной изолятор, отказ в участии в программах ресоциализации, негативных характеристик для суда [9, с.37]. Федеральные законы № 152-ФЗ и № 144-ФЗ не содержат специальных гарантий против злоупотреблений алгоритмами, хотя общее требование соразмерности вмешательства в частную жизнь

остаётся в силе. Целесообразно закрепление презумпции вспомогательного характера ИИ-оценок как средства инициации проверок, но не заменяющих процессуальные доказательства, формируемые в установленном законом порядке.

Анализ «цифрового следа» как ресурса ресоциализации выявляет его позитивный потенциал при условии правового регулирования [10, с.98]. Массивы данных о динамике поведения, участии в коррекционных программах, структуре коммуникаций и медицинских показателях осужденных способны обеспечить индивидуализацию исполнения наказания, подбор психологической помощи, прогнозирование успешности социальной адаптации.

В отличие от публичной функции надзора, предполагающей максимальную полноту информации, ресоциализационная ценность цифрового профиля возрастает при его структурированной доступности для самого осужденного и специалистов по реабилитации. Однако отсутствие четких правил обращения с данными после отбытия срока превращает ресурс исправления в источник дискриминации. Здесь возникает вопрос о праве на «цифровое забвение», необходимый для понимания, должен ли осужденный после освобождения сохранять цифровой профиль, включающий биометрические шаблоны и поведенческие паттерны, доступные работодателям, банкам или правоохранительным органам. Современное российское законодательство не содержит исчерпывающего ответа. Согласно зарубежным практикам, биометрические данные учреждений лишения свободы подлежат удалению по истечении фиксированных сроков после освобождения. Отсутствие нормативных ограничений на хранение и доступ к «цифровому следу» может фактически продлевать срок наказания на неопределенный период.

Поведенческие паттерны, зафиксированные нейросетями в период отбывания наказания, способны стать основанием для отказа в трудоустройстве или кредитовании через автоматизированные системы оценки благонадежности.

Коммуникативные данные, собранные в рамках ОРД-мероприятий, без соответствующего регулирования потенциально трансформируются в долговременные банки информации без автоматического удаления. Биометрические шаблоны, идентифицирующие лицо независимо от возраста, сохраняют свою актуальность после погашения судимости. Вышеизложенное без дополнительной правовой проработки противоречит конституционному принципу погашения судимости и права на реабилитацию, закрепленным в статьях 57 и 50 Конституции Российской Федерации.

Результаты и обсуждение

Предлагаемая автором доктринальная модель правового режима «цифрового следа» осужденного строится на принципе дифференциации в зависимости от природы данных и целей их использования. Согласно данной модели поведенческие паттерны, полученные из систем видеонаблюдения и не связанные с установленными правонарушениями, подлежат обязательному уничтожению по истечении одного года после освобождения с составлением акта подтверждения удаления. Биометрические данные переводятся в обезличенную форму и передаются в научные архивы ФСИН России для анализа статистических закономерностей без возможности идентификации субъекта. Коммуникативные и учетно-режимные сведения, имеющие значение для оценки рецидива, хранятся не более пяти лет в системах ограниченного доступа с обязательным судебным санкционированием запросов после освобождения лица.

В качестве законодательных предложений может быть рассмотрено введение в УК РФ статьи 77.1 «Правовой режим цифровых данных осужденного», где указанная норма закрепляет совокупность факторов: перечень категорий данных, составляющих «цифровой след»; исчерпывающие сроки хранения по каждой категории; процедуры уничтожения и обезличивания; право осужденного на ознакомление с цифровым профилем не реже одного раза в квартал; порядок обжалования алгоритмических оценок в дисциплинарном производстве. Ведомственные приказы ФСИН России, регулирующие эксплуатацию систем видеонаблюдения и биометрии, целесообразно дополнить технологическими регламентами автоматического удаления данных и ведения логов операций обработки данных. Прокурорский надзор расширяется на контроль соблюдения сроков хранения цифровых массивов и законности их передачи в другие государственные системы.

Реализация предложенной модели требует разработки доктринальных критериев допустимости ИИ-оценок в пенитенциарной практике. Нейросетевые выводы о поведенческих рисках должны рассматриваться исключительно как повод для проверки, но не как самостоятельное доказательство. При этом недопустимо автоматическое вынесение взысканий на основании цифровых меток, каждое дисциплинарное решение должно сопровождаться обязательным обоснованием с указанием верифицированных источников информации. Важно, чтобы осужденному предоставлялось право на апелляцию алгоритмических классификаций через администрацию учреждения с последующим судебным контролем.

Выводы

«Цифровой след» осужденного должен трансформироваться из инструмента исключительно государственного контроля в объект правовой защиты с четко очерченными пределами существования. Цифровизация уголовно-исполнительной системы Российской Федерации обладает очевидным потенциалом повышения эффективности надзора и персонализации ресоциализации за счет алгоритмов искусственного интеллекта, однако без формирования специального правового режима сопутствующие ей данные способны породить правовые риски. Доктринальная модель, предложенная в настоящем исследовании, обеспечивает сбалансированное развитие цифровых технологий УИС в соответствии с конституционными принципами соразмерности и защиты частной жизни.

Список литературы:

- [1] Голованова Н.А., Гравина А.А., Зайцев О.А. Уголовно-юрисдикционная деятельность в условиях цифровизации: монография. – М.: ИЗиСП, КОНТРАКТ, 2019. 212 с.
- [2] Лебедев А.А., Маслов И.Р. Цифровая трансформация криминалистической габитоскопии: синтез традиционных и поведенческих признаков в условиях киберпространства // Диалог. 2025, № 22(52). С. 47-48.
- [3] Минаев В.А., Бондарь К.М., Федорович В.Ю. Биометрия защиты объектов: возможности и перспективы // Информация и безопасность. 2025. Т. 28, № 1. С. 47-56.
- [4] Царькова Е.Г., Кочкина О.В. Применение искусственного интеллекта при обработке данных в научной и образовательной деятельности Федеральной службы исполнения наказаний // Ведомости уголовно-исполнительной системы. 2022, № 9(244). С. 51-59.
- [5] Хазиев Ш.Н., Штохов А.Н. Судебные экспертизы по делам об ошибочной биометрической идентификации // Теория и практика судебной экспертизы. 2024. Т. 19, № 3. С. 88-102.
- [6] Царькова Е.Г. К вопросу формирования обучающих датасетов для выявления источников распространения экстремистского контента в сети Интернет // Научно-технический вестник Поволжья. 2024. № 3. С. 134-136.
- [7] Пальянова Н.В. Использование искусственного интеллекта в сфере Legal Tech: современные возможности и перспективы // Социально-экономическое развитие и качество правовой среды: Труды VIII Моск. юрид. форума, XIX Междунар. науч.-прак. конф. Ч. 2. М.: МГЮА, 2021 С. 260-267.
- [8] Понкин И.В. Государственное управление и регуляторное пространство в сфере искус-

ственного интеллекта // Вестник Университета имени О.Е. Кутафина (МГЮА). 2022, № 11 (99). С. 108-116.

[9] Минбалеев А.В. Регулирование использования искусственного интеллекта в России // Информационное право. 2020. № 1. С. 36-39.

[10] Понкин И.В., Редькина А.И. Искусственный интеллект с точки зрения права // Вестник Российского университета дружбы народов. Серия: Юридические науки. 2018. Т. 22, № 1. С. 91-109.

References:

- [1] Golovanova N.A., Gravina A.A., Zaitsev O.A. Criminal jurisdictional activities in the context of digitalization: monographs. - M.: IZiSP, CONTRACT, 2019. 212 pp.
- [2] Lebedev A.A., Maslov I.R. Digital transformation of forensic habitoscopy: synthesis of traditional and behavioral features in cyberspace//Dialogue. 2025, № 22(52). S. 47-48.
- [3] Minaev V.A., Bondar K.M., Fedorovich V.Yu. Biometrics of object protection: opportunities and prospects//Information and security. 2025. T. 28, NO. 1. S. 47-56.
- [4] Tsarkova E.G., Kochkina O.V. The use of artificial intelligence in data processing in the scientific and educational activities of the Federal Penitentiary Service//Vedomosti of the penitentiary system. 2022, № 9(244). S. 51-59.
- [5] Khaziev Sh.N., Shtokhov A.N. Forensic examinations in cases of erroneous biometric identification//Theory and practice of forensic examination. 2024. VOL. 19, NO. 3. S. 88-102.
- [6] Tsarkova E.G. On the formation of training datasets to identify sources of distribution of extremist content on the Internet//Scientific and Technical Bulletin of the Volga Region. 2024. № 3. S. 134-136.
- [7] N.V. Palyanova. The use of artificial intelligence in the field of Legal Tech: modern opportunities and prospects//Socio-economic development and quality of the legal environment: Proceedings VIII Mosk. jurid. forum, XIX International. scientific-practical. conf. PART 2. M.: MOSCOW STATE LAW ACADEMY, 2021 S. 260-267.
- [8] Ponkin I.V. Public administration and regulatory space in the field of artificial intelligence//Bulletin of the University named after O.E. Kutafina (MSLA). 2022, № 11 (99). S. 108-116.
- [9] Minbaleev A.V. Regulation of the use of artificial intelligence in Russia//Information law. 2020. № 1. S. 36-39.
- [10] Ponkin I.V., Redkina A.I. Artificial intelligence from the point of view of law//Bulletin of the Peoples' Friendship University of Russia. Series: Legal Sciences. 2018. VOL. 22, NO. 1. S. 91-109.