Научная статья
УДК: 340.12:004.89
DOI: 10.17323/tis.2025.27969

Original article

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ОБРАБОТКИ И ИСПОЛЬЗОВАНИЯ ЛИЦА И ГОЛОСА КАК ИСКЛЮЧЕНИЯ ИЗ ОБЩЕГО РЕЖИМА ПЕРСОНАЛЬНЫХ ДАННЫХ ДЛЯ ОБУЧЕНИЯ МОДЕЛЕЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

LEGAL REGULATION OF THE PROCESSING AND USE OF FACES AND VOICES AS EXCEPTIONS TO THE GENERAL REGIME OF PERSONAL DATA FOR TRAINING ARTIFICIAL INTELLIGENCE MODELS

Артем Алексеевич ОЛИФИРЕНКО
Саратовская государственная юридическая академия, Саратов, Россия,
artemolifirenko@yandex.ru,
ORCID: 0000-0002-2186-281X,
SPIN-код: 9400-2044

Информация об авторе
А.А. Олифиренко — магистрант Саратовской государственной юридической академии, магистрант кафедры информационной безопасности Саратовского государственного технического университета имени Ю.А. Гагарина, специалист по защите данных ООО «Экосистема недвижимости “Метр квадратный”»

Аннотация. Проведен правовой анализ исключительного режима обработки изображения лица и голосовой записи как категорий персональных данных, прямо разрешенных к передаче без согласия субъекта в условиях действия ч. 4 ст. 6.1 Федерального закона № 123-ФЗ. Эти данные, обладая биометрической природой, интегрируются в составы, подлежащие централизованной обработке в архитектуре Единой информационной платформы национальной системы управления данными, функционирующей в логике нормативно ограниченного доступа. Выдвигается тезис о необходимости пересмотра подхода к правовому режиму обезличенных данных в условиях алгоритмической обработки, предполагающей возможность реконструкции субъектной принадлежности. Исследуется правовая природа данного исключения и его функциональная связь с процедурами обезличивания, архитектурой маршрута передачи данных, порядком формирования составов и ограничениями, установленными на стадии их дальнейшего использования.
Главное внимание уделено юридическим последствиям обучения ИИ на таких данных, при которых технически возможна реконструкция признаков, позволяющих установить субъектную принадлежность. В этом контексте рассматриваются пробелы действующего регулирования, включая отсутствие понятий, охватывающих алгоритмические структуры, способные к косвенной идентификации. Предложены нормативное разграничение ИИ-моделей, создаваемых на основе составов данных, в зависимости от степени их предрасположенности к субъектной реконструкции, а также формализация механизмов допуска, контроля и правовой подотчетности. Обоснованы необходимость введения обязательной процедуры верификации обученной модели ИИ на предмет ее соответствия условиям необратимости идентификации, а также установления перечня допустимых целей обучения. Сформулировано предложение о регулировании таких отношений специальным приказом Минцифры России, включающим аккредитацию доверенных вычислительных сред, классификацию моделей ИИ и порядок проведения правовой экспертизы результата.

Ключевые слова: персональные данные, биометрические данные, искусственный интеллект, модель с реконструкцией идентичности, обезличивание, согласие субъекта, правовой режим, обучение алгоритмов, нормативный контроль

Для цитирования: *Олифиренко А.А.* Правовое регулирование обработки и использования лица и голоса как исключения из общего режима персональных данных для обучения моделей искусственного интеллекта // Труды по интеллектуальной собственности (Works on Intellectual Property). 2025. Т. 54, № 3. С. 104–116; DOI: 10.17323/tis.2025.27969

Artem Alekseevich OLIFIRENKO
Saratov State Law Academy, Saratov, Russia,
artemolifirenko@yandex.ru,
ORCID: 0000-0002-2186-281X,
SPIN-code: 9400-2044

Information about the author
A.A. Olifirenko — master's student at Saratov State Law Academy, a master's student at the Department of Information Security at Yuri Gagarin State Technical University of Saratov, and a data protection specialist at "Square Meter" Real Estate Ecosystem LLC

Abstract. This article presents a comprehensive legal analysis of the special regime governing the processing of facial images and voice recordings as categories of personal data explicitly permitted for transfer without the subject's consent under Part 4 of Article 6.1 of the Federal Law No. 123-FZ. These data, by their biometric nature, are integrated into structured datasets subject to centralized processing within the architecture of the Unified Information Platform of the National Data Governance System, which operates under a legally constrained access framework. The article argues for a reassessment of the current legal regime applicable to anonymized data in the context of algorithmic processing that enables potential reidentification of data subjects. The analysis explores the legal essence of the aforementioned exception and its functional linkage to anonymization procedures, data transmission pathways, the formation of structured datasets, and the regulatory limitations imposed on their subsequent use. Central attention is devoted to the legal implications of training AI models on such data, particularly in scenarios where technical reconstruction of subject-specific traits is feasible. Within this framework, the study identifies normative gaps in current regulation, including the lack of legally defined concepts for algorithmic systems capable of indirect identification. The article proposes a legal typology of AI models trained on structured personal data, based on their inherent risk of enabling subject reidentification, and outlines mechanisms for regulatory access, oversight, and accountability. It substantiates the need for mandatory pre-deployment verification procedures to assess model compliance with conditions of non-reidentifiability and to establish a legally defined list of permissible training purposes. The author advocates for the adoption of a dedicated regulatory act by the Ministry of Digital Development of the Russian Federation, which would define trusted computing environments, establish a classification of AI models by risk level, and prescribe rules for legal assessment of model outputs.

Keywords: personal data, biometric data, artificial intelligence, identity-reconstructive model, anonymization, data subject consent, legal regime, algorithmic training, normative oversight

For citation: *Olifirenko A.A.* Legal Regulation of the Processing and Use of Faces and Voices as Exceptions to the General Regime of Personal Data for Training Artificial Intelligence Models // Works on Intellectual Property. 2025. Vol. 54 (3). P. 104–116; DOI: 10.17323/tis.2025.27969

ВВЕДЕНИЕ

Современный этап цифровой трансформации сопровождается качественным изменением архитектуры государственного управления данными и перераспределением центров нормативного контроля за обработкой персональной информации. Одним из ключевых инструментов этой трансформации выступает Федеральная государственная информационная система «Единая информационная платформа национальной системы управления данными» (ФГИС «ЕИП НСУД» [1]), регулируемая Постановлением Правительства РФ от 14.05.2021 № 733 [2] (и ранее заложенная в дорожной карте [3]) и предназначенная для централизованного формирования, хранения и передачи обезличенных персональных данных. Именно в структуре ЕИП НСУД в ближайшей перспективе предполагается реализация новой нормативной модели — работы с составами персональных данных [фактически датасетами для обучения моделей искусственного интеллекта (далее — ИИ-модели) в рамках Федерального закона № 123-ФЗ [4] по экспериментальному развитию ИИ в Москве].

Понятие «состав персональных данных» (далее — ПДн) было закреплено в ст. 13.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (в ред. Федерального закона № 233-ФЗ [5] от 08.08.2024) (далее — Федеральный закон № 152-ФЗ) как совокупность сведений, полученных в результате обезличивания персональных данных, сгруппированных по определенному признаку и не допускающих идентификацию конкретного субъекта без применения дополнительных действий. Особый статус в рамках составов данных получили изображение лица и запись голоса, которые, согласно ч. 4 ст. 6.1 Федерального закона № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации — городе федерального значения Москве, об особенностях обработки персональных данных при формировании региональных составов данных и предоставления доступа к региональным составам данных и внесении изменений в ст. 6 и 10 Федерального закона "О персональных данных"» (в ред. Федерального закона № 233-ФЗ) (далее — Закон № 123-ФЗ) допускаются к обработке без получения предварительного согласия субъекта — при условии уведомления и отсутствия его возражения.

Эти данные, несмотря на их биометрическую природу, не охватываются общим запретом, предусмотренным для специальных категорий персональных данных. Напротив, законодатель конструктивно вводит режим нормативного исключения, допускающий их обработку в пределах государственно организованной инфраструктуры, при соблюдении процедур предварительного оповещения и технической необратимости идентификации. В соответствии с проектом Постановления Правительства РФ от 14.02.2025 [6] предполагается нормативно закрепить, что ФГИС «ЕИП НСУД» станет системой, уполномоченной централизованно работать с такими данными в составе формируемых обезличенных наборов. В этих целях создается специализированная подсистема обработки обезличенных данных, в которой лицо и голос обрабатываются под государственным контролем с ограниченным и проверяемым доступом.

В российском информационном праве формируется новая правовая конструкция допустимой безсогласной обработки отдельных категорий биометрически значимой информации, основанная на механизме уведомления, отказа и обработки в пределах заранее одобренной и централизованной архитектуры. Эта конструкция выходит за пределы классической модели согласия.

Цель настоящего исследования — определить юридическую модель допустимой обработки изображения лица и голосовой записи как персональных данных, прямо разрешенных к обработке без согласия в условиях действия ч. 4 ст. 6.1 Федерального закона № 123-ФЗ. Особое внимание уделено институциональной логике исключения, юридическим гарантиям, режиму доступа к информации и последствиям введения такой модели для всей системы регулирования персональных данных в Российской Федерации. Кроме того, целью настоящего исследования является изучение допустимой обработки изображения лица и голосовой записи в рамках исключения, с уче-

том нормативных условий их обезличивания, включения в составы персональных данных и последующего использования для обучения алгоритмических ИИ-моделей.

МАТЕРИАЛЫ И МЕТОДЫ ИССЛЕДОВАНИЯ

Методологическая основа настоящего исследования сочетает в себе формально-юридический анализ, нормативную реконструкцию и герменевтический подход к толкованию понятийного аппарата закона. В качестве источников использованы положения федеральных законов № 152-ФЗ, № 123-ФЗ, Постановление Правительства Российской Федерации от 14.05.2021 № 733 (далее — ПП РФ № 733), а также проект Постановления Правительства Российской Федерации от 14.02.2025, содержащий положения о порядке функционирования ФГИС «ЕИП НСУД».

Анализ акцентирован на юридической природе допустимости обработки изображения лица и записи голоса в пределах специально установленного нормативного исключения. Также исследуются процедурные гарантии, сопровождающие реализацию такого исключения в условиях централизации доступа, уведомительного механизма и институционального контроля. Используются материалы приказов Минцифры России [7], а также научные публикации по вопросам правового режима обработки чувствительной информации, цифровой идентичности и построения инфраструктуры доверия при обращении с обезличенными данными.

Ключевые методы включают в себя: 1) системный анализ правовой конструкции ч. 4 ст. 6.1 Федерального закона № 123-ФЗ; 2) нормативную реконструкцию понятия «состав персональных данных» как новой юридической единицы в государственном регулировании цифровых потоков; 3) сопоставление моделей допустимой обработки биометрически значимой информации при отсутствии согласия в российской и международной правовых системах. Особое внимание уделено выявлению логики исключения как института и его последствий для баланса публичного интереса и информационной автономии личности.

ПРАВОВАЯ СПЕЦИФИКА ОБРАБОТКИ ЛИЦА И ГОЛОСА: ИСКЛЮЧЕНИЕ ИЗ ОБЩЕГО РЕЖИМА

Действующее регулирование обработки биометрических персональных данных (БПД), представленное положениями ст. 10, 13.1 Федерального закона № 152-ФЗ и ст. 6.1 Федерального закона № 123-ФЗ, формировалось на основе принципа приоритета согласия субъекта как универсального основания для любых операций с физиологической или поведенческой информацией. Но в редакции от 08.08.2024 эта конструкция подверглась содержательной трансформации. Впервые на уровне федерального закона допускается обработка изображений лица и голосовых записей без получения предварительного согласия — при условии уведомления субъекта и отсутствия возражения.

Несмотря на свою биометрическую природу, указанные данные выводятся из-под общего запрета, установленного ст. 10, и переходят в категорию персональных данных, прямо разрешенных к обработке, но только в пределах специально организованной информационной инфраструктуры, такой как ЕИП НСУД. Возникает фундаментальное методологическое противоречие: с одной стороны, данные продолжают оставаться чувствительными по смыслу закона; с другой — законодатель осознанно допускает их использование в рамках механизма институционального контроля. Это порождает новую категорию в теории защиты персональных данных — ограниченно допустимые данные, которые могут использоваться без согласия при наличии правовой процедуры, технической защиты и ограничения субъектного состава пользователей.

В связи с этим требуется пересмотр понятийного ядра законодательства о персональных данных. Конструкция «согласия» как универсального основания становится относительной и требует разграничения между добровольным согласием (по инициативе субъекта ПДн), обработкой на основе уведомления (по инициативе государства с правом отказа) и обработкой без законного основания (запрещенная).

Появляется и особая подкатегория данных — обезличенные, но контролируемо реконструируемые, которые технически обрабатываются в государственно защищенной системе, но юридически продолжают быть связанными с личностью. В ЕИП НСУД такие данные поступают в составы, где к ним предоставляется доступ только после проверки статуса пользователя, целей обращения и соответствия требованиям ст. 13.1 Федерального закона № 152-ФЗ.

Юридически механизм, предусмотренный ч. 4 ст. 6.1 Федерального закона № 123-ФЗ, представляет собой институционализированное исключение, сочетающее уведомительный порядок, запрет на свободную передачу, требования к уничтожению в случае возражения и обязательность обработки исключительно в рамках государственной информационной системы.

В более широком контексте формирование исключения, предусмотренного ч. 4 ст. 6.1 Федерального закона № 123-ФЗ, выявляет структурную коллизию

между классической доктриной персональных данных (основанной на прямой корреляции между субъектом и его цифровым представлением) и концепцией алгоритмического управления, в которой ключевым элементом становится автономная, институционально опосредованная идентификация. Как подчеркнули Х.Р. Уматгериева и Т. Хасбулатов, «биометрическая идентификация становится ключевым элементом обеспечения безопасности, поскольку она предполагает возможность автономной верификации без участия оператора» [8]. Это смещение от идентифицирующей операции, инициируемой субъектом, к фоновому административному распознаванию порождает необходимость нормативной переоценки функций хранения, доступа и юридической квалификации таких данных.

Как справедливо отметили В.Б. Наумов и Е.В. Тытюк, «данные, на которых алгоритм обучается, формируют его опыт, что означает прямую связь между данными для обучения и тем, какие решения будут в итоге приниматься алгоритмом» [9]. Хотя в настоящем исследовании не акцентируется внимание на механизмах машинного обучения как таковых, сама логика предикативного анализа, лежащая в основе государственной работы с биометрическими признаками, требует понимания субъектности в более гибкой форме: не как наличия идентификатора, а как функции, реконструируемой системой принятия решений.

В этих условиях возрастает потребность в доктринальной артикуляции новых понятий: «структурно восстанавливаемый субъект», «модель, косвенно способная к идентификации», «персонифицируемое управление». Их значение особенно заметно в рамках создаваемой в ЕИП НСУД подсистемы, в которой изображение лица и голос, пусть и подлежат предварительному уведомлению, но формируют новый тип цифровой субъектности, находящейся между приватной принадлежностью и публичной управляемостью.

Как подчеркнули Ю.А. Мильшин и А.М. Ахтямов, «биометрические технологии становятся основой для построения ИИ, способного к адаптации, самообучению и идентификации по сложным поведенческим и физиологическим паттернам, что требует нормативного переосмысления способов хранения, сопоставления и обезличивания таких данных» [10]. Хотя законодатель в рамках ЕИП НСУД стремится минимизировать риск повторной идентификации через технические процедуры и ограничение субъектов доступа, юридическая конструкция по-прежнему должна учитывать возможность институциональной реконструкции личности даже в условиях формального обезличивания.

Именно поэтому режим обработки изображения лица и голоса, несмотря на нормативную простоту (уведомление и отсутствие возражения), формирует новую технологию управления субъектностью — инструмент перехода от индивидуального контроля к централизованной инфраструктуре доверия, в которой субъект уже не распоряжается своими данными напрямую, но существует в пределах архитектуры допустимого.

NON-REIDENTIFIABILITY BY DESIGN КАК ПРАВОВО-ТЕХНИЧЕСКАЯ КОНСТРУКЦИЯ ОБЕЗЛИЧИВАНИЯ

Правовой режим обезличивания персональных данных, формируемых в процессе трансформации изображения лица и записи голоса, получил нормативное закрепление в положениях ч. 5 ст. 6.1 Федерального закона № 123-ФЗ, а также в проекте постановления правительства (по обезличиванию данных [11]), разрабатываемого во исполнение ч. 3 ст. 13.1 Федерального закона № 152-ФЗ. Этот режим впервые вводит жестко регламентированную модель обработки, основанную на правовом принципе необратимости идентификации, который в технической доктрине соответствует концепции non-reidentifiability by design [12] (рецитал (преамбула) 26 GDPR [13]) — нормативного дизайна системы, исключающего возможность восстановления субъектной связи при любых условиях, включая контекстную перекрестную идентификацию, атаки инверсии модели, объединение с внешними источниками и др.

Проект требований устанавливает, что обезличивание персональных данных, включая биометрические категории, допускается исключительно при выполнении совокупности условий (п. 1 проекта). Во-первых, применение только утвержденных методов обезличивания — идентификация произвольных или кастомных подходов категорически запрещается (подп. «а»). Во-вторых, требуется жесткое логическое и физическое разделение между идентифицирующей и обезличенной информацией, включая отдельное хранение массивов, исключающее их обратное сопоставление (подп. «б»). В-третьих, реализуются меры информационной безопасности, предписанные ст. 19 Федерального закона № 52-ФЗ: обязательное шифрование, контроль доступа, журналирование, инцидент-менеджмент (подп. «в»).

Центральный нормативный элемент — подпункт «е», прямо формулирующий требование невозможности повторного восстановления субъектной связи, которое распространяется не только на оператора, но и на всю архитектуру циркуляции данных. Здесь вводится ключевой параметр — обязательная поддержка подхода «без возможности их преобразования к исходному виду» как структурного свойства массива, а не результата конкретного алгоритма. Даже при

наличии у оператора всей совокупности входных и выходных данных, а также доступа к внешним источникам формально и технически должно быть исключено повторное определение субъектной принадлежности.

Указанный режим в силу своей нормативной природы преобразует презумпцию допустимости обработки. Если ранее при соблюдении метода считалось, что данные являются обезличенными, то теперь доказывать это должен субъект обезличивания, в том числе через количественные оценки и модельные сценарии. Проект постановления прямо отсылает к необходимости согласования с федеральным органом безопасности, который должен рассматривать исследовательское обоснование примененного метода и оценку вероятности субъектной реконструкции по каждому составу данных.

В юридическом измерении данный подход оформляется как отказ от принципа «обезличивание как технический акт» в пользу конструкции «обезличивание как правовое состояние данных», сформированное и проверенное институционально.

АРХИТЕКТУРА СОСТАВОВ ДАННЫХ И МАРШРУТ ПЕРЕДАЧИ

Маршрут передачи данных формализован в несколько уровней. Передача данных начинается с направления региональным оператором — государственным или муниципальным органом либо подконтрольной ему организацией — обезличенных персональных данных в региональную информационную систему, откуда данные поступают в ЕИП НСУД [14]. Такая передача осуществляется в соответствии с требованием, направляемым уполномоченным органом, в котором указывается конкретный перечень категорий персональных данных, включая изображения и голосовые записи. Региональный оператор не вправе отклониться от параметров требования и обязан обеспечить соответствие всей архитектуры передачи установленным нормам.

После загрузки обезличенных данных в ЕИП НСУД уполномоченный орган формирует составы персональных данных. В соответствии с проектом изменений к Положению о платформе (ПП РФ № 733) под составом понимается структурированная совокупность сведений, сгруппированных по аналитически значимым признакам, при условии, что такая группировка не позволяет определить принадлежность данных конкретному субъекту без дополнительных действий. Подобные признаки могут включать в себя территориальную принадлежность, возраст, пол, статус в социальной системе и другие данные, в том числе разрешенные биометрические параметры (табл. 1).

Сформированные составы доступны для обработки только в пределах ЕИП НСУД. Пункт 6 проекта постановления устанавливает, что пользователями подсистемы могут быть исключительно субъекты, прошедшие проверку на соответствие требованиям, установленным ч. 7 ст. 13.1 Федерального закона № 152-ФЗ. Это юридические лица, органы власти или

Таблица 1. Этапы формирования и передачи обезличенных данных

Этап	Нормативные основания	Содержание процесс
Сбор и предварительная обработка ПДн	Части 1, 4, 9 ст. 6.1 ФЗ № 123-ФЗ; ст. 11 ФЗ № 152-ФЗ	Оператор формирует массив данных, включая изображения лица и голосовые записи, полученные в рамках правомерной цели (например, госуслуги)
Обезличивание ПДн	Часть5 ст. 6.1 ФЗ № 123-ФЗ; ч. 3 ст. 13.1 ФЗ № 152-ФЗ; п. 3–5 проекта ПП РФ по обезличиванию	Обезличивание по утвержденным методикам с исключением субъектной связи. Применяются: физическая и логическая изоляция, криптозащита, проверка невозможности реидентификации
Верификация и формирование подтверждения	Часть 5 ст. 6.1 ФЗ № 123-ФЗ; ПП РФ № 733; п. 7 проекта ПП РФ по обезличиванию	Подтверждение оператора о невозможности восстановления идентификатора
Передача в ГИС	Части 2, 4 ст. 13.1 ФЗ № 152-ФЗ; п. 17 ПП РФ № 733	Оператор направляет обезличенные данные в государственную информационную систему (ЕИП НСУД) строго по требованию уполномоченного органа
Формирование составов данных	Часть 1 ст. 13.1 ФЗ № 152-ФЗ; п. 23 ПП РФ № 733	Уполномоченный орган агрегирует обезличенные ПДн по допустимым признакам (пол, возраст, район и другие данные), при этом исключается возможность субъектизации

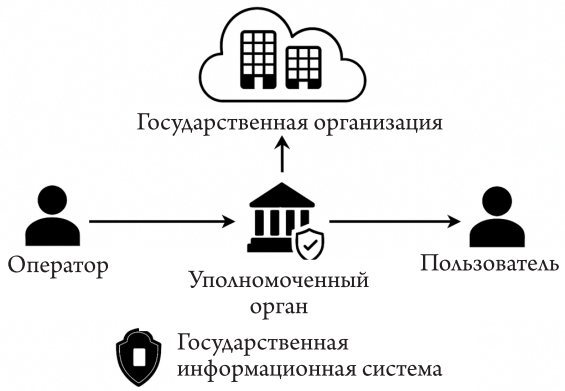
граждане, не имеющие признаков экстремистской и террористической деятельности, иностранного гражданства, недостоверных сведений в ЕГРЮЛ, а также судимостей по ст. 183, 272, 273, 274.1, 283 и 283.1 УК РФ [15]. Только при выполнении этих условий пользователь получает доступ к составу данных через защищенный интерфейс.

Сами составы данных не выгружаются, не передаются, не предоставляются и не извлекаются пользователем. Их обработка осуществляется исключительно внутри платформы ЕИП НСУД [16], при этом возможен только доступ к агрегированным результатам анализа, построенным по установленным нормативным сценариям. Реализуется архитектура одностороннего контролируемого доступа, исключающая возможность технического восстановления или извлечения индивидуализированной информации за пределами защищенной среды (но на данный момент в Инструкции ЕИП НСУД это не отражено [17]).

На маршруте передачи действует обязательный этап верификации состояния состава. До предоставления доступа пользователю система автоматически проверяет соответствие массивов обезличенных данных требованиям правового режима: наличию параметров, исключающих возможность восстановления субъектной связи, соответствию ранее утвержденным методикам обезличивания и требованиям информационной безопасности. При выявлении несоответствий передача состава приостанавливается до устранения нарушений. Эта проверка выступает частью реализуемого механизма институционального контроля на всем протяжении маршрута — от оператора до аналитической интерпретации.

Вся архитектура построена как каскадная модель с фиксированными нормативными промежуточными точками: оператор — уполномоченный орган — государственная информационная система — пользователь (рис. 1).

Рис. 1. Каскадная модель формирования составов данных



При этом ЕИП НСУД функционирует не как хранилище, а как нормативно верифицированный шлюз допустимой аналитики, где каждый результат формируется в рамках предельно допустимой модели использования данных.

В завершение положения ч. 10–12 ст. 6.1 Федерального закона № 123-ФЗ вводят запрет на действия, которые могут повлечь причинение вреда субъектам персональных данных или охраняемым законом ценностям. Это включает запрет на использование составов в целях дискриминации, угроз безопасности, подрыва прав субъектов, а также на передачу результатов обработки иностранным субъектам. В результате архитектура маршрута передачи выступает не только как технико-правовая структура, но и как элемент государственной политики доверенного управления данными.

ОБУЧЕНИЕ МОДЕЛИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА НА ОСНОВАНИИ СОСТАВА ПЕРСОНАЛЬНЫХ ДАННЫХ, СФОРМИРОВАННОГО НА УСЛОВИЯХ Ч. 4 СТ. 6.1 ФЕДЕРАЛЬНОГО ЗАКОНА № 123-ФЗ

Обучение ИИ-модели на персональных данных, образованных в результате их обезличивания, получило особую форму допустимой автоматизированной обработки на основании п. 9.1 ч. 1 ст. 6, ст. 13.1 Федерального закона № 152-ФЗ. В рамках действующего регулирования закрепляется возможность обработки обезличенных данных в целях, прямо указанных в федеральном законодательстве, включая ст. 6.1, 6.2 Федерального закона № 123-ФЗ и Федеральный закон № 58-ФЗ [18]. Эти правовые основания создают исключительный контур допустимости, в котором формируется новая институциональная модель использования данных — не как прямого инструмента идентификации, а как ресурса для построения функциональных моделей предсказательного анализа и поддержки управленческих решений.

Вместе с тем составы данных, включающие сведения, полученные в результате обезличивания изображений лица и голосовых записей, согласно ч. 2.1 ст. 10 Федерального закона № 152-ФЗ, допускаются к использованию в целях повышения эффективности государственного или муниципального управления, а также в иных целях, установленных федеральными законами. Это создает предпосылки для легального обучения ИИ-моделей на биометрических признаках при условии их предварительной трансформации и институционального контроля. Как подчеркивается в ч. 9.1 ст. 6 закона, такие действия не требуют согласия субъектов данных при условии соблюдения проце-

дуры обезличивания, утвержденной Правительством РФ (разбирали выше сам порядок обезличивания по проекту постановления правительства РФ) по согласованию с федеральным органом безопасности.

С технической точки зрения обучение ИИ-модели в рамках данного правового режима предполагает обучение модели в закрытой вычислительной инфраструктуре, где отсутствует возможность извлечения исходных записей и производится только работа с параметрическим представлением выборки (табл. 2). Обучение ИИ не затрагивает субъектные параметры как таковые, а оперирует математическими обобщениями — векториальными представлениями и латентными признаками.

Таблица 2. Этапы обучения ИИ-моделей

Этап	Нормативные основания	Содержание процесс
Перенос составов в вычислительный модуль	Часть 10 ст. 13.1 ФЗ № 152-ФЗ; п. 25, 26 ПП РФ № 733	Составы данных передаются внутри закрытого контура ЕИП НСУД. Осуществляется логическое разделение вычислений и хранения, исключается экстракция
Обучение модели в изолированной среде	Части 10–12 ст. 6.1 ФЗ № 123-ФЗ; ст. 19 ФЗ № 152-ФЗ	ИИ-модель обучается на агрегированных признаках в форме тензоров или латентных представлений. Доступ к индивидуальным значениям отсутствует
Верификация модели	Часть 11 ст. 13.1 ФЗ № 152-ФЗ; п. «е» проекта ПП РФ об обезличивании	В процессе обучения оценивается соблюдение ограничений: недопустимость предсказания индивидуальных свойств, запрет на извлечение исходных ПДн, тесты на устойчивость к инверсии
Получение агрегированных результатов	Части 6–7 ст. 13.1 ФЗ № 152-ФЗ; п. 30 ПП РФ № 733	Пользователь ГИС (например, орган власти) получает итоговую модель или ее функциональные компоненты без исходных данных, с сохранением всей нормативной обвязки
Ограничения на повторную идентификацию	Часть 12 ст. 6.1 ФЗ № 123-ФЗ; п. 9.1, 9.2 проекта ПП РФ об обезличивании	Запрещена любая постобработка модели или ее результатов, способная привести к повторной идентификации субъекта

На уровне юридического статуса ИИ-модели, обученной на подобном составе данных, возникает необходимость в дополнительной классификации. В действующей редакции Федерального закона № 123-ФЗ отсутствует понятие «модель, способная к реконструкции персональных данных», в то время как результаты обучения могут в ряде случаев допускать предсказание чувствительных атрибутов — например, через поведенческое распознавание или кластеризацию речевых особенностей. Это порождает потенциальный конфликт между декларативной анонимностью состава и фактической персонализируемостью модели. Требуется ввести новые правовые категории, такие как «персонифицируемая модель» и «модель с потенциальной реконструкцией идентичности», каждая из которых будет подлежать дифференцированному регулированию в зависимости от уровня рисков.

Следует подчеркнуть, что действующая правовая конструкция не устанавливает обязательных процедур валидации обученной модели на предмет ее способности к реконструкции субъектной связи. Упомянутые в проекте подзаконных актов механизмы контроля касаются преимущественно этапа обезличивания, а не постфактум анализа функциональности модели. Это создает правовой разрыв, при котором формальная законность источника данных не гарантирует, что обученная модель не воспроизводит информацию, позволяющую осуществить предсказательную идентификацию.

Дополнительной нерешенной проблемой является отсутствие нормативных ограничений на цели обучения моделей. В то время как ст. 6.1 Федерального закона № 123-ФЗ содержит запрет на использование составов в целях, способных причинить вред субъекту, в отношении самого процесса обучения отсутствует аналогичная норма. Это открывает потенциальную возможность подготовки моделей, которые впоследствии могут быть адаптированы для использования вне допустимого правового периметра, в том числе в коммерческих системах профилирования, без согласия субъектов.

Наконец, остается открытым вопрос институциональной подотчетности при проведении таких обучений. Статья 13.1 Федерального закона № 152-ФЗ определяет порядок доступа к составам данных, но не содержит положений об обязательной сертификации или аккредитации вычислительных систем, в которых осуществляется обучение. При этом с технической точки зрения утечка латентных представлений или параметров модели может иметь сопоставимые последствия с утечкой необезличенных персональных данных.

Введение требований к «доверенным вычислительным средам», а также регламента по периодическому аудиту моделей представляется необходимым условием обеспечения непрерывной правовой совместимости между источником данных и результатом обучения.

ЗАКЛЮЧЕНИЕ

Существующий нормативный режим допуска изображения лица и записи голоса в составы персональных данных, подлежащих централизованной обработке в рамках ЕИП НСУД, представляет собой шаг к институционализации безопасного использования персональных данных, не отнесенных к биометрическим (но по факту они ими являются) в государственном управлении данных. Однако дальнейшее применение таких составов для обучения ИИ-моделей требует нормативного реагирования (табл. 3), выходящего за рамки действующей конструкции ст. 6. Федерального закона № 152-ФЗ.

Таблица 3. Регулирование выявленных проблем

Проблема	**Пробел в законодательстве**	**Предлагаемая правовая мера (в приказе Минцифры)**
Отсутствие правовой квалификации ИИ-модели, способной к реконструкции личности	В действующем законодательстве (включая ФЗ № 152-ФЗ и подзаконные акты) полностью отсутствует правовая модель описания алгоритмических систем, способных к косвенной идентификации, — не определены ни категории моделей, сохраняющих латентные биометрические признаки, ни признаки допустимости их использования. Это приводит к отсутствию какого-либо режима регулирования рисков, связанных с реконструкцией личности по результатам работы обученной модели	Внести в приказ Минцифры следующие определения: 1) персонифицируемая модель — модель, структура которой сохраняет индивидуализируемые поведенческие или физиологические признаки субъекта, даже при отсутствии прямых идентификаторов; 2) модель с потенциальной реконструкцией идентичности — модель, обученная на обезличенных данных, но способная на основе параметров восстанавливать субъектную принадлежность. Установить правовой режим: а) обязательная предварительная классификация модели перед допуском к продуктивной среде; б) верификация на устойчивость к повторной идентификации; в) ограничение целей применения моделей, попадающих в эти категории
Отсутствие процедур валидации модели на возможность предиктивной идентификации	Отсутствие нормативно закрепленной обязанности по проверке обученных моделей на способность к восстановлению субъектной связи. Закон не устанавливает обязательных процедур верификации результата обучения на предмет рисков предсказательной идентификации — в частности, через косвенные поведенческие, речевые или физиологические признаки	Установить в приказе Минцифры: 1) обязательность предварительной и последующей проверки обученных моделей на предмет возможности восстановления субъектной связи; 2) разработку формализованного протокола проверки, включающего в себя оценку риска восстановления идентичности, с оформлением отчета в адрес уполномоченного органа; 3) включение данной проверки в перечень необходимых условий для допуска модели к эксплуатации в рамках государственных или иных регулируемых информационных систем
Неурегулированность целей обучения моделей	Закон регулирует только цели использования составов, но не цели самого обучения	Установить перечень допустимых целей обучения в приказе Минцифры, включив запрет на использование моделей, обученных на составе данных, для поведенческого таргетинга, коммерческого профилирования, оценки благонадежности субъектов без согласия. Также обязать включать целевую установку в техническое задание на обучение
Отсутствие институционального контроля за средой обучения	Статья 13.1 ФЗ № 152-ФЗ не требует сертификации или аккредитации ИТ-среды	Ввести в приказ обязательное условие: обучение ИИ-моделей осуществляется исключительно в доверенных вычислительных средах (ДВС), подлежащих аккредитации. Критерии ДВС: 1) отсутствие доступа к исходным данным после загрузки; 2) контроль логов, запрет извлечения модели и параметров; 3) ежеквартальный аудит соответствия требованиям безопасности

Представляется необходимым переход от оценки формального источника данных к нормативной оценке результата функционирования алгоритма. Предложенная модель регулирования, направленная на исключение возможности реконструкции субъектной связи в процессе или по результатам обучения, требует институционального оформления. Основой такой модели может выступить проект приказа Минцифры России, фиксирующий нормативные основания для допуска, оценки и контроля алгоритмических систем, использующих изображения лица и голос, разрешенные к передаче без согласия по ч. 4 ст. 6.1 Федерального закона № 123-ФЗ.

Ключевым элементом предлагаемого регулирования становится введение дифференцированной классификации алгоритмических моделей. В приказ целесообразно включить определение двух новых категорий: персонифицируемая модель — как модель, в параметрах которой сохраняются индивидуализирующие признаки субъекта, и модель с потенциальной реконструкцией идентичности — как модель, способная восстановить субъектную связь из ранее обезличенного массива. Каждая из этих категорий должна подпадать под отдельный режим допуска, включающий в себя предварительную квалификацию, нормативно установленную проверку устойчивости к повторной идентификации и установление ограничений на область применения.

В целях правовой верификации допустимости результата обучения в приказе Минцифры следует закрепить обязанность проведения обязательной процедуры валидации модели. Эта процедура должна охватывать как предрелизную, так и последующую стадии эксплуатации, включать оценку вероятности реконструкции индивидуальных признаков и оформляться в виде отчетности перед регулятором. Установление формализованного протокола тестирования на возможность восстановления субъектной связи создает механизм юридической ответственности за результат алгоритмического моделирования.

Регулирование должно охватывать также целевые установки обучения. Предлагается нормативно ограничить допустимые цели подготовки моделей, исключив возможность их последующего использования в системах, реализующих поведенческий таргетинг, ранжирование, профилирование, оценку благонадежности либо иное применение без индивидуального согласия. В приказе следует установить обязанность включать целевое назначение модели в техническое задание, предоставляемое на стадии допуска к обучающей выборке.

Наконец, ключевым элементом обеспечения нормативной совместимости между источником данных и результатом функционирования модели выступает среда обучения. В приказе необходимо закрепить понятие доверенной вычислительной среды как совокупности технических, организационных и криптографических механизмов, исключающих доступ к исходным данным, извлечение параметров модели, а также осуществляющих журналирование операций и последующий аудит. Допуск к обучающему составу может быть предоставлен только таким средам, прошедшим аккредитацию и сертификацию в установленном порядке.

Предлагаемая система регулирования основана на идее нормативной допустимости по результату, в рамках которой обезличивание рассматривается не как формальное свойство данных, а как проверяемое состояние всей цепочки — от источника до модели. Лишь при доказанной невозможности реконструкции субъектной информации может считаться, что цели Закона о персональных данных достигнуты. Приказ Минцифры России, отражающий данные положения, позволит институционализировать безопасную архитектуру обучения ИИ-моделей на изображении лица и голосе, обеспечивая баланс между интересами цифровой трансформации и необходимостью охраны частной жизни.

СПИСОК ИСТОЧНИКОВ

1. Федеральная государственная информационная система «Единая информационная платформа национальной системы управления данными». [Электронный ресурс]. — URL: https://nsud.gosuslugi.ru (дата обращения: 17.05.2025).
2. Постановление Правительства РФ от 14.05.2021 № 733 (ред. от 28.11.2024) «Об утверждении Положения о федеральной государственной информационной системе «Единая информационная платформа национальной системы управления данными» и о внесении изменений в некоторые акты Правительства Российской Федерации» // СЗ РФ. 2021. № 21. Ст. 3585; 2024. № 49 (Ч. V). Ст. 7623.
3. Распоряжение Правительства РФ от 03.06.2019 № 1189-р (ред. от 14.05.2021) «Об утверждении Концепции создания и функционирования национальной системы управления данными и плана мероприятий («дорожную карту») по созданию национальной системы управления данными на 2019–2021 годы» // СЗ РФ. 2019. № 23. Ст. 3041; 2021. № 21. Ст. 3585.
4. Федеральный закон от 24.04.2020 № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения

технологий искусственного интеллекта в субъекте Российской Федерации — городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона "О персональных данных"» // СЗ РФ. 2020. № 17. Ст. 2701; 2024. № 33 (Ч. I). Ст. 4929.

5. Федеральный закон от 08.08.2024 № 233-ФЗ «О внесении изменений в Федеральный закон "О персональных данных" и Федеральный закон "О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации — городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона "О персональных данных"» // СЗ РФ. 2024. № 33 (Часть I). Ст. 4929.
6. Проект Постановления Правительства Российской Федерации «О государственной информационной системе, предназначенной для обработки персональных данных, полученных в результате обезличивания персональных данных, и внесении изменений в Постановление Правительства Российской Федерации от 14 мая 2021 г. № 733» (подготовлен Минцифры России 14.02.2025) // СПС «Гарант». [Электронный ресурс]. — URL: https://www.garant.ru/products/ipo/prime/doc/56914890/ (дата обращения: 17.05.2025).
7. Приказ Минцифр России от 25.02.2021 № 114 «О вводе в эксплуатацию федеральной государственной информационной системы «Единая информационная платформа Национальной системы управления данными». [Электронный ресурс]. — URL: https://info.gosuslugi.ru/docs/section/ЕИП_НСУД/ (дата обращения: 17.05.2025).
8. *Уматгериева Х.Р., Хасбулатов Т.* Разработка и исследование биометрических методов и средств защиты информации // Экономика и социум. 2024. № 6-1 (121). [Электронный ресурс]. — URL: https://cyberleninka.ru/article/n/razrabotka-i-issledovanie-biometricheskih-metodov-i-sredstv-zaschity-informatsii (дата обращения: 17.05.2025).
9. *Наумов В.Б., Тытюк Е.В.* Правовые проблемы машинного обучения // Образование и право. 2020. № 6. [Электронный ресурс]. — URL: https://cyberleninka.ru/article/n/pravovye-problemy-mashinnogo-obucheniya (дата обращения: 17.05.2025).
10. *Мильшин Ю.А., Ахтямов А.М.* К вопросу об использовании биометрических данных искусственным интеллектом // Вестник СГЮА. 2024. № 4 (159). [Электронный ресурс]. — URL: https://cyberleninka.ru/article/n/k-voprosu-ob-ispolzovanii-biometricheskih-dannyh-iskusstvennym-intellektom (дата обращения: 17.05.2025).
11. Проект Постановления Правительства «Об установлении требований к обезличиванию персональных данных, методов и правил обезличивания персональных данных» // Федеральный портал проектов нормативных правовых актов. [Электронный ресурс]. — URL: https://regulation.gov.ru/Regulation/Npa/PublicView?npaID=156232 (дата обращения: 17.05.2025).
12. Generative AI in EU law: Liability, privacy, intellectual property, and cybersecurity / C. Novelli, F. Casolari, P. Hacker et al. // Computer Law & Security Review. 2024. Vol. 55. Article No. 106066. DOI: 10.1016/j.clsr.2024.106066
13. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) // OJ L 119, 4.5.2016, p. 1–88.
14. *Боднарук Т.Р., Боднарук М.Р.* Аналитика больших данных в государственном управлении: от проблем к решениям // Экономика и бизнес: теория и практика. 2024. № 10-1 (116). [Электронный ресурс]. — URL: https://cyberleninka.ru/article/n/analitika-bolshih-dannyh-v-gosudarstvennom-upravlenii-ot-problem-k-resheniyam (дата обращения: 17.05.2025).
15. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 21.04.2025) (с изм. и доп., вступ. в силу с 01.09.2025) // СЗ РФ. 1996. № 25. Ст. 2954; 2025. № 17. Ст. 2131.
16. Частые вопросы. Федеральная государственная информационная система «Единая информационная платформа национальной системы управления данными». [Электронный ресурс]. — URL: https://nsud.gosuslugi.ru/ifp/portals/pages/6 (дата обращения: 17.05.2025).
17. Инструкция по работе в федеральной государственной информационной системе «Единая информационная платформа национальной системы управления данными» в части описания информационных ресурсов, информационных систем, наборов данных, модели витрины данных, а также формирования регламентированных запросов. Версия 2.37, 2025. [Электронный ресурс]. — URL: https://info.gosuslugi.ru/download.php?id=3654 (дата обращения: 17.05.2025).
18. Федеральный закон от 31.07.2020 № 258-ФЗ (ред. от 28.12.2024) «Об экспериментальных правовых режимах в сфере цифровых и технологических ин-

новаций в Российской Федерации» // СЗ РФ. 2020. № 31 (часть I). Ст. 5017; 2024. № 52 (Ч. I). Ст. 8533.

REFERENCES

1. Federal'naya gosudarstvennaya informatsionnaya sistema "Yedinaya informatsionnaya platforma natsional'noy sistemy upravleniya dannymi". [Elektronnyj resurs]. — URL: https://nsud.gosuslugi.ru (data obrashcheniya: 17.05.2025).
2. Postanovlenie Pravitel'stva RF ot 14.05.2021 No. 733 (red. ot 28.11.2024) "Ob utverzhdenii Polozheniya o federal'noy gosudarstvennoy informatsionnoy sisteme "Yedinaya informatsionnaya platforma natsional'noy sistemy upravleniya dannymi" i o vnesenii izmeneniy v nekotorye akty Pravitel'stva Rossiyskoy Federatsii" // SZ RF. 2021. № 21. St. 3585; 2024. № 49 (Ch. V). St. 7623.
3. Rasporyazhenie Pravitel'stva RF ot 03.06.2019 No. 1189-r (red. ot 14.05.2021) "Ob utverzhdenii Kontseptsii sozdaniya i funktsionirovaniya natsional'noy sistemy upravleniya dannymi i plana meropriyatiy ("dorozhnuyu kartu") po sozdaniyu natsional'noy sistemy upravleniya dannymi na 2019–2021 gody" // SZ RF. 2019. № 23. St. 3041; 2021. № 21. St. 3585.
4. Federal'nyy zakon ot 24.04.2020 No. 123-FZ "O provedenii eksperimenta po ustanovleniyu spetsial'nogo regulirovaniya v tselyakh sozdaniya neobkhodimykh usloviy dlya razrabotki i vnedreniya tekhnologiy iskusstvennogo intellekta v sub'ekte Rossiyskoy Federatsii — gorode federal'nogo znacheniya Moskve i vnesenii izmeneniy v stat'i 6 i 10 Federal'nogo zakona " O personal'nykh dannykh" // SZ RF. 2020. No. 17. St. 2701; 2024. No. 33 (Ch. I). St. 4929.
5. Federal'nyy zakon ot 08.08.2024 No 233-FZ "O vnesenii izmeneniy v Federal'nyy zakon "O personal'nykh dannykh" i Federal'nyy zakon "O provedenii eksperimenta po ustanovleniyu spetsial'nogo regulirovaniya v tselyakh sozdaniya neobkhodimykh usloviy dlya razrabotki i vnedreniya tekhnologiy iskusstvennogo intellekta v sub'ekte Rossiyskoy Federatsii — gorode federal'nogo znacheniya Moskve i vnesenii izmeneniy v stat'i 6 i 10 Federal'nogo zakona "O personal'nykh dannykh" // SZ RF. 2024. № 33 (Ch. I). St. 4929.
6. Proekt Postanovleniya Pravitel'stva Rossiyskoy Federatsii "O gosudarstvennoy informatsionnoy sisteme, prednaznachennoy dlya obrabotki personal'nykh dannykh, poluchennykh v rezul'tate obezlichivaniya personal'nykh dannykh, i vnesenii izmeneniy v postanovlenie Pravitel'stva Rossiyskoy Federatsii ot 14 maya 2021 g. No. 733" (podgotovlen Mintsifry Rossii 14.02.2025) // SPS "Garant". [Elektronnyj resurs]. — URL: https://www.garant.ru/products/ipo/prime/doc/56914890/ (data obrashcheniya: 17.05.2025).
7. Prikaz Mintsifr Rossii ot 25.02.2021 No. 114 "O vvode v ekspluatatsiyu federal'noy gosudarstvennoy informatsionnoy sistemy "Yedinaya informatsionnaya platforma Natsional'noy sistemy upravleniya dannymi". [Elektronnyj resurs]. — URL: https://info.gosuslugi.ru/docs/section/ЕИП_НСУД/ (data obrashcheniya: 17.05.2025).
8. *Umatgereeva Kh.R., Khasbulatov T.* Razrabotka i issledovanie biometricheskikh metodov i sredstv zashchity informatsii // Ekonomika i sotsium. 2024. № 6-1 (121). [Elektronnyj resurs]. — URL: https://cyberleninka.ru/article/n/razrabotka-i-issledovanie-biometricheskih-metodov-i-sredstv-zaschity-informatsii (data obrashcheniya: 17.05.2025).
9. *Naumov V.B., Tytyuk E.V.* Pravovye problemy mashinnogo obucheniya // Obrazovanie i pravo. 2020. No. 6. [Elektronnyj resurs]. — URL: https://cyberleninka.ru/article/n/pravovye-problemy-mashinnogo-obucheniya (data obrashcheniya: 17.05.2025).
10. *Mil'shin Yu.A., Akhtyamov A.M.* K voprosu ob ispol'zovanii biometricheskikh dannykh iskusstvennym intellektom // Vestnik SGYuA. 2024. No. 4 (159). [Elektronnyj resurs]. — URL: https://cyberleninka.ru/article/n/k-voprosu-ob-ispolzovanii-biometricheskih-dannyh-iskusstvennym-intellektom (data obrashcheniya: 17.05.2025).
11. Proekt Postanovleniya Pravitel'stva "Ob ustanovlenii trebovaniy k obezlichivaniyu personal'nykh dannykh, metodov i pravil obezlichivaniya personal'nykh dannykh" // Federal'nyy portal proektov normativnykh pravovykh aktov. [Elektronnyj resurs]. — URL: https://regulation.gov.ru/Regulation/Npa/PublicView?npaID=156232 (data obrashcheniya: 17.05.2025).
12. *Bodnaruk T.R., Bodnaruk M.R.* Analitika bol'shikh dannykh v gosudarstvennom upravlenii: ot problem k resheniyam // Ekonomika I biznes: teoriya i praktika. 2024. No. 10-1 (116). [Elektronnyj resurs]. — URL: https://cyberleninka.ru/article/n/analitika-bolshih-dannyh-v-gosudarstvennom-upravlenii-ot-problem-k-resheniyam (data obrashcheniya: 17.05.2025).
13. Generative AI in EU law: Liability, privacy, intellectual property, and cybersecurity / C. Novelli, F. Casolari, P. Hacker et al. // Computer Law & Security Review. 2024. Vol. 55. Article No. 106066. DOI: 10.1016/j.clsr.2024.106066
14. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal

data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) // OJ L 119, 4.5.2016, p. 1–88.
15. Ugolovnyy kodeks Rossiyskoy Federatsii ot 13.06.1996 No. 63-FZ (red. ot 21.04.2025) (s izm. i dop., vstup. v silu s 01.09.2025) // SZ RF. 1996. No. 25. St. 2954; 2025. No. 17. St. 2131.
16. Chastye voprosy. Federal'naya gosudarstvennaya informatsionnaya sistema "Yedinaya informatsionnaya platforma natsional'noy sistemy upravleniya dannymi". [Elektronnyj resurs]. — URL: https://nsud.gosuslugi.ru/ifp/portals/pages/6 (data obrashcheniya: 17.05.2025).
17. Instruktsiya po rabote v federal'noy gosudarstvennoy informatsionnoy sisteme "Yedinaya informatsionnaya platforma natsional'noy sistemy upravleniya dannymi" v chasti opisaniya informatsionnykh resursov, informatsionnykh sistem, naborov dannykh, modeli vitriny dannykh, a takzhe formirovaniya reglamentirovannykh zaprosov. Versiya 2.37, 2025. [Elektronnyj resurs]. — URL: https://info.gosuslugi.ru/download.php?id=3654 (data obrashcheniya: 17.0.2025).
18. Federal'nyy zakon ot 31.07.2020 No. 258-FZ (red. ot 28.12.2024) "Ob eksperimental'nykh pravovykh rezhimakh v sfere tsifrovykh i tekhnologicheskikh innovatsiy v Rossiyskoy Federatsii" // SZ RF. 2020. No. 31 (Ch. I). St. 5017; 2024. No. 52 (Ch. I). St. 8533.