ВСЕРОССИЙСКИЙ КОНКУРС НАУЧНО-ИССЛЕДОВАТЕЛЬСКИХ И ТВОРЧЕСКИХ РАБОТ МОЛОДЁЖИ

«МЕНЯ ОЦЕНЯТ В XXI ВЕКЕ»

Направление: Право

Тема: Нормативно-правовое регулирование социальных аспектов функционирования цифровых идентификаторов

Соискатель: Молчанова Мария Владимировна

Научный руководитель: Банько Полина Владимировна

Место выполнения работы: Херсонская Государственная Морская Академия

2026

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ 3
1.ПОСТАНОВКА ЗАДАЧИ ИССЛЕДОВАНИЯ 5
2. АНАЛИЗ И ОБЗОР СУЩЕСТВУЮЩЕЙ ИНФОРМАЦИИ ПО ИССЛЕДУЕМОМУ ВОПРОСУ 6
3.ОСНОВНАЯ ЧАСТЬ 7
3.1. Понятие и виды цифровых идентификаторов: социальные функции и риски 7
3.2.Нормативная база РФ: коллизии и пробелы в защите прав граждан 9
3.3.Анализ случаев дискриминации при отказе от цифровой идентификации 10
3.4.Проект федерального закона «О гарантиях аналогового доступа»: концепция и структура 12
ЗАКЛЮЧЕНИЕ 13
СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ 14

ВВЕДЕНИЕ

Цифровой идентификатор давно перестал быть технической деталью. Сегодня это пропуск к самым обычным вещам: к пенсии, к врачу, к субсидии. К тому, что прежде требовало лишь паспорта и личного визита. Удобство цифровых сервисов не вызывает сомнений. Однако их безальтернативность порождает риск, о котором в научной дискуссии говорят пока сдержанно: дискриминацию тех, кто от цифровой идентификации отказался или не смог ею воспользоваться в принципе.

Позиция автора статьи формулируется в начале работы сознательно, чтобы далее не возвращаться к оговоркам. Цифровизация публичных услуг не должна превращаться в механизм отсечения. Доступ к услугам - не удобная опция, а элемент конституционного статуса человека; государство обязано обеспечить его реализацию для всех категорий населения, включая тех, кто не пользуется смартфоном и не намерен сдавать отпечаток пальца.

Как только механизм реализации права завязывается исключительно на технологию, уязвимые группы - от пожилых людей до жителей отдалённых сёл - оказываются отрезанными от социальной инфраструктуры. Речь в этой ситуации уже не об удобстве. Речь - о равенстве.

В правовом регулировании данной сферы налицо перекос. Законодатель занят внедрением технологий и защитой данных, тогда как социальные последствия цифровизации остаются на периферии правотворчества. В результате образуется правовая лазейка: формально гражданин вправе отказаться от биометрии и электронной подписи, фактически же отказ оборачивается препятствиями на каждом шагу.

Актуальность темы ощущается сегодня острее, чем когда-либо. В 2026 году Россия фактически завершает переход к тотальной цифровой идентификации. Свыше 100 миллионов образцов лиц и голосов уже собрано в Единой биометрической системе; за минувший год число биометрических оплат выросло почти вшестеро. «Оплата улыбкой» и проход в метро по лицу перестали быть новинкой и стали повседневностью.

Параллельно складывается единый «цифровой профиль»: учётная запись ЕСИА, биометрическое подтверждение, электронная подпись. Без него всё сложнее купить билет, снять квартиру, получить услугу.

Настораживает другое. Право человека на аналоговую жизнь - возможность получать госуслуги, расплачиваться, работать без цифрового следа - на законодательном уровне как целостная гарантия, так и не сформулировано. Формально 572-ФЗ запрещает принуждать к сдаче биометрии и отказывать в услуге тем, кто от неё отказался. Формально.

Однако провозглашённая добровольность не превратилась ни в запрет безальтернативных каналов, ни в механизм защиты. В результате формируется новая социальная группа: люди, которые не могут или не хотят пользоваться цифровыми инструментами и оказываются исключёнными из общества - общества, заметим, цифрового по услугам, по оплате, по документам.

Показательно, что и само государство проблему не отрицает. Оператор Единой биометрической системы в интервью «Российской газете» прямо признал: «биометрия не должна становиться единственным условием получения базовой услуги». Признал - и одновременно привёл цифры: за 2026 год от хранения биометрии отказались около 12 тысяч человек, тогда как в систему ежедневно регистрируются десятки тысяч.

Данные допускают двоякое прочтение: как знак доверия к системе - либо как свидетельство того, что путь отказа оказался слишком трудным. Второе прочтение представляется автору более точным: когда «согласиться» стоит одного нажатия, а «отказаться» - нескольких визитов и юридической подготовки, о добровольности говорить не приходится. Этот разрыв между декларацией и механизмом и составляет предмет настоящего исследования.

Объект исследования - общественные отношения, складывающиеся в процессе использования цифровых идентификаторов в социальной сфере. Предмет - нормы российского законодательства, их регулирующие, а также судебная и административная практика, в которой случаи дискриминации получают внешнее выражение.

Цель работы - обосновать наличие правового пробела в защите прав граждан, отказывающихся от цифровой идентификации, и предложить механизм его устранения.

Задач четыре: определить социальную функцию цифровых идентификаторов; выявить коллизии действующего законодательства; проанализировать судебную практику по делам, связанным с отказом от цифровых инструментов; разработать проект нормативного акта, гарантирующего аналоговый доступ к услугам.

Методология соединяет три подхода: формально-юридический анализ (для выявления пробелов), сравнительно-правовой метод (для оценки альтернативных моделей) и кейс-метод (для демонстрации реальных последствий правовых норм).

Научная новизна работы состоит в смещении фокуса исследования. Традиционные работы концентрируются на технической стороне идентификации и безопасности данных. Настоящая статья ставит в центр равенство доступа и предотвращение социальной изоляции.

1.ПОСТАНОВКА ЗАДАЧИ ИССЛЕДОВАНИЯ

Всякое исследование начинается с выбора угла зрения, и этот выбор порой оказывается важнее самого объекта. Тему цифровых идентификаторов можно изучать с десятков позиций: как проблему криптографии, как вопрос администрирования, как сюжет конкурентного права. Настоящая работа сознательно избирает иной ракурс - социальный. Предметом внимания является не устройство системы, а её воздействие на людей: кто получает доступ к услугам без препятствий, кто - с затруднениями, кто и вовсе остаётся за бортом.

Границы исследования очерчены сферой публичных и квазипубличных услуг: государственные услуги, банковское обслуживание, здравоохранение, транспорт, трудовые отношения. Выбор не случаен. Именно в этих сферах идентификация соприкасается с конституционными правами - на социальное обеспечение, охрану здоровья, труд, судебную защиту. Корпоративные пропуска, внутренние учётные записи и прочие узкоспециальные инструменты в анализ не входят: сколь интересны они ни были технически, их сбой не оставляет человека без пенсии или врачебной помощи.

Второе ограничение - территориальное и хронологическое. Нормативный массив проанализирован по состоянию на 2025 год включительно. Судебная практика охватывает период с 2020 по 2025 год, причём акцент сделан на актах 2024–2025 годов: именно они показывают, как правоприменитель отреагировал на новейшее регулирование биометрии и электронного документооборота. Региональная фактура, там где она привлекается, ограничена Волгоградской областью и рядом других субъектов. Автор отдаёт себе отчёт в условности любого обобщения на основе ограниченной выборки.

Формулировка самой проблемы на первый взгляд предельно кратка: в законодательстве отсутствуют механизмы, гарантирующие равенство доступа к услугам вне зависимости от способа идентификации. За этой скупой фразой, впрочем, стоит целый пласт социальных реалий. Технологии развиваются быстрее права и закрепляют модель «цифрового по умолчанию»: услугу сначала переводят в электронный канал, а затем - иногда, и не всегда - законодатель обращает внимание на тех, кто в канал не попал. Для государства и бизнеса модель выгодна: дешевле, быстрее, прозрачнее. Однако она игнорирует интересы значительной части населения. Оговорками здесь не обойтись: ущемление происходит уже сейчас, без всякого злого умысла. Система попросту спроектирована под «среднего цифрового гражданина», а не под реальное разнообразие людей.

Кого следует относить к уязвимым группам? Перечень шире привычного списка пенсионеров. Есть пожилые люди, для которых смартфон остаётся скорее источником тревоги, чем удобства. Есть жители дальних сёл, где мобильный интернет исчезает с первым снегопадом. Люди с инвалидностью по зрению, для которых экран - непреодолимая стена. Граждане без регистрации и постоянного адреса. Наконец - и об этом упоминают редко - люди технически вполне грамотные, которые по убеждениям не желают передавать свои биометрические данные в централизованные базы. Примыкают к ним и те, кто столкнулся с эпизодическими сбоями: потерянный телефон, заблокированная сим-карта, отказ ЕСИА в пиковые дни [8]. Цифровая исключённость - состояние не только постоянное, но и временное. От него не застрахован никто.

Методология исследования требует отдельного пояснения. Инструментов три, и они соединяются сознательно. Формально-юридический анализ показывает, что действительно предписано законом: что гарантировано, что декларировано, а что лишь подразумевается. Сравнительно-правовой метод необходим для оценки альтернатив - в том числе зарубежных моделей, где право на аналоговый доступ уже закреплено. Кейс-метод доводит анализ до конкретного человека: за каждым судебным актом - реальный спор, реальный отказ, реальное восстановление права. Только в совокупности эти подходы дают объёмную картину: и в тексте закона, и в регламенте ведомства, и в очереди перед окном МФЦ.

Отдельно - о задачах. Их четыре, и во введении они уже названы; здесь уместно лишь уточнить акценты. Первая задача вскрывает то, что за технической оболочкой идентификаторов скрывается институт распределения доступа. Вторая ищет места, где гарантии существуют лишь

на бумаге. Третья проверяет, компенсирует ли правоприменение дефицит законодательного регулирования. Четвёртая перерастает исследование в проект федерального закона «О гарантиях аналогового доступа» - в механизм, который превратил бы декларации в работающие правила.

Если свести задачу всей работы к одной фразе, она звучит так: показать, как нормы, формально нейтральные, на практике ограничивают права граждан. Для этого недостаточно прочитать законы. Необходим анализ регламентов, ведомственных порядков и свежей судебной практики - а её отсутствие в значительной части литературы, по мнению автора, обедняет дискуссию. Доктрина обсуждает нормы. Жизнь давно перешла к их правоприменению.

И последнее - о возможных возражениях. Может показаться, что разговор о «дискриминации нецифровых» преувеличен: право на личный приём ведь сохраняется повсеместно. Возражение серьёзное, и оно не обходится молчанием. Да, формальная альтернатива почти всегда существует. Но равенство формальных возможностей - не равенство фактическое. Очередь на месяц вперёд. Одно окно на весь район. Третий визит из-за «неправильно оформленной» бумаги. Всё это - способы отказать, не отказывая. Предмет настоящего исследования - именно этот разрыв между нормой и практикой. Показать его изнутри, через законы, судебные акты и региональную фактуру, - значит выполнить поставленную задачу.

2. АНАЛИЗ И ОБЗОР СУЩЕСТВУЮЩЕЙ ИНФОРМАЦИИ ПО ИССЛЕДУЕМОМУ ВОПРОСУ

Прежде чем предлагать решения, следует честно обозреть, что сделано до нас. Обзор литературы - не формальность ради списка источников, а способ занять осмысленное место в идущей дискуссии. Место это определилось одним обстоятельством: тема цифровых идентификаторов принадлежит прежде всего технической и управленческой традиции. Собственно юридическое - и тем более социально-правовое - содержание она обросла сравнительно недавно.

Первая и наиболее разработанная линия - технико-правовая. Её представители смотрят на идентификацию сквозь призму информационной безопасности и эффективности государственного управления. Правоведы этого направления заняты коллизиями между требованиями к защите данных и потребностями их обработки [19, с. 47]. В фокусе - законность обработки, полномочия операторов, утечки. Работы важные. Но их оптика упускает главное: сама постановка вопроса исходит из того, что идентификация уже состоялась, и спор идёт лишь о её безопасности. Для значительной части граждан проблема начинается раньше - с самого факта навязанной идентификации и её последствий.

Иной взгляд у социологической традиции, для которой цифровые идентификаторы - прежде всего социальный феномен. Социологи фиксируют устойчивый рост цифрового неравенства и связывают его с демографическими и географическими факторами [17]. Внутри этой традиции сложилась, по сути, собственная периодизация. Сначала - «разрыв первого порядка»: доступ к оборудованию и сети. Затем - «разрыв второго порядка»: навыки и цифровая грамотность. Сегодня всё отчётливее проявляется «разрыв третьего порядка» - различие в реальных выгодах, которые люди извлекают из одних и тех же сервисов. Российская специфика добавляет к схеме измерение географическое: для жителя райцентра и жителя отдалённого села один и тот же «удобный» сервис означает совершенно разное. Социологическая оптика точна в диагностике. Но её предел - в том, что неравенство она фиксирует, а вопросом о правовых средствах его устранения, как правило, не задаётся.

Третья линия рассуждений - экономическая - исходит из эффекта масштаба: ценность цифровой инфраструктуры растёт вместе с числом пользователей. Аргумент небесполезен; он объясняет настойчивость, с которой государство и бизнес продвигают единые системы идентификации. Правда, у этой медали есть оборотная сторона, на которую экономическая литература смотрит куда менее охотно. Тот же эффект масштаба создаёт ловушку для тех, кто остаётся за пределами системы: чем универсальнее цифровой канал, тем беднее и дороже становится альтернативный. Аналоговые окна закрываются не потому, что исчез спрос, - а потому,

что их содержание объявлено нерациональным. Так экономическая логика оборачивается социальными издержками. Это превращение, по убеждению автора, заслуживает несравненно большего внимания, чем получает.

Зарубежные исследования указывают на прямую зависимость между уровнем доверия к государству и готовностью граждан пользоваться цифровыми идентификаторами [21, с. 89]. Там, где доверие высоко, цифровизация читается как расширение возможностей. Там, где оно низко, принудительная цифровизация рождает напряжение. Показательны и национальные модели. Во Франции закон о цифровом государстве 2016 года прямо запрещает отказывать в услуге человеку без онлайн-доступа. В Эстонии, напротив, цифровой идентификатор стал фактически монопольным входом в государственное управление. Сопоставление моделей даёт лаконичный вывод: результат зависит не столько от технологии, сколько от встроенных правовых гарантий. Для российской дискуссии это, вероятно, самый практичный урок.

В отечественной науке доминирует всё тот же технико-правовой подход. ЕСИА и биометрические системы исследуются как инструменты оптимизации госуслуг; социальное измерение идентификации остаётся на периферии. Риски отказа от идентификации почти не исследованы. Судебную практику 2024–2025 годов доктрина не осмысляет вовсе. Отсюда заметный пробел: наука не предлагает критериев, по которым можно было бы отличить приемлемую цифровизацию от дискриминационной.

Подводя итог обзору, следует констатировать: литература даёт три оптики - безопасность, неравенство, экономику масштаба. Ни одна в отдельности, да и все вместе не отвечают на вопрос, который настоящая работа ставит в центр: как правовые нормы о цифровых идентификаторах влияют на фактическое равенство доступа к базовым услугам? Доктринального ответа нет. Есть лишь фрагменты - замечания о защите данных, сюжеты о цифровом неравенстве, судебные кейсы без систематизации.

Позиция автора в этой дискуссии такова. Право не может ограничиваться техническими регламентами и вопросами безопасности; оно обязано учитывать социальные последствия внедрения технологий. Иначе цифровизация из инструмента развития превращается в фактор углубления неравенства. Поэтому в настоящей работе соединяются правовой анализ норм, социологическая диагностика неравенства и кейс-анализ правоприменения. Комбинация не нова по методу. Но, насколько известно автору, применительно к российскому материалу 2024–2025 годов она не предпринималась - и это, при всей скромности заявки, составляет элемент новизны.

Практическая значимость обзора, пожалуй, в одном. Он показывает: спор идёт не о том, нужна ли цифровизация (она нужна и происходит), а о том, какими правовыми средствами обеспечить её совместимость с равенством. Ответа литература пока не дала. Попытка дать его - содержание последующих разделов.

3. ОСНОВНАЯ ЧАСТЬ

3.1. Понятие и виды цифровых идентификаторов: социальные функции и риски

Без терминов разговор о дискриминации повиснет в воздухе. Цифровой идентификатор в широком смысле - любая совокупность сведений, позволяющая однозначно соотнести действия в цифровой среде с конкретным человеком. Определение кажется предельно нейтральным: логин, номер счёта, запись в реестре. Что здесь социального? Однако стоит перенести понятие в поле публичных услуг, как его содержание меняется радикально. Идентификатор перестаёт быть ключом к аккаунту. Он становится пропуском к правам.

Уместна аналогия с документами прошлого века. Паспорт ведь тоже когда-то был «просто бумагой» - но именно он определял, куда человеку можно, а куда нельзя, какие льготы положены, а какие нет. Цифровой идентификатор сегодня занимает ту же нишу, только на новом технологическом уровне. Разница - и существенная - в одном. Бумажный документ нельзя отозвать удалённо, заблокировать «по техническим причинам», ограничить региональными

настройками. Цифровой - можно. Именно эта управляемость превращает идентификацию из технической процедуры в социальный институт [10].

На практике гражданин сталкивается не с одним идентификатором, а с целой лестницей - от простого логина, который можно сменить за минуту, до биометрии, которую сменить невозможно. Между ними - учётная запись ЕСИА, уже не просто ключ к порталу, а фактически публично-правовой идентификатор [8]. У каждого уровня - свой «ценник» для гражданина.

Логин и пароль - базовый, самый массовый уровень. Он уязвим к компрометации, требует либо хорошей памяти, либо менеджера паролей, зато не раскрывает физиологических данных. По сути, это первый и последний по-настоящему «отзывной» идентификатор: смена его не оставляет следов. ЕСИА - конструкция уже иного качества. Подтверждённая государством учётная запись связывает пользователя не только с реестром госуслуг, но и с государственными базами данных; идентификация из договорной становится публично-правовой [8]. Биометрия - метод самый надёжный и одновременно самый чувствительный [5]. Отпечаток и геометрию лица «сменить» невозможно: утечка биометрического шаблона - компрометация, строго говоря, пожизненная. Электронная подпись - инструмент юридической значимости, подтверждающий волеизъявление лица [4]. Её особенность в ином: она уравнивает человека с организацией. Подпись гражданина имеет ту же силу, что подпись директора, - и потому незаметно превращается в обязательный атрибут «серьёзного» участника оборота.

Присмотримся к оттенкам этой лестницы. Чем выше уровень идентификации, тем больше преимуществ у гражданина - и тем выше цена ошибки, утечки или отказа от участия. Логин восстановим. Биометрия - нет. Перед нами асимметричный риск, и компенсировать его асимметрию никто не спешит.

Социальная функция идентификаторов, как уже отмечалось, двойственна. С одной стороны, они радикально упрощают взаимодействие: заявление, которое раньше требовало визита в кабинет и очереди, теперь подаётся за несколько минут. С другой - те же инструменты работают механизмом сегрегации, причём не декларируемой, а структурной. Доступ к услуге, привязанный к цифровому профилю, отсекает тех, кто профиля не имеет. Происходит это не по решению чиновника и не по злому умыслу, а по умолчанию, самим дизайном системы. Вероятно, это самая коварная форма ограничения: человек не получает отказа. Он получает ошибку загрузки.

Позволим себе тезис посильнее. Риск цифровой идентификации никогда не был заключён в самой технологии. Технология нейтральна; пароль не знает, кто его набирает. Риск возникает там и тогда, где и когда безальтернативность технологического решения закрепляется регламентом или деловой практикой. Запись к врачу - только через приложение. Заявление на пособие - только через портал. Справка - только в электронном виде. Каждый такой регламент по отдельности выглядит разумно, даже прогрессивно. Но сумма этих «прогрессивных» решений даёт неожиданный результат: гражданин без смартфона и стабильного интернета выпадает из социальной инфраструктуры [19, с. 47].

Отдельно подчеркнём: речь вовсе не о маргинальных группах. По данным опроса, проведённого Финансовым университетом и НПФ «Социум» в 36 городах России, уверенно чувствуют себя в цифровой среде лишь 21,1 % граждан старше 60 лет - против 75,8 % среди молодёжи [17]. Это не «узкий круг лиц». Это миллионы людей, чья социальная жизнь так или иначе проходит через публичные услуги. И для каждого из них безальтернативность цифровой идентификации означает фактическое сужение круга прав.

Позиция автора по данному вопросу однозначна. Цифровая идентификация должна оставаться правом, а не обязанностью - до тех пор, пока законодатель не создаст гарантий, делающих отказ безопасным. Пока гарантий нет, каждый новый шаг к «полной цифровизации» углубляет разрыв между равенством формальным и равенством фактическим. Причём разрыв этот растёт не оттого, что кто-то целенаправленно нарушает закон, а оттого, что закон молчит.

3.2. Нормативная база РФ: коллизии и пробелы в защите прав граждан

Действующее российское законодательство в этой области построено по «мозаичному» принципу. Каждый фрагмент в отдельности выглядит разумно - но мозаика в целостную картину не складывается. Конституция РФ в статье 19 гарантирует равенство перед законом, в статье 33 закрепляет право на обращение в государственные органы [1]. Однако текст Конституции форму реализации этих прав не уточняет. Именно в этой, казалось бы, мелочи и скрывается вся проблема. Имеет ли право на обращение гражданин, не пользующийся электронными каналами? Формально - безусловно. Фактически - лишь если для него оставлена физическая альтернатива, доступность которой никто не обязан обеспечивать.

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» регулирует обработку сведений о гражданине, но статуса цифрового идентификатора как самостоятельного правового института - инструмента доступа к правам - не определяет [3]. Получается странная вещь: данные, образующие идентификатор, защищены; сам идентификатор как элемент конституционно значимого доступа юридически невидим. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи» регламентирует лишь один вид идентификации, оставляя за скобками пароли, биометрию, ЕСИА [4]. Каждый закон отвечает на свой узкий вопрос. На главный - что делать, если человек не хочет участвовать в этой системе? - не отвечает ни один.

Парадоксально, но прямой ответ частично всё же существует. Федеральный закон от 29.12.2022 № 572-ФЗ прямо устанавливает добровольность биометрической идентификации: отказ гражданина от сдачи биометрии не может служить основанием для отказа в предоставлении государственных услуг [5]. Федеральный закон № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» закрепляет за заявителем право выбирать форму обращения - электронную, личную или через представителя [6]. На бумаге конструкция выглядит безупречно. Декларации продуманы, гарантии проговорены. Но работает ли она за пределами текста нормативных актов?

Ответ, к сожалению, во многом отрицательный. Обоснование сводится к четырём пунктам.

Первое. ЕСИА - инфраструктура, на которую завязано практически всё государственное взаимодействие, - функционирует на основании постановления Правительства РФ от 03.11.2022 № 1948 [8]. Документ, по существу, технический: порядок регистрации, уровни учётных записей, правила подключения ведомств. Социальных гарантий в нём нет - и, строго говоря, их там быть не должно. Но именно поэтому возникает зона «правовой тишины»: главная точка входа в государственные услуги регулируется актом, не содержащим ни одного обязательства государства перед «нецифровым» гражданином.

Второе. Постановление Правительства РФ от 27.03.2023 № 478 закрепляет право на отказ от сбора биометрии через МФЦ и прямо декларирует: такой отказ не препятствует получению государственных услуг [9]. Механизм реализован - и это заслуга регулятора. Однако закон умалчивает о последствиях отказа для коммерческого сектора. Банк, работодатель, страховая компания - ни один из них прямым запретом на дискриминацию «нецифровых» клиентов не связан. 115-ФЗ требует идентификации клиента, но молчит о способах её осуществления [7]; трудовое законодательство молчит о способах кадрового документооборота [2]. Декларация о добровольности, адресованная одним лишь государственным органам, при расширяющейся практике частной биометрии превращается в фикцию.

Третье - и здесь, по убеждению автора, главная коллизия всей конструкции. Законодательство допускает альтернативные способы подтверждения личности, но реальную их доступность обеспечивать никого не обязывает. Допустить - не значит гарантировать. Регламент услуги может скромно упомянуть «личный приём», не уточнив ни часы работы, ни количество окон, ни территориальную доступность. В Волгоградской области, по наблюдениям автора, подобная формулировка нередко означает одно окно на район и очередь в несколько часов. Формальное право на альтернативу есть. Механизма реализации - нет. Это и есть пробел, который не закрывает ни 152-ФЗ, ни 572-ФЗ, ни какой-либо иной действующий акт.

И четвёртый элемент - отсутствие санкций. Ни один из перечисленных законов не предусматривает ответственности за фактическое принуждение к цифровой идентификации - за те случаи, когда «добровольный» отказ обставляется процедурными препятствиями. Норма без санкции в отечественной правоприменительной традиции, увы, остаётся декларацией, а не регулятором. Именно поэтому судебная практика, к которой далее переходит исследование, выступает компенсаторным механизмом: суды достраивают то, что не достроил законодатель.

3.3. Анализ случаев дискриминации при отказе от цифровой идентификации

Банковская сфера показательной оказывается по очевидной причине: именно там цифровая идентификация быстрее всего перестала быть опцией. Формально банк обязан идентифицировать клиента, но не обязан использовать для этого биометрию [7]. Норма ясна. Ясно и то, что на практике она часто остаётся формальностью: банковские приложения предлагают сдачу биометрии как путь «простой» и «безопасный», а альтернативы по умолчанию либо отсутствуют, либо скрыты в глубине настроек.

Показательно дело, рассмотренное Вологодским городским судом. Т-Банк включил в условия обслуживания пункт об автоматическом согласии на сбор биометрии: клиенту достаточно было продолжать пользоваться приложением. Суд решением от 19.07.2024 по делу № 2-978/2024 (2-11374/2023) признал этот пункт ничтожным, а согласие - недействительным [11]. Логика суда заслуживает отдельного разбора. Уведомление мелким шрифтом «продолжая, вы соглашаетесь» не образует свободного, информированного и однозначного волеизъявления. Иными словами, согласие, полученное «из единственного выхода», согласием не является. Апелляция вывод подтвердила: Вологодский областной суд в определении от 18.03.2025 по делу № 33-802/2025 особо подчеркнул, что реальной возможности отказаться от обработки биометрии, не отказываясь при этом от сервиса в целом, у клиента не было [12].

Ценность этого кейса двойная. Во-первых, он устанавливает важный стандарт: молчаливое согласие на цифровую идентификацию недействительно - что соответствует и статье 9 закона № 152-ФЗ [3]. Во-вторых - и здесь центральный пункт - он обнажает пределы судебной защиты. Суд защитил конкретного клиента от конкретной манипуляции. Запретить банку биометрию в принципе суд не может и не должен; обязать обеспечить удобную альтернативу каждому клиенту - тоже. Эта функция по природе своей законодательная. И пока законодатель её не выполняет, каждая судебная победа остаётся победой в отдельном деле, а не в системе.

Стоит учесть и общий фон: к сходным выводам давно пришла Судебная коллегия Верховного Суда РФ, ориентировавшая суды на то, что условия присоединения к сервису не вправе скрывать от гражданина существенные права [10]. Вологодское дело, думается, - прямое продолжение этой линии, только в новой технологической плоскости.

Другой кейс демонстрирует обратную сторону цифровизации банковского сервиса. Ивановский районный суд решением от 25.08.2025 по делу № 2-1021/2025 (М-495/2025) обязал банк восстановить клиентке доступ к дистанционному распоряжению денежными средствами: счёт был фактически заблокирован для онлайн-операций, а обращения в Банк России не помогли [14]. Человека исключили из привычной цифровой среды - и пришлось идти в суд, чтобы вернуться. Пример этот, как представляется, зеркалит проблему. Цифровизация без гарантий оставляет гражданина один на один и с навязанной технологией, и с её внезапным отключением.

Теперь - о трудовых отношениях. Трудовой кодекс не требует обязательного использования электронной подписи [2]. Читать это следует буквально: ЭП - не условие приёма на работу, а инструмент оформления части отношений. Однако внутренние регламенты компаний нередко переиначивают норму на свой лад. Полный переход на кадровый электронный документооборот без бумажной альтернативы делает выполнение трудовых функций невозможным для сотрудника, не готового или не имеющего технической возможности использовать ЭП. Согласие на КЭДО перестаёт быть выбором - оно становится условием доступа к рабочему месту.

Практика 2024–2025 годов этот перекос начинает выправлять. Первомайский районный суд г. Краснодара решением от 13.08.2024 по делу № 2-3978/24 сформулировал принципиальное

правило: согласие работника на переход к КЭДО должно быть получено на бумажном носителе до начала использования системы; электронное «само по себе» не считается [13]. Это не формализм, а осознанная защита слабой стороны трудовых отношений: работодатель, контролирующий всю цифровую инфраструктуру, не вправе одновременно выступать и инициатором перехода, и его исполнителем.

Определение Второго кассационного суда общей юрисдикции от 25.09.2025 по делу № 88-23802/2025 развивает ту же логику на ином участке: уведомление об увольнении направляется строго на адрес, предусмотренный договором, а произвольный выбор канала коммуникации лишает юридической силы даже электронный документ [15]. Смысл обоих решений прост и важен. Электронный формат - не панацея, а договорная конструкция, требующая взаимного согласия и предсказуемости. Цифровой канал не «лучше» бумажного; он равнозначен - но лишь тогда, когда обе стороны согласились на него заранее.

Впрочем, за пределами этих актов остаётся зона молчания. Компании, полностью отказавшиеся от бумажных носителей, по-прежнему создают риск дискриминации сотрудников, не готовых к цифровому взаимодействию. Суды решают проблему по частям и задним числом - после того, как нарушение уже произошло. Предотвратить его могла бы норма об обязательности альтернативного канала. Её, повторим, в законе нет.

Третий кейс - самый социально чувствительный. В ряде регионов получение социальных выплат и льгот привязано к цифровым платформам. Пенсионер без мобильного приложения вынужден либо обращаться за помощью к родственникам (что само по себе ставит его в зависимое положение), либо отказываться от льгот, на которые имеет полное право.

Постановление Правительства РФ от 27.03.2023 № 478 закрепляет право на отказ от сбора биометрии в МФЦ и декларирует, что отказ не препятствует получению государственных услуг [9]. Декларация хорошая. Практика - иная. МФЦ в регионах перегружены; очереди и ограниченное время работы добавляют сложностей. В Волгоградской области, по наблюдениям автора, часть мер социальной поддержки предоставляется преимущественно через региональные цифровые сервисы, а пиковые нагрузки на многофункциональные центры лишь усиливают разрыв между формальной гарантией и реальным доступом. Показательна и асимметрия усилий: чтобы «попасть в цифру», гражданину хватает пяти минут; чтобы остаться в «аналоге», нужны несколько часов, порой два визита, порой помощь постороннего человека. Государственная услуга формально открыта всем. Фактически - ценой, которую не каждый готов или способен заплатить.

Отметим деталь, которую обычно упускают. Речь не только о пожилых. В ту же категорию попадают жители дальних сёл с нестабильным интернетом, люди с инвалидностью по зрению, для которых интерфейсы часто недоступны, граждане без регистрации по месту жительства - и, наконец, те, кто принципиально не желает передавать биометрические данные в государственные базы. Такое волеизъявление, подчеркнём, закон допускает полностью [5]. Сегрегация «цифровой идентичности» - не проблема узкой группы. Это проблема всех, кто по любой причине оказался по другую сторону цифрового барьера.

Три сюжета - банковский, трудовой и социальный - на первый взгляд друг с другом не связаны. Банк, работодатель, региональный орган власти действуют в разных сферах и по разным мотивам. Но объединяет их одно: отсутствие чётких правил, гарантирующих равный доступ к услугам вне зависимости от способа идентификации. Ни злонамеренности, ни некомпетентности отдельных организаций здесь нет. Просто никто не обязан обеспечивать альтернативу - а потому альтернатива постепенно исчезает из практики. Судебная практика существование проблемы лишь косвенно подтверждает: она фиксирует отдельные нарушения, но системную причину устранить не в силах.

3.4. Проект федерального закона «О гарантиях аналогового доступа»: концепция и структура

Проект закона призван устранить выявленный пробел. Идея его проста и, по убеждению автора, давно назрела: закрепить право гражданина на получение любой публичной услуги в нецифровом формате - без дополнительных условий, ограничений и «санкций» за такой выбор.

Оговорим сразу, чего проект не делает. Он не тормозит цифровизацию. Не запрещает банкам развивать биометрию. Не заставляет государство содержать избыточные бумажные процедуры. Он лишь закрепляет правило сосуществования двух форматов - правило, которое сегодня существует в декларациях, но отсутствует в механизмах. Именно поэтому подход реалистичен: он не вступает в противоречие с уже действующей системой.

Основные положения проекта таковы.

Гарантия аналогового доступа. Отказ от цифровых идентификаторов не может служить основанием для отказа в предоставлении услуги - как государственной, так и публично значимой коммерческой (банковской, страховой, операторской). Подчеркнём: норма охватывает не только государственный сектор. Как показывает вологодское дело, основная зона риска давно находится на границе публичного и частного [11; 12].

Запрет на дискриминацию. Действия, ограничивающие права граждан из-за отказа от цифровых технологий, признаются незаконными и влекут административную ответственность. Здесь существующее регулирование сознательно раздвигается: санкции за нарушение порядка обработки персональных данных есть [3], а за «процедурное принуждение» к цифровой идентификации - нет.

Институт «цифровых омбудсменов». Региональная сеть специалистов, помогающих получать услуги и контролирующих соблюдение прав граждан. Это ключевая новелла проекта: она превращает право на альтернативу из декларации в работающий механизм - в том числе для граждан, не способных отстаивать интересы самостоятельно. Опыт ивановского дела [14] нагляден: гражданин сегодня сильно зависит от собственной юридической активности. Омбудсмен этот порог входа снижает.

Механизмы контроля. Обязательность альтернативных каналов в регламентах услуг - не в общем виде, а с конкретными параметрами: часы приёма, количество окон, территориальная доступность, сроки. Регламент, где альтернатива упомянута одним предложением, исполнением обязанности считаться не должен.

Структура проекта классическая, в пять глав. Глава 1 - общие положения и понятия. Глава 2 - права граждан на аналоговый доступ и запрет дискриминации. Глава 3 - обязанности органов власти и организаций. Глава 4 - статус и полномочия цифровых омбудсменов. Глава 5 - переходные положения. Выбор продиктован не эстетикой, а функцией: основная нагрузка приходится на главы 2–4, где закрепляются права, обязанности и контроль.

Отметим, что проект не существует в вакууме. Действующее регулирование частично уже движется в нужную сторону: 572-ФЗ устанавливает добровольность биометрии [5], 210-ФЗ - право выбора формы обращения [6], постановление № 478 - механизм отказа через МФЦ [9]. Но, как показано выше, эти нормы разрозненны, санкций не имеют и частный сектор не охватывают. Проект «О гарантиях аналогового доступа» систематизирует их, добавляет ответственность и расширяет сферу действия.

Представляется, что такой подход не только устранит выявленные пробелы, но и создаст устойчивый механизм защиты. Принципиально, что проект ценность цифровых технологий не отрицает - он задаёт правила их сосуществования с традиционными способами взаимодействия. Опыт вологодских судов показывает: правосудие уже движется в эту сторону, однако без законодательного закрепления каждая победа остаётся частным случаем. А право, как справедливо замечено ещё римскими юристами, от удачи истца зависеть не должно.

ЗАКЛЮЧЕНИЕ

Проведённое исследование позволяет сформулировать главный вывод с достаточной степенью уверенности: правовой пробел в регулировании цифровых идентификаторов в России носит не локальный, а системный характер. Проявляется он на трёх уровнях сразу - понятийном, институциональном и санкционном. На понятийном закон так и не определил цифровой идентификатор как самостоятельный правовой институт: данные, из которых он состоит, защищены, но сам идентификатор как инструмент доступа к правам юридически невидим. На институциональном уровне нет ни органа, ни механизма, отвечающих за реальную доступность нецифровых способов получения услуг. На санкционном - нет ответственности за фактическое принуждение к цифровой идентификации. Норма без санкции, как известно из общей теории права, работает плохо; норма без механизма реализации не работает вовсе.

При этом законодатель, казалось бы, нужные ответы уже дал. 572-ФЗ провозглашает добровольность биометрии, 210-ФЗ закрепляет право выбора формы обращения, постановление № 478 предусматривает механизм отказа через МФЦ. Как показал анализ, каждая из этих гарантий адресована исключительно государственному сектору. Банки, работодатели, страховые компании - то есть организации, с которыми гражданин взаимодействует ежедневно, - остаются вне периметра этих обязательств. Именно поэтому декларация о добровольности на практике нередко оказывается фикцией: гражданин формально свободен от биометрии, но фактически вынужден её сдавать, чтобы получить кредит, устроиться на работу или оформить полис.

Судебная практика в 2024–2025 годах стала важным компенсаторным механизмом. Решения Вологодского городского суда, Ивановского районного суда, Первомайского районного суда Краснодара и кассационные акты показывают: суды последовательно защищают право гражданина на свободное и информированное волеизъявление, не допускают молчаливого согласия и требуют предсказуемости цифровых процедур. Однако судебная защита по своей природе реактивна: она устраняет последствия, но не предотвращает нарушения. Пока не появится законодательно закреплённый механизм гарантий и ответственности, каждое дело будет оставаться частным случаем, а не элементом системы.

Проект федерального закона «О гарантиях аналогового доступа» призван закрыть этот разрыв. Его ключевые преимущества - в универсальности (охват и публичного, и частного сектора), конкретике (обязательные параметры альтернативных каналов) и наличии санкций. Кроме того, институт цифровых омбудсменов снижает порог доступа к защите прав: помощь становится доступной тем, кто не способен самостоятельно пройти бюрократические процедуры.

Практическая значимость исследования состоит в том, что оно не просто фиксирует проблему, а предлагает её системное решение. Право на аналоговый доступ не означает отказа от цифровизации - оно означает, что цифровизация не должна становиться условием реализации конституционных прав. Равенство перед законом и право на обращение в органы власти должны быть одинаково доступны всем - независимо от наличия смартфона, биометрического профиля или навыков работы с цифровыми сервисами.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

Нормативные правовые акты

1. Конституция Российской Федерации: принята всенародным голосованием 12.12.1993 (с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // Официальный интернет-портал правовой информации. - URL: http://pravo.gov.ru/(дата обращения: 05.10.2026).
2. Трудовой кодекс Российской Федерации: Федеральный закон от 30.12.2001 № 197-ФЗ (ред. от 2025) // Собрание законодательства РФ. - 2002. - № 1 (ч. I). - Ст. 3.
3. О персональных данных: Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 2025) // Собрание законодательства РФ. - 2006. - № 31 (ч. I). - Ст. 3451.
4. Об электронной подписи: Федеральный закон от 06.04.2011 № 63-ФЗ (ред. от 2025) // Собрание законодательства РФ. - 2011. - № 15. - Ст. 2036.
5. Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации: Федеральный закон от 29.12.2022 № 572-ФЗ (ред. от 2025) // Собрание законодательства РФ. - 2023. - № 1 (ч. I). - Ст. 17.
6. Об организации предоставления государственных и муниципальных услуг: Федеральный закон от 27.07.2010 № 210-ФЗ (ред. от 2025) // Собрание законодательства РФ. - 2010. - № 31. - Ст. 4179.
7. О противодействии легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма: Федеральный закон от 07.08.2001 № 115-ФЗ (ред. от 2025) // Собрание законодательства РФ. - 2001. - № 33 (ч. I). - Ст. 3418.
8. Об утверждении Положения о единой системе идентификации и аутентификации и предоставления государственной услуги по регистрации и аутентификации физических лиц в единой системе идентификации и аутентификации: постановление Правительства РФ от 07.10.2019 № 1287 (ред. от 2025) // Собрание законодательства РФ. - 2019. - № 42. - Ст. 5864.
9. Об установлении случая отказа физического лица от сбора, хранения и обработки его биометрических персональных данных: постановление Правительства РФ от 27.03.2023 № 478 // Официальный интернет-портал правовой информации. - URL: http://pravo.gov.ru/ (дата обращения: 05.10.2026).

Материалы судебной практики

10. Определение Судебной коллегии по гражданским делам Верховного Суда РФ от 11.02.2020 № 78-КГ19-52 // Официальный сайт Верховного Суда РФ. - URL:http://vsrf.ru/ (дата обращения: 05.10.2026).
11. Решение Вологодского городского суда Вологодской области от 19.07.2024 по делу № 2-978/2024 (2-11374/2023) // СудАкт.ру. - URL: https://sudact.ru/ (дата обращения: 05.10.2026).
12. Апелляционное определение Вологодского областного суда от 18.03.2025 по делу № 33-802/2025 // СудАкт.ру. - URL:https://sudact.ru/ (дата обращения: 05.10.2026).
13. Решение Первомайского районного суда г. Краснодара от 13.08.2024 по делу № 2-3978/24 // СудАкт.ру. - URL: https://sudact.ru/ (дата обращения: 05.10.2026).
14. Решение Ивановского районного суда Ивановской области от 25.08.2025 по делу № 2-1021/2025 (М-495/2025) // СудАкт.ру. - URL:https://sudact.ru/ (дата обращения: 05.10.2026).
15. Определение Второго кассационного суда общей юрисдикции от 25.09.2025 по делу № 88-23802/2025 // Клерк.ру. - URL: https://www.klerk.ru/ (дата обращения: 05.10.2026).

16. Биометрия в 2026: как государство и бизнес используют технологии // Коммерсантъ. - 2026. - 19 мая. - URL: https://www.kommersant.ru/doc/8671574 (дата обращения: 05.10.2026).

17. Маглели, П. А. Как преодолеть неравенство цифровизации в России / П. А. Маглели // Молодой учёный. - 2025. - № 49 (600). - URL: https://moluch.ru/archive/600/130929 (дата обращения: 05.10.2026).

18. Менщикова, Н. Л. Использование цифровых сервисов для записи на приём к врачу пожилыми людьми: результаты социологического исследования / Н. Л. Менщикова // Современные проблемы здравоохранения и медицинской статистики. - 2025. - № 4. - С. 269–283.

19. Петрова, К. А. Защита конфиденциальности данных и прав личности в цифровой среде: правовое регулирование и практические механизмы / К. А. Петрова // Научные записки молодых исследователей. - 2025. - Т. 13, № 2. - С. 46–53.

20. Поволоцкий, В. «Биометрия - не таблетка от всего»: интервью / В. Поволоцкий // Российская газета. - 2026. - 24 авг. - URL: https://rg.ru/2026/08/24/glava-cbt-vladislav-povolockij-biometriia-ne-tabletka-ot-vsego.html (дата обращения: 05.10.2026).

21. OECD Digital Economy Outlook 2021. - Paris: OECD Publishing, 2021. - 235 p.