

УДК 342.9

DOI: 10.34670/AR.2026.50.55.007

Цифровой риск-ориентированный государственный контроль и пределы юридической ответственности контролируемых лиц в условиях становления цифрового общества

Макулова Аделина Олеговна

Аспирант,
Университет «Синергия»,
125190, Российская Федерация, Москва,
Ленинградский просп., 80 Г;
e-mail: adelina.makulova@mail.ru

Аннотация

В статье исследуется влияние цифровизации контрольно-надзорной деятельности на трансформацию оснований, процедур и пределов юридической ответственности контролируемых лиц. Актуальность темы обусловлена тем, что современная модель государственного контроля в России строится на сочетании риск-ориентированного подхода, профилактики нарушений, платформенных решений и дистанционных форм взаимодействия между государством и участниками регулируемых отношений. Цель исследования состоит в выявлении того, каким образом цифровые инструменты изменяют содержание контрольной функции государства и какие правовые гарантии должны сопровождать применение данных, алгоритмов и автоматизированных решений при привлечении к ответственности. Методологическую основу составили формально-юридический, системный, сравнительно-правовой и функциональный методы. Научная новизна работы заключается в обосновании положения о том, что цифровизация меняет не только форму контроля, но и саму юридическую конструкцию ответственности: от последующего карательного реагирования происходит переход к непрерывному аналитическому наблюдению, профилактике, цифровой фиксации фактов и удалённому процессуальному взаимодействию. Обосновывается вывод о недопустимости полностью автоматизированного привлечения к юридической ответственности без сохранения права на объяснение, опровержение цифровых доказательств и рассмотрение дела уполномоченным должностным лицом либо судом. Предлагаются направления совершенствования законодательства: закрепление требований к проверяемости алгоритмов, специальный режим использования цифровых доказательств в контрольно-надзорном производстве, унификация правил дистанционных процессуальных действий и усиление гарантий защиты персональных данных.

Для цитирования в научных исследованиях

Макулова А.О. Цифровой риск-ориентированный государственный контроль и пределы юридической ответственности контролируемых лиц в условиях становления цифрового общества // Вопросы российского и международного права. 2026. Том 16. № 4А. С. 62-71. DOI: 10.34670/AR.2026.50.55.007

Ключевые слова

Государственный контроль; контрольно-надзорная деятельность; юридическая ответственность; цифровое общество; цифровизация; риск-ориентированный подход; административная ответственность; персональные данные; автоматизированные решения; цифровые доказательства.

Введение

Становление цифрового общества в России сопровождается качественным изменением механизмов публичного управления. На уровне стратегического планирования государство связывает развитие цифровых технологий с модернизацией управления, повышением качества публичных услуг, внедрением данных и искусственного интеллекта в деятельность органов власти [Указ Президента РФ № 203, 2017; Указ Президента РФ № 490, 2019]. В этой логике реформируется и контрольная (надзорная) деятельность, которая постепенно перестаёт быть исключительно инструментом последующего выявления нарушений и всё в большей степени приобретает признаки постоянного анализа риска, профилактики, дистанционного мониторинга и платформенного сопровождения [Федеральный закон № 248-ФЗ, 2020; Постановление Правительства РФ № 604, 2021; Минцифры России, [www...](#); Единый реестр контрольных (надзорных) мероприятий, [www...](#)].

При этом проблема юридической ответственности в условиях цифрового контроля приобретает особую остроту. Чем активнее государство использует цифровой след, автоматическую обработку сведений, удалённые форматы мероприятий и алгоритмы отбора объектов контроля, тем заметнее меняются вопросы о составе правонарушения, допустимости доказательств, распределении бремени доказывания, пределах усмотрения должностного лица и гарантиях прав контролируемого лица [Федеральный закон № 152-ФЗ, 2006; Захаров, Режецкая, 2025; Зайцев, 2025; Рымкевич, 2023; Тотурбиев, 2025; Кружилин, 2025; Плаксин, Абузярова, Алимпеев и др., 2026]. В научной литературе справедливо отмечается, что цифровизация публичного управления и административной юрисдикции не устраняет традиционных принципов законности, вины, соразмерности и процессуальной справедливости, а, напротив, требует их дополнительной институционализации [Захаров, Режецкая, 2025; Зайцев, 2025; Рымкевич, 2023; Тотурбиев, 2025; Кружилин, 2025].

Цель настоящей статьи — определить, каким образом цифровизация государственного контроля трансформирует юридическую ответственность контролируемых лиц и какие правовые пределы должны быть установлены для автоматизации контрольных процедур. Для достижения поставленной цели необходимо: во-первых, раскрыть нормативные предпосылки цифровизации контроля; во-вторых, показать влияние цифровых инструментов на конструкцию юридической ответственности; в-третьих, сформулировать предложения по совершенствованию законодательства и правоприменительной практики.

Нормативная архитектура цифрового государственного контроля

Современная правовая модель цифрового государственного контроля формируется на пересечении нескольких блоков нормативного регулирования. Во-первых, это стратегические документы, в которых цифровая трансформация рассматривается как долгосрочный вектор развития государства. Стратегия развития информационного общества в Российской Федерации

на 2017–2030 годы закрепила курс на широкое внедрение цифровых технологий в управление и общественные отношения [Указ Президента РФ № 203, 2017]. Национальная стратегия развития искусственного интеллекта на период до 2030 года дополнительно обозначила необходимость использования систем интеллектуального анализа данных в публичной сфере, включая управление и контроль [Указ Президента РФ № 490, 2019].

Во-вторых, центральное место занимает Федеральный закон от 31.07.2020 № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации». Именно этот закон институционально закрепит приоритет профилактики, риск-ориентированного подхода, стандартизацию контрольных процедур, цифровую фиксацию значимых действий и создание единого реестра контрольных (надзорных) мероприятий как федеральной государственной информационной системы [Федеральный закон № 248-ФЗ, 2020]. Правила формирования и ведения данного реестра утверждены постановлением Правительства РФ от 16.04.2021 № 604 [Постановление Правительства РФ № 604, 2021]. Следовательно, цифровизация контроля в настоящее время перестала быть факультативной практикой отдельных ведомств и получила нормативно обязательный характер.

Во-третьих, цифровой контроль невозможен вне общего информационно-правового режима. Его базу образуют Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», определяющий общие начала обращения информации, функционирования государственных информационных систем и защиты информационных ресурсов [Федеральный закон № 149-ФЗ, 2006], а также Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», который устанавливает пределы обработки персональных данных, включая случаи автоматизированного принятия решений, способных повлечь юридические последствия для граждан [Федеральный закон № 152-ФЗ, 2006]. Наконец, Федеральный закон от 31.07.2020 № 258-ФЗ об экспериментальных правовых режимах создаёт возможность тестирования новых цифровых решений и алгоритмов в регулируемой среде [Федеральный закон № 258-ФЗ, 2020].

Платформенная инфраструктура контрольно-надзорной деятельности уже сегодня включает не только единый реестр контрольных мероприятий, но и специальные цифровые сервисы. На портале контрольно-надзорной деятельности и на странице Минцифры представлено мобильное приложение «Инспектор», предназначенное для проведения контрольных и профилактических мероприятий в дистанционном режиме, включая видео-конференц-связь, фото- и видеофиксацию нарушений, работу с чек-листами и контроль геолокации [Минцифры России, www.mtc.gov.ru]. Сам по себе этот факт свидетельствует о переходе контроля к модели, в которой цифровая среда становится не внешним средством оформления результатов, а непосредственным пространством осуществления надзорной функции.

Следовательно, цифровой государственный контроль в современной России представляет собой не набор отдельных ИТ-решений, а целостную правовую конструкцию, где данные, реестры, алгоритмы и удалённые интерфейсы становятся элементами правовой процедуры. Именно поэтому вопрос о юридической ответственности уже нельзя рассматривать в отрыве от цифровой формы производства.

Как цифровизация меняет юридическую конструкцию ответственности

Традиционно юридическая ответственность в контрольно-надзорной сфере воспринималась как результат выявления нарушения в ходе проверки, составления процессуальных документов

и последующего назначения санкции. Однако цифровизация меняет как минимум четыре элемента этой конструкции.

Во-первых, трансформируется момент обнаружения нарушения. Если прежде ключевое значение имело личное взаимодействие инспектора с объектом контроля, то теперь нарушение всё чаще выявляется посредством анализа цифрового следа: сведений из реестров, сопоставления данных нескольких государственных систем, дистанционного наблюдения, фото- и видеофиксации, а также удалённого обмена документами [Федеральный закон № 248-ФЗ, 2020; Постановление Правительства РФ № 604, 2021; Минцифры России, [www...](http://www.mcs.gov.ru); Единый реестр контрольных (надзорных) мероприятий, [www...](http://www.frc.gov.ru)]. Это означает, что событие, имеющее юридическое значение, может быть сформировано не единичным актом восприятия должностного лица, а совокупностью цифровых сигналов, обработанных в информационной системе.

Во-вторых, меняется доказательственная база. Цифровые доказательства в сфере контроля включают электронные документы, записи из государственных информационных систем, данные аудио- и видеосъёмки, метаданные, сведения о маршрутах и времени совершения действий, результаты автоматизированной сверки показателей. Такие доказательства обладают высокой воспроизводимостью, но одновременно требуют подтверждения происхождения, целостности, неизменности и относимости. Без специального нормативного режима для цифровых доказательств возрастает риск того, что информационная система будет восприниматься как самодостаточный носитель истины, хотя любая цифровая запись создаётся, хранится и интерпретируется через конкретную технологическую архитектуру и конкретный алгоритм.

В-третьих, изменяется соотношение профилактики и наказания. Федеральный закон № 248-ФЗ нормативно усилил профилактические инструменты: информирование, консультирование, профилактический визит, предостережение и иные формы предупреждения нарушений [Федеральный закон № 248-ФЗ, 2020]. В цифровой среде эта линия получает дополнительное развитие: система способна заранее сигнализировать о риске несоблюдения обязательных требований, а надзорный орган — направлять адресные уведомления и рекомендации. Тем самым юридическая ответственность перестаёт быть единственным и даже главным способом воздействия. Она должна рассматриваться как завершающий элемент более широкой модели правового комплаенса, в которой цифровой контроль сначала предупреждает, затем фиксирует и лишь после этого, при наличии достаточных оснований, санкционирует.

В-четвёртых, меняется процессуальное положение контролируемого лица. С одной стороны, цифровые платформы расширяют возможности участия: позволяют оперативно получать уведомления, направлять документы, подключаться к дистанционным мероприятиям, знакомиться с данными реестра и отслеживать процессуальный статус дела [Постановление Правительства РФ № 604, 2021; Минцифры России, [www...](http://www.mcs.gov.ru); Единый реестр контрольных (надзорных) мероприятий, [www...](http://www.frc.gov.ru)]. С другой стороны, возрастает опасность «скрытой асимметрии», когда государственный орган располагает массивом интегрированных данных и алгоритмических профилей риска, а контролируемое лицо не имеет информации о том, на основании каких критериев оно было отнесено к группе повышенного риска либо включено в план контрольных действий. В такой ситуации формальное сохранение права на обжалование не компенсирует дефицит прозрачности.

Таким образом, цифровизация ведёт к смещению центра тяжести в конструкции ответственности: от очного выявления нарушения и бумажной фиксации фактов — к

аналитической модели, в которой важнейшую роль начинают играть данные, их технологическая обработка и архитектура информационных систем. Именно это обстоятельство требует переосмысления пределов автоматизации.

Пределы автоматизации: законность, вина, персональные данные и право на человеческое решение

Несмотря на очевидные преимущества цифровизации, автоматизация контрольных процедур не может быть безграничной. В публично-правовой сфере она ограничивается как общими принципами юридической ответственности, так и специальными требованиями законодательства о данных и судебными позициями по делам, связанным с автоматической фиксацией правонарушений.

Прежде всего, для привлечения к юридической ответственности недостаточно установить лишь статистически значимую вероятность нарушения. Алгоритм может использоваться для категорирования риска, отбора объектов контроля, приоритизации ресурсов, но не должен подменять собой юридическую квалификацию деяния. Юридическая ответственность предполагает наличие нормативного основания, установленного события нарушения, надлежащего субъекта, причинной связи, а в предусмотренных случаях — вины. Алгоритмический вывод о «подозрительном поведении» сам по себе этим требованиям не равен.

Особое значение имеет законодательство о персональных данных. Федеральный закон № 152-ФЗ прямо устанавливает, что решение, порождающее юридические последствия для субъекта персональных данных либо иным образом затрагивающее его права и законные интересы, не может основываться исключительно на автоматизированной обработке персональных данных, если отсутствует письменное согласие субъекта или специальное федеральное законодательное основание [Федеральный закон № 152-ФЗ, 2006]. Более того, оператор обязан разъяснить порядок принятия такого решения, его возможные юридические последствия и предоставить возможность заявить возражения [Федеральный закон № 152-ФЗ, 2006]. Для контрольно-надзорной деятельности эта норма имеет системообразующее значение: цифровой профиль риска, автоматическая сверка данных, машинное выявление несоответствий могут служить основанием для дальнейших процессуальных действий, но не должны превращаться в окончательное и непререкаемое решение о виновности.

Правовая позиция о недопустимости подмены правовой оценки автоматической фиксацией подтверждается и конституционно-судебной практикой. Рассматривая дела, связанные с особым порядком привлечения к административной ответственности при автоматической фиксации правонарушений, Конституционный Суд Российской Федерации исходил из того, что применение технических средств не устраняет необходимость проверки обстоятельств дела, возможности опровержения презумпции участия собственника и судебного контроля за выводами публичной власти [Постановление КС РФ № 42-П, 2023]. Хотя указанные позиции сформулированы применительно к делам о нарушениях правил дорожного движения, их значение шире: автоматизация допустима как средство фиксации и предварительной квалификации, но не как замена правосудию и процессуальным гарантиям.

Не менее важен вопрос объяснимости алгоритма. В практике государственного контроля уже используются цифровые модели, формирующие профили риска и влияющие на частоту либо интенсивность вмешательства государства. Если критерии такого категорирования закрыты, изменчивы или не поддаются внешней проверке, возникает угроза скрытой

дискриминации, системных ошибок и невозможности эффективного обжалования. Отсюда следует, что алгоритмы, применяемые в контрольной сфере, должны отвечать минимум четырём требованиям: нормативной определённости цели; документированности источников данных; возможности последующего аудита; процессуальной раскрываемости в части, необходимой для защиты прав контролируемого лица.

Наконец, цифровой контроль неизбежно связан с обработкой значительных массивов данных, включая персональные данные, коммерческую информацию и служебные сведения. В этих условиях принцип пропорциональности приобретает особое значение. Государство вправе собирать и интегрировать лишь те данные, которые действительно необходимы для реализации контрольной функции, а срок хранения, объём доступа и режим межведомственного обмена должны быть нормативно определены. Иначе существует риск превращения контрольно-надзорной деятельности в режим тотального цифрового наблюдения, не ограниченного предметом конкретного контроля.

Направления совершенствования законодательства и правоприменения

Представляется, что дальнейшее развитие цифрового государственного контроля должно сопровождаться одновременным усилением правовых гарантий. В противном случае эффективность цифровых сервисов будет достигаться ценой размывания стандартов законности и доверия к публичной власти.

Во-первых, в законодательстве о государственном контроле целесообразно прямо закрепить понятие цифрового доказательства и минимальные требования к его допустимости. К таким требованиям следует отнести идентифицируемость источника, возможность проверки времени и способа формирования записи, подтверждение отсутствия несанкционированного изменения, а также обеспеченную для контролируемого лица возможность ознакомиться с исходным массивом данных, а не только с выводом информационной системы.

Во-вторых, требуется специальное регулирование алгоритмов, используемых для риск-категорирования и инициирования контрольных процедур. Такое регулирование должно включать обязательную документацию модели, описание применяемых критериев, периодическую валидацию на предмет ошибок и предвзятости, а также внешний аудит в случаях, когда результат алгоритмической оценки влияет на объём публичного вмешательства. Использование искусственного интеллекта в контрольной сфере возможно и оправданно, но лишь при сохранении принципа контролируемости технологии человеком [Указ Президента РФ № 490, 2019; Федеральный закон № 258-ФЗ, 2020].

В-третьих, необходимо унифицировать правила дистанционных процессуальных действий. Практика применения мобильного приложения «Инспектор» и иных цифровых сервисов показывает, что удалённое взаимодействие уже стало частью повседневной надзорной работы [Минцифры России, www...]. Однако, чем шире используются ВКС, электронные кабинеты, цифровая фото- и видеофиксация, тем больше потребность в единых правилах идентификации участников, подтверждения их полномочий, фиксации процессуальных возражений, обеспечения непрерывности записи и хранения материалов.

В-четвёртых, следует усилить гарантии информированности контролируемого лица. Лицу, в отношении которого применяются цифровые инструменты анализа риска, должно быть доступно понимание того, какие сведения были использованы, каков нормативный источник соответствующей обязанности, по какой причине инициировано контрольное действие и каким

образом можно оспорить как фактические данные, так и способ их алгоритмической обработки. Эта гарантия прямо вытекает из общих начал надлежащей административной процедуры и поддерживается законодательством о персональных данных [Федеральный закон № 152-ФЗ, 2006].

В-пятых, необходимо синхронизировать реформу контрольно-надзорной деятельности с законодательством об административных правонарушениях и иными видами юридической ответственности. Научно обоснованно отмечается, что несогласованность процедур контроля и последующего юрисдикционного реагирования ведёт к правовой неопределённости, особенно в цифровой среде, где граница между профилактикой, выявлением и доказыванием нарушения становится более подвижной [Зайцев, 2025; Кружилин, 2025]. Следовательно, цифровизация не должна развиваться фрагментарно: ей требуется межотраслевая юридическая настройка.

Заключение

Проведённый анализ позволяет сделать несколько выводов. Во-первых, цифровизация государственного контроля в Российской Федерации уже приобрела нормативно завершённые очертания: она опирается на стратегические акты, Федеральный закон № 248-ФЗ, систему государственных реестров и специализированные цифровые сервисы [Указ Президента РФ № 203, 2017; Указ Президента РФ № 490, 2019; Федеральный закон № 248-ФЗ, 2020; Постановление Правительства РФ № 604, 2021; Минцифры России, [www...](#); Единый реестр контрольных (надзорных) мероприятий, [www...](#)]. Во-вторых, цифровая трансформация изменяет не только технику осуществления контроля, но и саму юридическую конструкцию ответственности, поскольку ключевое значение начинают иметь данные, их аналитическая обработка, дистанционная фиксация фактов и платформенная процессуальная коммуникация. Во-третьих, юридическая ответственность в цифровой среде не может строиться на презумпции безошибочности информационной системы. Алгоритмы и автоматизированные инструменты допустимы как средство выявления риска и подготовки решения, но не как его безусловная замена.

Отсюда вытекает общий теоретический и практический вывод: в условиях становления цифрового общества главный вопрос заключается не в том, следует ли цифровизировать государственный контроль, а в том, как обеспечить правовую совместимость цифровой эффективности и конституционных гарантий. Оптимальная модель состоит в сочетании риск-ориентированного и профилактического цифрового контроля с обязательным сохранением человеческого правового суждения, проверяемости алгоритмов, защиты персональных данных и доступности эффективного обжалования. Именно такая модель способна обеспечить баланс публичных интересов, интересов безопасности и прав контролируемых лиц.

Библиография

1. Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы». URL: <https://www.kremlin.ru/acts/bank/41919> (дата обращения: 01.02.2026).
2. Указ Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации». URL: <https://www.kremlin.ru/acts/bank/44731> (дата обращения: 01.02.2026).
3. Федеральный закон от 31.07.2020 № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации». URL: <https://publication.pravo.gov.ru/document/view/0001202007310018> (дата обращения: 01.02.2026).
4. Постановление Правительства РФ от 16.04.2021 № 604 «Об утверждении Правил формирования и ведения единого реестра контрольных (надзорных) мероприятий». URL:

- <https://publication.pravo.gov.ru/Document/View/0001202104210021> (дата обращения: 01.02.2026).
5. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». URL: <https://www.kremlin.ru/acts/bank/24157> (дата обращения: 05.02.2026).
 6. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных». URL: <https://letters.kremlin.ru/info-service/acts/9> (дата обращения: 05.02.2026).
 7. Федеральный закон от 31.07.2020 № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации». URL: <https://publication.pravo.gov.ru/Document/View/0001202007310024> (дата обращения: 16.03.2026).
 8. Мобильное приложение «Инспектор» // Министерство цифрового развития, связи и массовых коммуникаций РФ. URL: <https://digital.gov.ru/activity/czifrovizaciya-gosudarstva/czifrovaya-transformaciya/czifrovyie-platformy-i-resheniya-dlya-gosorganov/cifrovizaciya-kontrolno-nadzornoj-deyatelnosti/mobilnoe-prilozhenie-inspektor> (дата обращения: 16.03.2026).
 9. Единый реестр контрольных (надзорных) мероприятий. URL: <https://proverki.gov.ru/> (дата обращения: 16.03.2026).
 10. Захаров И. В., Режецкая А. И. Цифровизация публичного управления: правовые основы становления и развития // Труды по интеллектуальной собственности. 2025. Т. 53. № 2. URL: <https://tis.hse.ru/article/view/27357> (дата обращения: 16.03.2026).
 11. Зайцев И. А. Административная юрисдикция в условиях цифровизации // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2025. № 1 (69). С. 73–82. URL: <https://cyberleninka.ru/article/n/administrativnaya-yurisdiksiya-v-usloviyah-tsifrovizatsii> (дата обращения: 16.03.2026).
 12. Рымкевич Я. А. Юридическая ответственность в цифровом пространстве // Образование и право. 2023. № 7. С. 436–440. URL: <https://cyberleninka.ru/article/n/yuridicheskaya-otvetstvennost-v-tsifrovom-prostranstve> (дата обращения: 16.03.2026).
 13. Тотурбиев А. А. Совершенствование государственного контроля в условиях цифровизации // Вестник науки. 2025. Т. 2. № 3 (84). С. 245–255. URL: <https://cyberleninka.ru/article/n/sovershenstvovanie-gosudarstvennogo-kontrolya-v-usloviyah-tsifrovizatsii> (дата обращения: 16.03.2026).
 14. Кружилин В. С. Синхронизация реформирования правовой основы контрольно-надзорной деятельности и законодательства об административных правонарушениях: вопросы теории и практики // Государственная служба и кадры. 2025. URL: <https://cyberleninka.ru/article/n/sinhronizatsiya-reformirovaniya-pravovoy-osnovy-kontrolno-nadzornoj-deyatelnosti-i-zakonodatelstva-ob-administrativnyh> (дата обращения: 01.04.2026).
 15. Плаксин С. М., Абузярова И. А., Алимпеев Д. Р. и др. Контрольно-надзорная и разрешительная деятельность в Российской Федерации. Мировой опыт применения механизмов контрольно-надзорной деятельности. Аналитический доклад – 2025. М.: Издательский дом НИУ ВШЭ, 2026. URL: <https://publications.hse.ru/view/1137108772> (дата обращения: 16.03.2026).
 16. Постановление Конституционного Суда РФ от 17.07.2023 № 42-П «По делу о проверке конституционности части 2 статьи 1.7 Кодекса Российской Федерации об административных правонарушениях...». URL: https://www.consultant.ru/document/cons_doc_LAW_452324/ (дата обращения: 16.03.2026).

Digital Risk-Oriented State Control and the Limits of Legal Liability of Controlled Persons in the Context of the Formation of a Digital Society

Adelina O. Makulova

Postgraduate Student,
Synergy University,
125190, 80 G, Leningradskiy ave., Moscow, Russian Federation;
e-mail: adelina.makulova@mail.ru

Abstract

The article examines the impact of the digitalization of control and supervisory activities on the transformation of the grounds, procedures, and limits of legal liability of controlled persons. The relevance of the topic is conditioned by the fact that the modern model of state control in Russia is

built on a combination of a risk-oriented approach, prevention of violations, platform solutions, and remote forms of interaction between the state and participants in regulated relations. The aim of the study is to identify how digital tools change the content of the state control function and what legal guarantees should accompany the use of data, algorithms, and automated decisions when holding persons liable. The methodological basis was formed by formal-legal, systemic, comparative-legal, and functional methods. The scientific novelty of the work lies in substantiating the proposition that digitalization changes not only the form of control but also the very legal construction of liability: there is a transition from subsequent punitive response to continuous analytical observation, prevention, digital recording of facts, and remote procedural interaction. A conclusion is substantiated regarding the inadmissibility of fully automated bringing to legal liability without preserving the right to explanation, refutation of digital evidence, and consideration of the case by an authorized official or court. Directions for improving legislation are proposed: the consolidation of requirements for the verifiability of algorithms, a special regime for the use of digital evidence in control and supervisory proceedings, unification of the rules of remote procedural actions, and strengthening guarantees for the protection of personal data.

For citation

Makulova A.O. (2026) Tsifrovoy risk-orientirovanny gosudarstvennyy kontrol' i predely yuridicheskoy otvetstvennosti kontroliruemyykh lits v usloviyakh stanovleniya tsifrovogo obshchestva [Digital Risk-Oriented State Control and the Limits of Legal Liability of Controlled Persons in the Context of the Formation of a Digital Society]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 16 (4A), pp. 62-71. DOI: 10.34670/AR.2026.50.55.007

Keywords

State control, control and supervisory activities, legal liability, digital society, digitalization, risk-oriented approach, administrative liability, personal data, automated decisions, digital evidence.

References

1. Ukaz Prezidenta RF ot 09.05.2017 № 203 «O Strategii razvitiya informatsionnogo obshchestva v Rossiyskoy Federatsii na 2017–2030 gody» [Decree of the President of the Russian Federation No. 203 of 09.05.2017 "On the Strategy for the Development of the Information Society in the Russian Federation for 2017–2030"]. Available at: <https://www.kremlin.ru/acts/bank/41919>
2. Ukaz Prezidenta RF ot 10.10.2019 № 490 «O razvitii iskusstvennogo intellekta v Rossiyskoy Federatsii» [Decree of the President of the Russian Federation No. 490 of 10.10.2019 "On the Development of Artificial Intelligence in the Russian Federation"]. Available at: <https://www.kremlin.ru/acts/bank/44731>
3. Federal'nyy zakon ot 31.07.2020 № 248-FZ «O gosudarstvennom kontrole (nadzore) i munitsipal'nom kontrole v Rossiyskoy Federatsii» [Federal Law No. 248-FZ of 31.07.2020 "On State Control (Supervision) and Municipal Control in the Russian Federation"]. Available at: <https://publication.pravo.gov.ru/document/view/0001202007310018>
4. Postanovleniye Pravitel'stva RF ot 16.04.2021 № 604 «Ob utverzhenii Pravil formirovaniya i vedeniya yedinogo reyestra kontrol'nykh (nadzornykh) meropriyatiy» [Decree of the Government of the Russian Federation No. 604 of 16.04.2021 "On Approval of the Rules for the Formation and Maintenance of the Unified Register of Control (Supervisory) Measures"]. Available at: <https://publication.pravo.gov.ru/Document/View/0001202104210021>
5. Federal'nyy zakon ot 27.07.2006 № 149-FZ «Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii» [Federal Law No. 149-FZ of 27.07.2006 "On Information, Information Technologies and Protection of Information"]. Available at: <https://www.kremlin.ru/acts/bank/24157>
6. Federal'nyy zakon ot 27.07.2006 № 152-FZ «O personal'nykh dannykh» [Federal Law No. 152-FZ of 27.07.2006 "On Personal Data"]. Available at: <https://letters.kremlin.ru/info-service/acts/9>
7. Federal'nyy zakon ot 31.07.2020 № 258-FZ «Ob eksperimental'nykh pravovykh rezhimakh v sfere tsifrovyykh innovatsiy

- v Rossiyskoy Federatsii» [Federal Law No. 258-FZ of 31.07.2020 "On Experimental Legal Regimes in the Sphere of Digital Innovations in the Russian Federation"]. Available at: <https://publication.pravo.gov.ru/Document/View/0001202007310024>
8. Mobil'noye prilozheniye «Inspektor» [Mobile Application "Inspector"]. (n.d.). *Ministry of Digital Development, Communications and Mass Media of the Russian Federation*. Available at: <https://digital.gov.ru/activity/czifrovizacziya-gosudarstva/czifrovaya-transformacziya/czifrovye-platformy-i-resheniya-dlya-gosorganov/cifrovizaciya-kontrolno-nadzornoy-deyatelnosti/mobilnoe-prilozhenie-inspektor>
 9. Yedinyy reyestr kontrol'nykh (nadzornyykh) meropriyatiy [Unified Register of Control (Supervisory) Measures]. (n.d.). Available at: <https://proverki.gov.ru/>
 10. Zakharov I.V., Rezhetskaya A.I. (2025). Tsifrovizatsiya publichnogo upravleniya: pravovyye osnovy stanovleniya i razvitiya [Digitalisation of Public Administration: Legal Foundations of Formation and Development]. *Trudy po intellektual'noy sobstvennosti*, 53(2). Available at: <https://tis.hse.ru/article/view/27357>
 11. Zaytsev I.A. (2025). Administrativnaya yurisdiksiya v usloviyakh tsifrovizatsii [Administrative Jurisdiction in the Context of Digitalisation]. *Yuridicheskaya nauka i praktika: Vestnik Nizhegorodskoy akademii MVD Rossii*, 1(69), 73-82. Available at: <https://cyberleninka.ru/article/n/administrativnaya-yurisdiksiya-v-usloviyah-tsifrovizatsii>
 12. Rymkevich Ya.A. (2023). Yuridicheskaya otvetstvennost' v tsifrovom prostranstve [Legal Responsibility in the Digital Space]. *Obrazovaniye i pravo*, 7, 436-440. Available at: <https://cyberleninka.ru/article/n/yuridicheskaya-otvetstvennost-v-tsifrovom-prostranstve>
 13. Toturbiyev A.A. (2025). Sovershenstvovaniye gosudarstvennogo kontrolya v usloviyakh tsifrovizatsii [Improvement of State Control in the Context of Digitalisation]. *Vestnik nauki*, 2(3/84), 245-255. Available at: <https://cyberleninka.ru/article/n/sovershenstvovanie-gosudarstvennogo-kontrolya-v-usloviyah-tsifrovizatsii>
 14. Kruzhilin V.S. (2025). Sinkhronizatsiya reformirovaniya pravovoy osnovy kontrol'no-nadzornoy deyatel'nosti i zakonodatel'stva ob administrativnykh pravonarusheniyakh: voprosy teorii i praktiki [Synchronisation of Reforming the Legal Framework of Control and Supervisory Activities and Legislation on Administrative Offences: Issues of Theory and Practice]. *Gosudarstvennaya sluzhba i kadry*. Available at: <https://cyberleninka.ru/article/n/sinhronizatsiya-reformirovaniya-pravovoy-osnovy-kontrolno-nadzornoy-deyatelnosti-i-zakonodatelstva-ob-administrativnykh>
 15. Plaksin S.M., Abuzyarova I.A., Alimpeyev D.R. et al. (2026). *Kontrol'no-nadzornaya i razreshitel'naya deyatel'nost' v Rossiyskoy Federatsii. Mirovoy opyt primeneniya mekhanizmov kontrol'no-nadzornoy deyatel'nosti. Analiticheskiy doklad – 2025* [Control, Supervisory and Permissive Activities in the Russian Federation. World Experience in Applying Mechanisms of Control and Supervisory Activities. Analytical Report – 2025]. Moscow: HSE Publishing House. Available at: <https://publications.hse.ru/view/1137108772>
 16. Postanovleniye Konstitutsionnogo Suda RF ot 17.07.2023 № 42-P «Po delu o proverke konstitutsionnostichasti 2 stat'i 1.7 Kodeksa Rossiyskoy Federatsii ob administrativnykh pravonarusheniyakh...» [Ruling of the Constitutional Court of the Russian Federation No. 42-P of 17.07.2023 "On the Case of Reviewing the Constitutionality of Part 2 of Article 1.7 of the Code of the Russian Federation on Administrative Offences..."]. Available at: https://www.consultant.ru/document/cons_doc_LAW_452324/