СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПРАВОВЫХ СИСТЕМ В ОБЛАСТИ РАЗВИТИЯ И РЕГУЛИРОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В РОССИИ, США И КИТАЕ

Лукиных Д.С.

1. Введение

Искусственный интеллект перестал быть исключительно технологической категорией и превратился в самостоятельный объект правовой политики. На рубеже 2020-х годов государства начали регулировать ИИ не только как инструмент повышения производительности и экономического роста, но и как источник новых юридических рисков: вмешательства в частную жизнь, непрозрачного автоматизированного принятия решений, нарушения интеллектуальных прав, дискриминации, информационной безопасности и трансформации публичной власти. Показательно, что Россия, Соединённые Штаты Америки и Китайская Народная Республика закрепили развитие ИИ в документах стратегического уровня: в России — в Национальной стратегии развития искусственного интеллекта до 2030 года, утверждённой Указом Президента РФ от 10 октября 2019 г. № 490; в США — в системе президентских актов, меморандумов OMB, рамок NIST и федеральной политики, которая после 2025 года была переориентирована на курс «American AI dominance»; в Китае — в Плане развития искусственного интеллекта нового поколения 2017 года и последующих обязательных административных правилах для генеративного ИИ. [1]

Актуальность темы определяется тем, что право в сфере ИИ сегодня решает двойственную задачу. С одной стороны, оно должно создавать условия для инвестиций, испытаний, внедрения и коммерциализации новых технологий. С другой стороны, именно право задаёт пределы допустимого использования ИИ там, где затрагиваются частная жизнь, свобода выражения мнения, права на результаты интеллектуальной деятельности, защита персональных данных и национальная безопасность. Сравнение трёх крупных юрисдикций особенно важно потому, что они демонстрируют три различные модели правового ответа: российскую — стратегико-государственную и экспериментальную; американскую — фрагментированную, прецедентно-административную и рыночно ориентированную; китайскую — централизованную, детально администрируемую и тесно связанную с государственным управлением данными и контентом. [5]

Цель настоящего исследования состоит в выявлении сходств и различий в правовых системах России, США и Китая в части развития и регулирования искусственного интеллекта, а также в оценке того, как эти различия проявляются не только в текстах нормативных актов, но и в судебной практике. Для достижения этой цели решаются следующие задачи: во-первых, анализируются стратегические и нормативные основы регулирования ИИ в

каждой из трёх юрисдикций; во-вторых, исследуются три репрезентативных судебных кейса — *Glukhin v. Russia*, *Thaler v. Perlmutter* и *Li v. Liu*; в-третьих, на основе сопоставления актов и кейсов формулируются выводы о моделях ответственности, подходах к авторству, правозащитных гарантиях и влиянии права на инновационную среду. [9]

Методологическую основу работы составляет сравнительно-правовой метод в сочетании с case-study. Сравнительно-правовой подход позволяет сопоставить не только отдельные нормы, но и институциональную логику регулирования: место стратегических документов, роль исполнительной власти, характер судебного контроля, уровень детализации обязательств разработчиков, пользователей и платформ. Метод case-study необходим потому, что именно судебные дела показывают пределы действующего регулирования: где норма оказывается слишком общей, где суд формулирует критерий, отсутствующий в законе, и где правоприменение фактически замещает законодательное молчание. [9]

Структурно статья состоит из шести разделов. После введения рассматриваются российская, американская и китайская модели регулирования ИИ. Затем проводится развернутый сравнительный анализ по ключевым вопросам: авторство и охраноспособность результатов, созданных с использованием ИИ; баланс инноваций и прав человека; подотчётность разработчиков, пользователей и платформ; влияние правовой среды на инвестиции и конкурентоспособность. В заключении формулируются выводы и рекомендации, прежде всего применительно к дальнейшему развитию российского регулирования. [1]

2. Правовое регулирование развития и использования ИИ в Российской Федерации

Российская модель регулирования искусственного интеллекта строится прежде всего как государственно-стратегическая. Базовым актом выступает Указ Президента РФ от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации», которым утверждена Национальная стратегия развития искусственного интеллекта на период до 2030 года. В 2024 году стратегия была существенно обновлена Указом Президента РФ от 15 февраля 2024 г. № 124: по официальным и справочным материалам были расширены понятия, зафиксированы достигнутые результаты по состоянию на IV квартал 2023 года, скорректированы задачи, дополнены показатели, а раздел V дополнен блоками о поддержке организаций — разработчиков технологий ИИ и внедрении доверенных технологий ИИ. Это означает, что государство рассматривает ИИ уже не как экспериментальную цифровую новеллу, а как элемент долгосрочной промышленной, оборонной и технологической политики. [1]

Одновременно по состоянию на апрель 2026 года в России отсутствует единый федеральный закон «об искусственном интеллекте» как кодифицированный акт

общего действия. Однако это не означает правового вакуума. Российское регулирование распределено между несколькими блоками: стратегическими актами; экспериментальными режимами; законодательством о персональных данных и биометрии; нормами об информационной безопасности; общими положениями гражданского права и интеллектуальной собственности; отраслевыми актами об отдельных цифровых технологиях. Именно эта фрагментарность является одной из определяющих черт российской модели. [1]

С точки зрения позитивного права особенно значимы два федеральных закона. Во-первых, Федеральный закон от 24 апреля 2020 г. № 123-ФЗ о проведении эксперимента по установлению специального регулирования в целях разработки и внедрения технологий искусственного интеллекта в субъекте РФ — городе федерального значения Москве. Именно в нём содержится одно из ранних нормативных определений ИИ: это «комплекс технологических решений, позволяющий имитировать когнитивные функции человека». Во-вторых, Федеральный закон от 31 июля 2020 г. № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации», который распространяет логику «регуляторных песочниц» на более широкий круг цифровых решений. Закон № 258-ФЗ прямо связывает экспериментальные режимы с задачей «формирования комплексной системы регулирования общественных отношений», а также с созданием благоприятных правовых условий для разработки и внедрения новых технологий. [5]

Не менее важен блок законов о данных и безопасности. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» регулирует согласие на обработку, специальные категории данных, биометрические персональные данные, а также принятие решений, порождающих юридические последствия для субъекта данных, на основе исключительно автоматизированной обработки. По сведениям СПС [5], согласие должно быть «конкретным, предметным, информированным, сознательным и однозначным». Отдельно действует Федеральный закон от 29 декабря 2022 г. № 572-ФЗ о биометрической идентификации и аутентификации, а в аспекте инфраструктурной устойчивости — Федеральный закон от 26 июля 2017 г. № 187-ФЗ о безопасности критической информационной инфраструктуры РФ. В результате российский режим ИИ формируется не через один отраслевой закон, а через пересечение норм о данных, безопасности, экспериментах и цифровой инфраструктуре. [5]

В 2025–2026 годах государственный курс на ИИ был дополнительно встроен в систему отраслевых и межотраслевых документов Правительства РФ: акты этого периода связывают реализацию Национальной стратегии ИИ с высокопроизводительными вычислениями, алгоритмами искусственного интеллекта, цифровой трансформацией отраслей и инвестиционной политикой. Это подтверждает, что стратегия 2019 года после обновления 2024 года не утратила практического значения и продолжает использоваться как рамка для конкретных мер управления.

2.1. Анализ дела *Glukhin v. Russia*

Для оценки реального состояния российского регулирования ИИ в чувствительной сфере биометрического правоприменения ключевое значение имеет дело *Glukhin v. Russia* (жалоба № 11519/20), по которому Европейский суд по правам человека вынес решение 4 июля 2023 года. Согласно официальному пресс-релизу ЕСПЧ, дело касалось использования технологии распознавания лиц для установления личности и задержания заявителя после одиночной акции в московском метро 23 августа 2019 года: он держал картонную фигуру Константина Котова и баннер о возможном пятилетнем лишении свободы «for peaceful protests». Заявителя идентифицировали по изображениям из социальных сетей, записям камер видеонаблюдения, а впоследствии — с использованием live facial recognition в метрополитене; затем его привлекли к административной ответственности и оштрафовали на 20 000 рублей. [9]

ЕСПЧ единогласно установил нарушение статьи 8 и статьи 10 Конвенции. В официальных материалах Суда технология охарактеризована как «highly intrusive facial recognition technology», а в пресс-релизе — как «particularly intrusive». Суд подчеркнул, что применение такой технологии к участнику мирной протестной акции несовместимо с идеалами и ценностями демократического общества, основанного на верховенстве права, если отсутствуют достаточные правовые гарантии против злоупотреблений и произвола. Существенно и то, что официальный пресс-релиз ЕСПЧ указал: в период 2017–2022 гг. в Москве было установлено более 220 000 камер, все из которых оснащены технологией live facial recognition. Для академического анализа это важнее распространённых в вторичной литературе цифр, поскольку именно такая оценка содержится в официальном документе Суда. [9]

Наиболее значим вывод ЕСПЧ о качестве национального регулирования. Суд указал, что российское право в рассматриваемый период не требовало от полиции ни фиксировать использование facial recognition technology, ни уведомлять об этом, а внутреннее законодательство не содержало достаточно детализированных правил и «strong safeguards against abuse and arbitrariness». Суд также отметил отсутствие «pressing social need»: заявитель не представлял опасности, речь шла о мирной форме выражения мнения, а вменённое нарушение было административным и сравнительно малозначительным. Следовательно, даже если формальные правовые основания для видеонаблюдения и полицейской деятельности существовали, их оказалось недостаточно для легитимации именно биометрического, превентивно-наблюдательного и фактически тотального способа идентификации. [9]

Сравнительно-правовое значение дела *Glukhin* состоит в том, что оно высветило центральную слабость российской модели: опережающее внедрение технологии по отношению к детализации гарантий. В стратегических и программных документах государство последовательно стимулирует внедрение ИИ, включая «доверенные технологии», поддержку разработчиков и экспериментальные режимы. Однако в сфере публичного использования биометрического ИИ —

особенно в правоохранительной и транспортной среде — долгое время отсутствовали чёткие критерии необходимости, пропорциональности, пределов цели, обязательного журналирования, независимого контроля, сроков хранения, уведомления и механизмов оспаривания. Иначе говоря, российская система оказалась сильной в мобилизации и инфраструктурном развертывании, но слабой в экзистенциально важном для ИИ элементе — ex ante safeguards. [5]

2.2. Сильные и слабые стороны российской модели

К сильным сторонам российской модели следует отнести стратегическую определённость, институциональную поддержку отечественных разработок, использование экспериментальных правовых режимов и увязку ИИ с задачами технологической независимости, безопасности и цифровой трансформации публичного сектора. Российское право не игнорирует ИИ; напротив, оно стремится включить его в государственное планирование и экономическую политику. [1]

Слабые стороны — это прежде всего фрагментарность, отсутствие единого риск-ориентированного закона общего действия, дефицит специальных гарантий для биометрических и иных высокорисковых систем, а также ограниченность устоявшейся судебной практики по вопросам авторства, ответственности и допустимости автоматизированных решений. В сфере интеллектуальной собственности российский ГК РФ по-прежнему исходит из антропоцентрической формулы: «автором результата интеллектуальной деятельности признается гражданин, творческим трудом которого создан такой результат»; аналогично автором произведения признаётся гражданин, творческим трудом которого оно создано. Но применительно к результатам, созданным с использованием генеративного ИИ, эта формула пока не получила в России авторитетного судебного наполнения. [5]

3. Правовое регулирование ИИ в Соединённых Штатах Америки

Американская модель регулирования ИИ принципиально отличается от российской отсутствием всеобъемлющего федерального закона для частного сектора. По состоянию на апрель 2026 года США сохраняют фрагментированный режим, в котором сочетаются президентские акты, федеральные меморандумы для органов исполнительной власти, добровольные стандарты NIST, отраслевое регулирование, право штатов и судебная практика. Важнейшая особенность актуального состояния состоит в том, что системообразующий для 2023–2024 годов Executive Order 14110 от 30 октября 2023 года (*Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*) был отменён в январе 2025 года, а новая администрация сместила акцент на минимизацию барьеров для инноваций и укрепление «America’s global AI dominance».

Это не означает полного отказа от риск-ориентированного подхода, но означает институциональную перенастройку. OMB Memorandum M-24-10 от 28 марта

2024 года, принятый во исполнение EO 14110, требовал от агентств создавать AI governance bodies, назначать Chief AI Officers, публиковать inventories AI use cases и применять минимальные практики управления рисками в случаях, затрагивающих права и безопасность. После 2025 года OMB Memorandum M-25-21 от 3 апреля 2025 года сохранил курс на федеральное использование ИИ, но уже в логике ускоренного внедрения при условии, что применение ИИ остаётся trustworthy, secure and accountable. Таким образом, в США на федеральном уровне сохранилась не модель общего запрета или лицензирования ИИ, а модель управляемого административного внедрения в государственном секторе и более свободного режима для частных разработчиков.

Существенную роль играет NIST AI Risk Management Framework 1.0. NIST прямо характеризует AI RMF как добровольный ресурс, который помогает организациям управлять рисками ИИ; он является rights-preserving, non-sector-specific и use-case agnostic. Для генеративного ИИ NIST опубликовал отдельный профиль к AI RMF, обновлённый 8 апреля 2026 года. Правовое значение этого инструмента состоит в том, что США предпочитают не столько жёсткое предварительное регулирование всех ИИ-систем, сколько стандарты надлежащей практики, которые затем используются агентствами, закупщиками, судами и участниками рынка в качестве ориентира. [13]

При этом фрагментарность остаётся системной проблемой. Уже в конце 2025 года Белый дом официально констатировал, что в стране складывается «patchwork of 50 different States' AI regimes», способный особенно тяжело ударить по стартапам и инновационным компаниям. Независимо от политической оценки такой формулировки, она подтверждает: США пока не выработали единого федерального стандарта регулирования ИИ для всей экономики. [11]

3.1.Подход США к интеллектуальной собственности и AI-generated works

Наиболее проработанным и юридически устойчивым в США сегодня является подход к авторскому праву на результаты, созданные с использованием ИИ. U.S. Copyright Office в Policy Statement от 16 марта 2023 года *Works Containing Material Generated by Artificial Intelligence* подтвердил, что для охраны авторским правом требуется человеческое авторство: Office не регистрирует произведения, созданные машиной или простым механическим процессом «without any creative input or intervention from a human author». Вопрос ставится так: является ли произведение в сущности продуктом человеческого авторства, где компьютер — лишь assisting instrument, или же традиционные элементы авторства были «conceived and executed» машиной. Для сложных генеративных систем USCO прямо указал, что одни лишь текстовые prompts, как правило, не означают, что человек контролировал традиционные элементы авторства в достаточной степени. [16]

Эта позиция была дополнительно подтверждена в отчёте U.S. Copyright Office

Copyright and Artificial Intelligence, Part 2: Copyrightability (январь 2025 года). Office пришёл к выводу, что действующее право в целом достаточно; законодательные изменения для сохранения критерия human authorship не требуются; purely AI-generated material не охраняется; вопросы должны решаться case-by-case; prompts alone в существующем технологическом контексте обычно недостаточны; однако человеческие авторы могут обладать правами на отбор, координацию, аранжировку и иные творческие модификации. [16]

3.2. Разбор дела *Thaler v. Perlmutter*

Дело *Thaler v. Perlmutter* стало центральным прецедентом в американской дискуссии о human authorship. Заявитель, доктор Стивен Талер, подал заявку на регистрацию изображения *A Recent Entrance to Paradise*, указав в качестве единственного автора принадлежащую ему ИИ-систему *Creativity Machine* и утверждая, что работа была «autonomously created by machine». Copyright Office отказал в регистрации, после чего заявитель оспаривал этот отказ сначала в федеральном окружном суде округа Колумбия, затем в D.C. Circuit, а после — пытался добиться пересмотра в Верховном суде США. 2 марта 2026 года Верховный суд отказал в certiorari, тем самым оставив в силе решения нижестоящих инстанций.

Федеральный окружной суд сформулировал спор предельно ясно: единственный вопрос состоял в том, «whether a work generated entirely by an artificial system absent human involvement is eligible for copyright». Ответ был отрицательным. D.C. Circuit закрепил это ещё жёстче: «The Creativity Machine cannot be the recognized author of a copyrighted work because the Copyright Act of 1976 requires all eligible work to be authored in the first instance by a human being». Суд также отметил, что альтернативный довод Талера о его собственном авторстве как создателя и пользователя системы был процессуально утрачен, поскольку не был своевременно представлен в административной процедуре. Нормативной основой выступала прежде всего 17 U.S.C. § 102(a), согласно которой copyright subsists in “original works of authorship”; суды прочитали эту формулу в свете устойчивой доктрины human authorship.

Значение дела *Thaler* двоякое. С одной стороны, оно создаёт ясность: в американском праве ИИ не может быть признан автором, а полностью автономно созданный результат без существенного человеческого творческого вклада не подлежит охране авторским правом. С другой стороны, дело не закрывает вопрос о произведениях, где ИИ использован как сложный инструмент: напротив, и USCO, и суды оставили пространство для охраны тех аспектов результата, где человек действительно осуществлял творческий выбор, компоновку или переработку. Поэтому американская система не запрещает творчество с ИИ, а проводит жёсткую демаркацию между инструментальным использованием технологии и попыткой признать саму машину субъектом авторского права. [16]

3.3. Роль судебной практики и регуляторов

Американская подотчётность в сфере ИИ строится не только через copyright litigation. Федеральная торговая комиссия (FTC) использует существующие полномочия в сфере deceptive practices для контроля AI claims. На официальном AI-ресурсе FTC отражены, в частности, дело против IntelliVision, где оспаривались утверждения о том, что facial recognition software свободно от гендерных и расовых искажений, а также дело против DoNotPay, связанное с вводящими в заблуждение заявлениями об «AI lawyer». Это типично для американского подхода: вместо единого AI code регулятор применяет уже существующие механизмы consumer protection, unfairness и deception к новым технологическим продуктам. [18]

Сильные стороны американской модели — это гибкость, быстрый судебный отклик, развитость административных стандартов и способность использовать существующие институты без ожидания полного «закона об ИИ». Слабые стороны — нормативная фрагментарность, высокая зависимость от политических циклов исполнительной власти, различия между режимами штатов и сохранение значительных зон неопределённости для бизнеса и авторов. [11]

4. Правовое регулирование ИИ в Китайской Народной Республике

Китайская модель регулирования ИИ наиболее тесно соединяет стратегическое планирование, административное нормотворчество и государственный контроль над данными и цифровыми сервисами. Нормативной отправной точкой остаётся *New Generation Artificial Intelligence Development Plan*, утверждённый Государственным советом КНР в 2017 году. План закрепил трёхэтапную траекторию развития: к 2020 году — догоняющее развитие; к 2025 году — существенный прорыв; к 2030 году — превращение Китая в «world’s primary AI innovation center». Официальные материалы Государственного совета также указывают на ориентиры по объёму индустрии: более 1 трлн юаней для core AI industry и более 10 трлн юаней для связанных отраслей к 2030 году, а также на задачу формирования более полного правового, нормативного и этического порядка для ИИ. [19]

Если российская модель строится через стратегию плюс фрагментарные законы, а американская — через soft law и судебную практику, то китайская модель характеризуется быстрым принятием обязательных административных правил для отдельных сегментов. Ключевой акт — *Interim Measures for the Administration of Generative Artificial Intelligence Services*, принятый семью регуляторами КНР и вступивший в силу 15 августа 2023 года. Уже статья 3 закрепляет основную формулу китайского подхода: необходимо «adhere to equal emphasis on development and security», сочетать продвижение инноваций с законным управлением, применять «inclusive and prudent regulation» и одновременно — классифицированный, дифференцированный надзор. [22]

Содержание *Interim Measures* показывает высокую степень детализации.

Провайдеры генеративного ИИ обязаны не создавать и не распространять запрещённый контент, предотвращать дискриминацию, уважать права интеллектуальной собственности и персональные права, повышать прозрачность и надёжность сервисов. Статья 7 требует, чтобы данные и базовые модели использовались из законных источников, без нарушения интеллектуальных прав; при обработке персональной информации необходимо получать согласие или опираться на иное законное основание; требуется улучшать качество данных. Отдельно предусмотрены обязанности по маркировке сгенерированных изображений и видео в соответствии с правилами deep synthesis, ограничения на ненужный сбор персональной информации, меры в отношении незаконного контента и пользователей, а также специальные требования безопасности для сервисов, обладающих способностью влиять на общественное мнение или осуществлять social mobilization. [22]

Эти меры встроены в более широкий комплекс китайского законодательства о данных. *Data Security Law* требует, чтобы сбор данных осуществлялся lawful and proper methods и в пределах цели и объёма. *Personal Information Protection Law* закрепляет принципы законности, добросовестности, необходимости, открытости и прозрачности, минимизации объёма, а также устанавливает основания обработки и экстерриториальное действие в случаях, когда обработка связана с предоставлением товаров и услуг лицам в КНР или анализом их поведения. Дополнительное усиление режима произошло с вступлением в силу с 1 января 2025 года *Network Data Security Management Regulations* (Госсовет КНР, Decree No. 790). В результате китайское регулирование ИИ оказалось встроено в наиболее плотную из рассматриваемых систем data governance. [21]

4.1. Разбор дела *Li v. Liu*

На этом фоне особый интерес представляет дело *Li v. Liu*, рассмотренное Пекинским интернет-судом 27 ноября 2023 года, № (2023) Jing 0491 Min Chu No. 11279. Оно важно тем, что при жёстком административном контроле над ИИ Китай занял сравнительно гибкую позицию в вопросе авторства результатов, созданных с использованием генеративной модели. По официальному тексту решения, истец Ли Юнкай 24 февраля 2023 года сгенерировал изображение с помощью Stable Diffusion, используя набор prompts, negative prompts и параметров, после чего опубликовал результат на платформе Xiaohongshu. Ответчик впоследствии использовал изображение без разрешения, удалив водяной знак и разместив его в сети. [22]

Суд подробно воспроизвёл процесс генерации: выбор модели, формулирование подсказок, негативных подсказок, подбор параметров, многократное тестирование и окончательный выбор одного результата из множества вариантов. В решении прямо указано, что интеллектуальный вклад истца выражался в «designing the way the characters are presented, selecting prompt words, arranging the order of prompt words, setting relevant parameters, and selecting which picture ultimately meets expectations». Суд подчеркнул, что такое

произведение не является «mechanical intellectual achievement»: разные лица, используя разные prompts и параметры, могли бы получить иные результаты. [22]

Далее Пекинский интернет-суд сделал два концептуально важных вывода. Во-первых, сама AI-model не может быть автором по Закону КНР об авторском праве; автором может быть только субъект, признаваемый правом. Во-вторых, если именно человек осуществил существенный интеллектуальный вклад и результат отражает его personalized expression, автором признаётся этот человек. На этом основании суд признал спорное изображение произведением изобразительного искусства, охраняемым авторским правом, установил авторство истца, признал нарушение права на воспроизведение и права на распространение через информационную сеть, обязал ответчика извиниться и взыскал компенсацию в 500 юаней. Одновременно суд отметил желательность добросовестной маркировки использования ИИ; хэштег «AI illustration» счёл достаточным для информирования публики. [22]

4.2. Особенности китайской модели

Сильная сторона китайского подхода — институциональная цельность. Развитие ИИ и его контроль не разведены по разным плоскостям, а соединены в единую систему: стратегические цели, контентные обязательства, правила для данных, требования к обучающим наборам и моделям, маркировка, административный надзор. В сфере авторского права китайские суды демонстрируют прагматизм: ИИ не становится субъектом, но и человеческий вклад не редуцируется до «ручного» рисования; достаточно, чтобы он был интеллектуально содержательным и индивидуализированным. [19]

Слабость китайской модели заключается в высокой плотности государственного контроля и тесной связи регулирования ИИ с режимом информационной и политической управляемости. Для инноваций это создаёт предсказуемую, но одновременно жёсткую среду, где вопросы контента, данных и допуска к рынку тесно переплетены с интересами государства.

5. Сравнительный анализ на основе нормативной базы и судебных кейсов

5.1. Три модели правового ответа на ИИ

Сопоставление России, США и Китая показывает, что различия между ними проходят не только по линии «строже — мягче», но и по линии правовой архитектуры. Россия регулирует ИИ преимущественно через стратегические документы и специальные режимы, дополняя их общими законами о данных, биометрии и безопасности. США строят регулирование через сочетание executive policy, agency guidance, sectoral enforcement и судебной практики. Китай, напротив, соединяет государственное стратегическое планирование с детальными административными требованиями к конкретным категориям AI-services. В этом смысле речь идёт о трёх разных юридических технологиях

управления одним и тем же объектом.

Для России характерно нормативное «рассеивание» ИИ по разным отраслям права. Это повышает адаптивность и позволяет не ждать принятия единого кодекса, но одновременно осложняет правоприменение: субъекты рынка и граждане вынуждены собирать правовой режим из множества актов разной юридической силы. США решают ту же проблему иначе: отсутствие общего закона компенсируется высокой способностью агентств и судов быстро вырабатывать рабочие критерии. Китай же снижает неопределённость за счёт более подробных административных правил, но ценой увеличения регуляторной плотности и усиления государственного контроля. [5]

5.2. Авторство и охраноспособность результатов, созданных с использованием ИИ

Наиболее яркое различие между юрисдикциями проявляется в сфере авторства. США занимают наиболее жёсткую позицию. И USCO, и федеральные суды исходят из того, что copyright в принципе требует human authorship. Полностью автономно созданный машиной результат не получает охраны. Более того, текущая позиция USCO исходит из того, что одни лишь prompts, без достаточного человеческого контроля над традиционными элементами авторства, как правило, не образуют охраноспособного человеческого вклада. В деле *Thaler* эта логика доведена до предельной ясности: если в заявке в качестве автора назван исключительно ИИ, регистрация невозможна. [14, 15]

Китайский подход выглядит более гибким, но не противоположным. Пекинский интернет-суд также отказался признавать ИИ автором. Однако он сосредоточился не на абстрактном вопросе «создала ли машина картинку», а на юридически более точном вопросе: воплощён ли в результате достаточный интеллектуальный вклад конкретного человека. Если такой вклад доказан через выбор модели, формулирование prompts и negative prompts, настройку параметров, многократный отбор и финальное решение автора, результат может охраняться. Тем самым Китай не отменяет human authorship, а функционально расширяет понимание того, какие действия человека в эпоху генеративного ИИ являются творческими. [22]

Россия находится между этими моделями, но пока без устойчивой судебной конкретизации. Российский ГК РФ уже содержит антропоцентрическую основу: автор — это гражданин, творческим трудом которого создан результат. Никаких норм, допускающих признание ИИ автором, российское право не содержит. Следовательно, исходная догматика в России ближе к американской и китайской в том, что субъектом авторства остаётся человек. Но в отличие от США и Китая, где уже появились авторитетные позиции USCO и судебные решения, российская система по состоянию на апрель 2026 года не выработала устойчивого судебного теста для определения того, когда prompt engineering, curating, iterative selection и иные формы взаимодействия с генеративной моделью достигают уровня «творческого труда». [5]

Из этого следуют разные практические последствия. В США высокая правовая определённость снижает риск фиктивного признания машинного авторства, но одновременно оставляет создателей AI-assisted works в ситуации, когда им приходится очень точно доказывать человеческий вклад. В Китае пространство для такой охраны шире, что может стимулировать креативные индустрии и локальные AI-platforms. В России же неопределённость сама по себе становится регуляторным фактором: разработчики и пользователи не знают, как именно суды оценят их вклад, а потому часть конфликтов либо не доходит до суда, либо разрешается вне рамок выработанной доктрины. [14, 15]

5.3. Баланс инноваций, прав человека и безопасности

Второй ключевой критерий сравнения — как каждая система балансирует стимулирование ИИ и защиту фундаментальных интересов личности и общества. Россия в стратегических документах подчёркивает развитие доверенных технологий, поддержку отечественных разработчиков, проведение экспериментов и технологическую устойчивость. Однако дело *Glukhin v. Russia* показало, что в чувствительных сценариях — прежде всего в биометрическом наблюдении в публичном пространстве — правовые гарантии отставали от фактического внедрения технологии. Российская система смогла развернуть инфраструктуру facial recognition, но не обеспечила сопоставимую детализацию safeguards: журналирование применения, прозрачность, пределы цели, независимый контроль, критерии необходимости и пропорциональности. [5]

Американская модель, напротив, менее склонна к единому предписывающему закону, но сильнее опирается на судебный и регуляторный контроль ex post. Это видно не только в *Thaler*, но и в деятельности FTC, которая использует уже имеющиеся полномочия против deceptive AI claims и небезопасных утверждений о технологиях распознавания лиц. В федеральном секторе агентства обязаны учитывать риски high-impact AI, особенно когда затрагиваются права и безопасность. Проблема, однако, в том, что такой режим распределён по множеству актов и институтов, а потому не всегда обеспечивает одинаковый уровень защиты во всех секторах и штатах.

Китай сочетает проинновационную установку с жёстким административным контролем. Формула *Interim Measures* — «equal emphasis on development and security» — не является декоративной: именно поэтому одновременно поощряются вычислительные мощности, модели и данные, но вводятся правила о lawful source of training data, защите персональной информации, маркировке синтетического контента, реагировании на незаконный контент и специальных процедурах для сервисов, способных влиять на общественное мнение. В отличие от России, где основной пробел обнаружился в сфере safeguards против публичного биометрического применения, Китай стремится прописать обязанности провайдеров заранее. Но в отличие от США, эти обязанности теснее увязаны с более широкими целями государственного контроля и информационной политики. [20]

5.4. Ответственность и подотчётность: разработчики, пользователи, платформы

Судебные кейсы показывают и различное распределение ответственности. В деле *Thaler* вопрос был поставлен не о вреде и не о безопасности, а о правовом статусе результата. Американская система фактически отвечает так: ответственность за заявку, раскрытие обстоятельств создания и квалификацию произведения несёт человек-заявитель; машина не становится субъектом, а потому не может служить узлом для перераспределения прав. Это исключает соблазн «списать» юридическую неопределённость на автономность ИИ и принуждает участников рынка описывать человеческий вклад предельно чётко.

В деле *Li v. Liu* китайский суд пошёл ещё дальше в операционализации человеческой ответственности: он не только признал автора-человека, но и связал правовую охрану с конкретно описанными действиями по созданию результата. Это важно, потому что такая логика пригодна и за пределами авторского права. Если законодатель или суд способны реконструировать, кто выбирал модель, кто настраивал параметры, кто отбирал финальный выход и кто распространял контент, то появляется основа для более точного распределения обязанностей между разработчиком, сервис-провайдером и конечным пользователем. [22]

В российском деле *Glukhin* ответственность предстала под иным углом: не как вопрос авторства, а как вопрос подотчётности государства за применение ИИ в публичной власти. Именно здесь выявился дефицит процедурной ответственности: если закон не требует фиксировать сам факт использования facial recognition и не предусматривает внятных механизмов уведомления и контроля, то становится затруднённым последующее оспаривание, а значит — и сама юридическая подотчётность. Таким образом, в сфере публичного ИИ проблема ответственности в России имеет не столько частноправовой, сколько административно-правовой и конституционно-правовой характер. [9]

Сопоставление показывает, что США и Китай, несмотря на различие политико-правических систем, в одном сходятся: они не признают ИИ самостоятельным юридическим носителем авторства или ответственности. Ответственность всегда возвращается к человеку или организации — разработчику, заявителю, провайдеру, пользователю, платформе, органу власти. Российская система теоретически исходит из того же, но на практике нуждается в более детальных правилах, которые позволили бы эту ответственность технически и процессуально проследить. [5]

5.5. Влияние на инвестиции, экосистему и глобальную конкурентоспособность

Правовая модель ИИ влияет не только на правозащиту, но и на инновационную экосистему. Для инвестора и разработчика важны предсказуемость, стабильность требований, ясность по поводу прав на результаты, допустимости использования данных и риска санкций. США остаются привлекательной

юрисдикцией благодаря сочетанию развитого рынка капитала, сильной исследовательской среды и правовой гибкости. Но фрагментарность — включая различия между федеральными и штатными режимами — увеличивает транзакционные издержки и compliance burden. Официальное признание Белым домом проблемы «patchwork» подтверждает, что этот риск осознаётся на государственном уровне. [11]

Китай выигрывает в скорости институционального ответа. Когда появляется новый тип AI-service, государство сравнительно быстро создаёт обязательные административные правила, интегрирует их в систему data governance и даёт рынку сигнал о допустимых моделях поведения. Это повышает предсказуемость для крупных игроков, особенно на внутреннем рынке. Одновременно жёсткие требования к контенту, данным и безопасности могут увеличивать регуляторный порог входа и сдерживать более открытые исследовательские и креативные практики. [20]

Российская модель с точки зрения инноваций имеет потенциал благодаря государственному спросу, экспериментальным режимам и поддержке «доверенных» решений. Однако для глобальной конкурентоспособности ей препятствуют два связанных фактора. Первый — недостаточная нормативная определённость по частноправовым вопросам ИИ, включая результаты генеративных систем. Второй — риски правозащитной и процессуальной неопределённости в высокорисковых сценариях применения ИИ, что может снижать доверие к российским решениям на внешних рынках и осложнять трансграничное взаимодействие в чувствительных секторах. [5]

5.6. Различия правовых культур и взаимные уроки

Различия между странами объясняются и более широкими особенностями правовых культур. Американская система склонна оставлять пространство для рыночной инициативы, а затем корректировать его через суды, агентства и прецедентно развиваемые стандарты. Российская система делает ставку на стратегию государства, экспериментальное регулирование и секторальное распределение норм. Китайская — на централизованное программирование развития с одновременной административной детализацией правил. Ни одна из этих моделей не является универсально «лучшей»; каждая по-своему отвечает на вопрос, как совместить инновацию и контроль. [11]

Россия могла бы заимствовать из американского опыта более чёткое doctrinal clarification вопросов авторства и раскрытия AI-generated components, а из китайского — адресные ex ante обязанности для провайдеров высокорисковых систем, прежде всего в сфере данных, маркировки и прослеживаемости. США могли бы учесть полезность более ясных требований к provenance данных и к маркировке синтетического контента, не отказываясь при этом от судебной гибкости. Китай, в свою очередь, мог бы почерпнуть из американского и европейского правозащитного опыта более выраженный независимый контроль за применением ИИ государственными органами и более сильную процедуру

оспаривания решений, основанных на алгоритмических инструментах. [15]

Наиболее важный вывод сравнительного анализа состоит в следующем: право ИИ сегодня развивается не как самостоятельная замкнутая отрасль, а как узловая точка пересечения конституционного, информационного, административного, гражданского и интеллектуального права. Поэтому успешная модель регулирования должна одновременно отвечать как минимум на четыре вопроса: кто вправе разрабатывать и внедрять систему; на каких данных она обучается и используется; кто и при каких условиях несёт ответственность за её применение; как обеспечиваются проверяемость, оспоримость и защита прав человека. Именно в способности дать связный ответ на эти четыре вопроса и проявляется зрелость национального правового режима ИИ. [5]

6. Заключение и рекомендации

Проведённый анализ показывает, что Россия, США и Китай сформировали три различные, но уже достаточно зрелые модели правового регулирования искусственного интеллекта. Российская модель основана на стратегическом государственном управлении, экспериментальных режимах и фрагментарном распределении норм между несколькими отраслями законодательства. Американская — на сочетании судебной практики, агентского регулирования, добровольных стандартов и точечного применения существующих институтов к новым технологиям. Китайская — на централизованном развитии ИИ, встроенном в плотную систему административных правил, data governance и контентного контроля. Во всех трёх юрисдикциях ИИ не признаётся самостоятельным субъектом авторства; субъектом права остаётся человек или организация. Но критерии человеческого вклада, степень предварительной регламентации и характер safeguards различаются существенно. [5]

Дело *Glukhin v. Russia* особенно важно для российской правовой политики. Оно показывает, что стимулирование развития ИИ без детальных процессуальных гарантий в сфере биометрического наблюдения создаёт системный правовой риск. Формального наличия законов о персональных данных, полиции, видеонаблюдении или даже о биометрии недостаточно, если отсутствуют специальные правила о допустимых целях использования facial recognition, обязательном журналировании, независимом контроле, сроках хранения, уведомлении, праве на обжалование и стандартах необходимости и соразмерности. В этом смысле главный урок кейса — не в отрицании самой технологии, а в необходимости правового проектирования safeguards до её массового внедрения. [9]

Нужен ли России специальный закон об ИИ? Представляется, что с учётом накопленной фрагментарности и появления высокорисковых сценариев ответ скорее положительный, но при одном существенном уточнении: речь должна идти не о декларативном «законе о перспективах ИИ», а о функциональном риск-ориентированном акте. Такой закон или пакет взаимосвязанных поправок

должен, как минимум, закрепить классификацию высокорисковых систем; требования к прослеживаемости и документированию; специальные правила для биометрического ИИ в публичном пространстве; обязанности разработчиков и операторов по качеству данных, оценке воздействия и управлению инцидентами; порядок раскрытия информации о генеративном контенте; а также рамку для распределения ответственности между разработчиком, внедряющей организацией и пользователем. [5]

В сфере интеллектуальной собственности России целесообразно выработать официальные разъяснения — на уровне Пленума Верховного Суда РФ, доктринальных обзоров или специальных разъяснений компетентных органов — о том, какие формы взаимодействия с генеративным ИИ могут считаться творческим вкладом автора. Здесь полезен осторожный синтез американского и китайского опыта: от США — жёсткое сохранение human authorship и запрет на фиктивное признание ИИ субъектом; от Китая — готовность видеть творческий вклад не только в ручном исполнении, но и в осмысленном выборе модели, prompts, параметров, отборе и переработке результата. [15]

В более широком плане перспективным направлением является не полная унификация правовых систем, а гармонизация отдельных принципов: человеческая подотчётность, законность происхождения данных, маркировка синтетического контента, право на оспаривание решений, основанных на высокорисковом ИИ, и специальные safeguards для биометрического наблюдения. Именно такое сочетание — а не простое копирование чужой модели — способно обеспечить России одновременно развитие собственной ИИ-экосистемы, защиту прав граждан и конкурентоспособность в глобальном технологическом соперничестве. [9]

Список использованных источников

1. Указ Президента Российской Федерации от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации»; официальное опубликование; Национальная стратегия развития ИИ до 2030 года. (Kremlin)
2. Указ Президента Российской Федерации от 15.02.2024 № 124 «О внесении изменений в Указ Президента Российской Федерации от 10 октября 2019 г. № 490»; материалы о содержании изменений. (publication.pravo.gov.ru)
3. Федеральный закон от 31.07.2020 № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации». (publication.pravo.gov.ru)
4. Федеральный закон от 24.04.2020 № 123-ФЗ о проведении эксперимента по установлению специального регулирования в целях разработки и внедрения технологий ИИ в городе Москве. (publication.pravo.gov.ru)
5. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

материалы СПС КонсультантПлюс по статьям 9, 11, 16, 18, 19. (КонсультантПлюс)

6. Федеральный закон от 29.12.2022 № 572-ФЗ о биометрической идентификации и аутентификации. (publication.pravo.gov.ru)
7. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». (publication.pravo.gov.ru)
8. Гражданский кодекс Российской Федерации, статьи 1228 и 1257. (КонсультантПлюс)
9. *Glukhin v. Russia*, European Court of Human Rights, judgment of 4 July 2023, application no. 11519/20; официальный пресс-релиз и материалы HUDOC. (hudoc.echr.coe.int)
10. Executive Order 14110 of October 30, 2023, *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*; OMB Memorandum M-24-10 of March 28, 2024.
11. White House, *Initial Rescissions of Harmful Executive Orders and Actions* (20 January 2025); White House, *Removing Barriers to American Leadership in Artificial Intelligence* (23 January 2025). (The White House)
12. OMB Memorandum M-25-21 of April 3, 2025, *Accelerating Federal Use of AI through Innovation, Governance, and Public Trust*.
13. NIST, *AI Risk Management Framework (AI RMF 1.0)*; NIST, *Generative AI Profile* (updated April 8, 2026). (NIST)
14. U.S. Copyright Office, *Works Containing Material Generated by Artificial Intelligence* (Policy Statement, March 16, 2023). (copyright.gov)
15. U.S. Copyright Office, *Copyright and Artificial Intelligence, Part 2: Copyrightability* (January 2025). (copyright.gov)
16. *Thaler v. Perlmutter*, U.S. District Court for the District of Columbia; *Thaler v. Perlmutter*, U.S. Court of Appeals for the D.C. Circuit; Supreme Court docket, certiorari denied March 2, 2026.
17. 17 U.S.C. § 102(a), Legal Information Institute, Cornell Law School. (law.cornell.edu)
18. Federal Trade Commission, official AI resources and enforcement materials (including IntelliVision and DoNotPay matters). (Federal Trade Commission)
19. State Council of the PRC, *New Generation Artificial Intelligence Development Plan* (2017); official State Council and State Council Gazette materials. (NHC)
20. *Interim Measures for the Administration of Generative Artificial Intelligence Services* (effective August 15, 2023), official text. (Центральный комитет Китая)
21. *Data Security Law of the People's Republic of China*; *Personal Information*

Protection Law of the People's Republic of China; *Network Data Security Management Regulations* (effective January 1, 2025). (en.spp.gov.cn)

22. Beijing Internet Court, Civil Judgment *Li v. Liu*, (2023) Jing 0491 Min Chu No. 11279, judgment of 27 November 2023; official English version. (english.bjinternetcourt.gov.cn)