Мониторинг международных трендов правового регулирования для развития законодательства в сфере цифровой экономики в России

- **Регуляция криптовалют**
- **Ценообразование на платформах**
- **Регуляция персональных данных**
- **Развитие открытых ИИ-моделей и прав на ИИ-контент**
- **Данные в конкуренции**

Мониторинг №8 (20) (Август 2025)

Мониторинг подготовлен коллективом сотрудников лаборатории анализа лучших международных практик Института экономической политики имени Е. Т. Гайдара (Института Гайдара).

Авторский коллектив: науч. сотр. Гирич М.Г., науч. сотр. Ермохин И.С., ст. науч. сотр. Левашенко А.Д., науч. сотр. Магомедова О.С., науч. сотр. Черновол К.А., науч. сотр. Фонда Экономической политики Голованова Д.А.

«Здравствуй, август, венчан хмелем,
Смуглый юноша-сатир!
Мы ковры под дубом стелем,
Мы в лесу готовим пир!..»
В. Брюсов

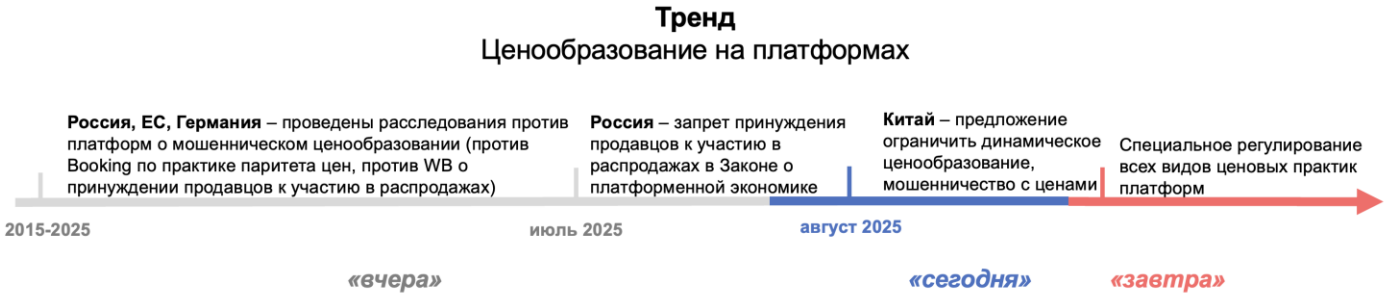
В августе 2025 г. можно выделить 5 событий, которые определяют тренды развития регулирования цифровой экономики в мире.

Тренд № 1. Регуляция криптовалют

Гонконг предложил обязательное лицензирование всех компаний, работающих с криптовалютами, ЕС установил требования к рискам и лимиты для банковских вложений в криптовалюты, Луизиана (США) запретила участие иностранных компаний в майнинге, а Таиланд запустил пилотный проект для конвертации криптовалют в бат туристами.

Тренд № 2. Ценообразование на платформах

В Китае предложен проект регулирования ценовых практик на платформах, включая участие продавцов в распродажах, алгоритмическое ценообразование на основе данных, автоматические списания, ограничение паритета цен и пр.



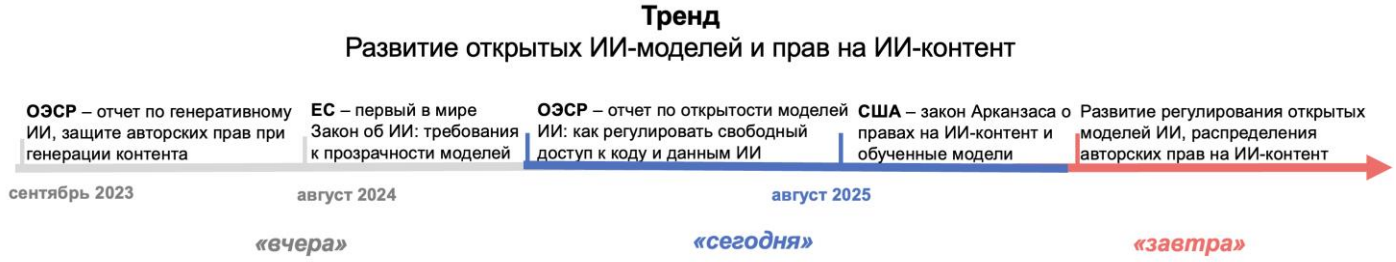
Тренд № 3. Регуляция персональных данных

В Калифорнии обсуждался запуск централизованной платформы для запросов потребителей на удаление их данных из баз брокеров данных. Штаты США начали прокурорскую проверку законности нового сервиса Instagram, позволяющего пользователям публиковать геоданные в режиме реального времени[1]. В Австрии суд признал неправомерным сбор пользовательских данных с помощью механизма «Pay or OK».

Тренд № 4. Развитие открытых ИИ-моделей и прав на ИИ-контент

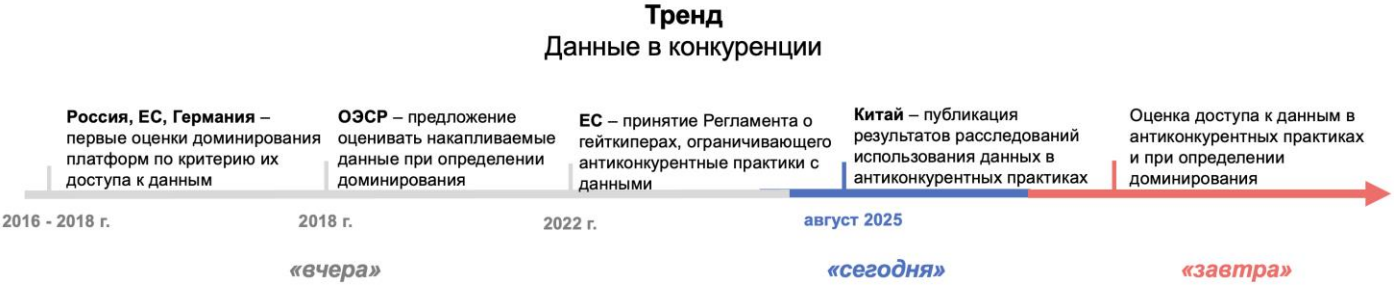
[1] Деятельность компании Meta признана экстремистской и запрещена на территории Российской Федерации.

В августе 2025 г. ОЭСР выпустила отчет, а в Арканзасе (штат США) принят закон, которые объясняют, как регулировать открытые модели ИИ и кому принадлежат права на созданный ИИ контент: это зависит от того, чьи данные использовались для обучения модели.



Тренд № 5. Данные в конкуренции

В августе 2025 г. Верховный суд Китая опубликовал сборник дел по вопросам защиты данных, включая использование данных в антиконкурентных практиках платформ, например, ограничение возможности переноса данных между платформами и пр.



В августе 2025 г. в России введен ряд нововведений.

1. Введены специальные требования ПОД/ФТ для майнеров и майнинг-пулов

Правительство РФ[2,3] утвердило стандарт ПОД/ФТ[4] для майнеров и организаторов майнинг-пулов[5]. Требуется разработать правила внутреннего ПОД/ФТ - контроля до начала любых операций с цифровой валютой, включая её распределение после майнинга.

Правила охватывают организацию внутреннего контроля, идентификацию и изучение клиентов, управление рисками, выявление подозрительных операций и направление сведений о них в Росфинмониторинг, заморозку (блокировку) активов, обучение кадров, ежегодные внутренние проверки, а также хранение данных не менее 5 лет после завершения отношений с клиентом.

2. Введены новые правила обезличивания персональных данных

Правительство утвердило новые требования и методы обезличивания персональных данных для выполнения операторами данных требования передавать обезличенные данные в ГИС Минцифры[6]. Требуется, чтобы операторы раздельно хранили персональные и обезличенные персональные данные; исключали из обезличенных данных информацию, доступ к которой ограничен законом (включая необезличенные ПД); использовали для обезличивания техники с целью дальнейшей передачи обезличенных данных в ГИС Минцифры; обеспечивали техническую возможность изменять обезличенные данные без их восстановления.

Осуществлять обезличивание предлагается 5 методами: введение идентификаторов (в зарубежной практике, например, в Регламенте ЕС GDPR метод известен как псевдонимизация); изменение состава или семантики; декомпозиция; перемешивание; преобразование (включая агрегирование массивов данных)[7]. Хотя данный набор методов соответствует международной

[2] Постановление Правительства РФ от 7 августа 2025 г. № 1180
[3] https://www.consultant.ru/document/cons_doc_LAW_511974/9d0f569c0eb594c99074582e750e82d845f13d2d/
[4] ПОД/ФТ - Противодействие отмыванию денег и финансированию терроризма.
[5] Объединение майнеров, которые совместно добывают криптовалюту и делят вознаграждение пропорционально внесённой мощности
[6] В соответствии с поправками в ФЗ № 152 от 08.08.2024 г.
[7] Ранее последние 4 метода обезличивания уже предусматривались методическими рекомендациями Роскомнадзора от 2013 г. URL: https://10.rkn.gov.ru/docs/10/Metod.rekomendacii-Ob_utverzhdenii_trebovanij_i_metodov_po_obezlichivaniju_personal6nykh_dannykh.pdf

практике регулирования де-идентификации персональных данных, перечень методов является закрытым, что ограничивает операторов данных в выборе альтернативных методов.

3. Предложена внесудебная блокировка за брань

В Госдуме рассматривается законопроект по применению внесудебной блокировки (по ст. 15.1-1 ФЗ «Об информации»[8]) к нецензурной брани. Это существенно упрощает инициирование пользователями жалоб в генпрокуратуру для внесудебной блокировки контента, поскольку основанием могут служить любые ругательства.

4. Предложены новые меры противодействия киберпреступлениям

Минцифры представило законопроект об обязательствах операторов связи по противодействию телефонному и онлайн мошенничеству[9]. Абонент вправе блокировать вызовы с номеров с нероссийской нумерацией, а операторы обязаны не пропускать такие звонки, информировать пользователей о статусе вызова, передавать госорганам записи разговоров с признаками противоправных действий, выявлять подозрительные номера и передавать сведения о них в ГИС для противодействия правонарушениям с использованием ИКТ.

Для разграничения разрешённых и запрещённых устройств связи создаётся центральная база идентификаторов пользовательского оборудования, куда операторы вносят данные из своих корпоративных баз. Вызовы с телефонов, оформленных на юрлиц или ИП, допускаются только при наличии сведений в базе. Органы безопасности могут запрещать работу конкретного оборудования в российской сети. Предлагаемые меры направлены на установление государственного контроля телефонной связи, включая виртуальные системы, в целях обеспечения экономической безопасности граждан, но могут привести к расходам операторов.

[8] https://sozd.duma.gov.ru/bill/989488-8
[9] https://regulation.gov.ru/projects/159652

Ключевые аспекты

1. Регуляция криптовалют

Опыт Гонконга

В Гонконге в августе 2025 г. обсуждался проект регулирования торговли виртуальными активами[10]. Предусмотрено обязательное лицензирование компаний, осуществляющих операции с виртуальными активами (как криптовалюты), распространение на них требований ПОД/ФТ. Предлагаемые правила расширяют уже имеющееся регулирование: ранее оно охватывало только криптобиржи, а также порядок выпуска и обращения стейблкоинов. Теперь под регулирование попадут все компании, которые помогают клиентам покупать, продавать или хранить криптовалюту: от криптообменников и криптоброкеров до криптокошельков, консультантов и управляющих криптоактивами.

Опыт ЕС

Европейское банковское управление (EBA) опубликовало проект правил[11], по которым банки должны учитывать свои вложения в криптоактивы и определять объем резервов, необходимый для покрытия риска волатильности криптоактивов в соответствии с Регламентом ЕС о нормативных требованиях к капиталу (CRR III)[12]. Банки могут приобретать криптоактивы (например, криптовалюты, стейблкоины) как часть собственного инвестиционного портфеля или для обслуживания клиентов.

Согласно проекту различным категориям криптовалют присваиваются разные коэффициенты риска, определяющие сколько капитала банк должен зарезервировать под такие вложения. Например, для токенов, обеспеченных реальными активами (например, золотом) (ARTs[13] по регламенту MiCA[14]) установлен коэффициент 250%, а для необеспеченных криптовалют (таких как Bitcoin) — установлен максимальный коэффициент риска 1250%.

Для сравнения коэффициент риска для золота составляет 100%, для акции — 250%. То есть коэффициент 250% делает даже обеспеченные токены рискованнее обычных активов, а 1250% для необеспеченных криптовалют приравнивает их к самым рискованным вложениям, фактически запрещая банкам держать такие активы.

Таким образом, если, например, банк покупает Bitcoin на 100 млн евро, к такому активу применяется коэффициент риска 1250%. Это означает, что для расчёта активов с учётом риска[15] сумма увеличивается в 12,5 раз и составляет 1,25 млрд евро. Однако поскольку банки обязаны держать капитал в размере не менее 8% от суммы активов, взвешенных с учётом риска, то в данном случае банк будет обязан зарезервировать 100 млн евро собственного капитала. Иными словами, под каждый вложенный в Bitcoin 1 евро банк должен держать ещё 1 евро капитала.

Вводятся и количественные ограничения: суммарный объём необеспеченных криптоактивов на балансе банка не должен превышать 1% от его основного капитала первого уровня[16]. Такие меры фактически направлены на ограничение масштабного накопления банками волатильных криптовалют.

Опыт США (Луизиана)

В штате Луизиана вступил в силу Blockchain Basics Act[17], запрещающий определённым иностранным компаниям приобретать или владеть предприятиями по майнингу криптовалют в штате, а именно — гражданам и организациям из стран, находящихся под санкциями США[18][19] (например, из России, Ирана), а также компаниям, которые Госдеп США признал

[10] https://www.fstb.gov.hk/fsb/en/publication/consult/doc/VADEALING_consultation_paper_en.pdf
[11] https://www.eba.europa.eu/sites/default/files/2025-08/616d6b06-cdcf-4246-a7cc-2173dfd32fa6/Draft%20RTS%20on%20crypto%20asset%20exposures%20Article%20501d-5.pdf
[12] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401623
[13] Asset Referenced Tokens
[14] Markets in Crypto-Assets Regulation — европейский регламент, устанавливающий правила регулирования криптоактивов и услуг, связанных с ними, принятый в 2023 году
[15] Risk-Weighted Assets (RWA)
[16] Капитал первого уровня - основной капитал банка, включающий акционерный капитал, нераспределённую прибыль и иные резервы, которые используются для покрытия убытков и обеспечения устойчивости банка
[17] https://www.legis.la.gov/legis/BillInfo.aspx?s=24rs&b=HB488&sbi=y
[18] https://www.pmddtc.state.gov/ddtc_public?id=ddtc_kb_article_page&sys_id=24d528fddbfc930044f9ff621f961987
[19] Правила международной торговли оружием США

организациями, вызывающими особую обеспокоенность. Такие компании не могут заниматься майнингом, иначе штраф – до 1 млн долл. или до 25% от стоимости доли, принадлежащей компании-нарушителю в этом бизнесе.

Также закон запрещает властям Луизианы принимать платежи в цифровых валютах центральных банков и участвовать в их тестировании. Однако в Луизиане можно участвовать в поддержании работы блокчейна — держать компьютеры, помогающие сети работать, а также заниматься майнингом дома.

Опыт Таиланда

В августе 2025 г. Тайская Комиссия по ценным бумагам и биржам предложила концепцию регуляторной песочницы для криптовалют[20], чтобы предоставить возможность иностранным туристам обменивать криптовалюты на тайский бат для оплаты покупок в стране. Стартовал пилотный проект TouristDigiPay[21], позволяющий туристам через лицензированные криптовалютные платформы и кошельки конвертировать криптовалюты в бат. После обмена средства зачисляются на специальный туристический электронный кошелёк, с которого можно оплачивать товары и услуги по QR-кодам у местных продавцов. Проект рассчитан на 18 месяцев и предназначен только для иностранных туристов, временно проживающих в Таиланде. При этом установлены лимиты на операции, например, не более 50 000 бат (1 500 долл.) в месяц на оплату мелких покупок. Проект особенно актуален для российских туристов, которые сталкиваются с ограничениями при оплате банковскими картами за рубежом.

Опыт России

В России уже приняты меры, аналогичные подходу ЕС, предусматривающие количественное ограничение в 1% капитала для криптовалют: в мае 2025 г. Банк России опубликовал Информационное письмо, рекомендовав кредитным организациям самостоятельно оценивать риски по операциям с цифровыми валютами, обеспечить полное покрытие таких вложений собственными средствами (капиталом) и устанавливать по ним лимит — не более 1% от собственных средств.

Также в отличие от Гонконга и Таиланда, где внимание уделяется регулированию поставщиков услуг и созданию «песочниц» для стимулирования туризма, в России таких инициатив пока нет. Однако действует закон о майнинге: заниматься им могут только компании и ИП, зарегистрированные в реестре ФНС, такой подход сопоставим с мерами США, где ограничивается участие иностранных компаний в майнинг-бизнесе.

2. Ценообразование на платформах

Опыт Китая

Китай опубликовал проект Правил ценообразования для платформ и продавцов в электронной коммерции[22].

Платформе запрещается: повышать тарифы, вводить штрафы, отменять ценовые субсидии или скидки для продавцов, ограничивать трафик, блокировать продавца, снижать обзор его товаров, вводить иные ограничения, с целью:

1) вынудить продавца участвовать в распродажах или скидках;

2) ограничить возможность продавца предлагать оптимальные цены на товары, услуги на разных платформах (ограничение практики паритета цен);

3) подключать систему автоматического сопоставления цен, автоматического снижения цен и пр.;

4) иным образом ограничивать право продавцов на ценообразование.

Исключение составляют платформы с едиными методами ценообразования, как платформы такси.

Если платформа изменяет комиссию, требуется учитывать финансовое положение продавцов для разумного определения тарифов, необоснованные платежи запрещены. Если тарифы меняются, требуется провести общественные обсуждения (не менее 7 дней), а если продавца не устраивают новые тарифы, платформа должна позволить расторгнуть договор без последствий.

[20] https://www.sec.or.th/EN/Pages/News_Detail.aspx?SECID=11899&NewsNo=173&NewsYear=2025&Lang=EN

[21] https://www.nationthailand.com/business/digital-assets/40054107

[22] https://www.samr.gov.cn/hd/zjdc/art/2025/art_65b6620cb5114ea49c72494b084d3e42.html

Если применяются разные цены для разных категорий потребителей в зависимости от условий сделки, требуется заранее публично раскрывать правила формирования цен. Также требуется раскрывать правила дифференцированного по времени ценообразования (динамическое ценообразование) с объяснением факторов, влияющих на формирование цены.

При проведении акций, распродаж необходимо на видном для потребителя месте публиковать правила акции, сроки её проведения, указывать базовую цену, от которой рассчитана скидка. Если платформа субсидирует цены продавцов, требуется раскрыть информацию о правилах и сроках субсидирования. Если товары или услуги продвигаются посредством платного ранжирования (например, плата продавца за повышение видимости), требуется явным образом указать, что это «реклама».

Запрещаются антиконкурентные практики:

1) продавать товары, услуги по цене ниже себестоимости для вытеснения конкурентов или монополизации рынка (хищническое ценообразование);

2) устанавливать разные цены на один и тот же товар, услугу при равных условиях сделки, основываясь на готовности платить или предпочтениях потребителя, используя данные, алгоритмы без ведома потребителя. Таким образом ограничивается дискриминация при алгоритмическом ценообразовании;

3) использовать выражения, подогревающие ожидание роста цен, например, ложные сведения о дефиците товаров, высоком спросе и пр.;

4) привлекать потребителей или продавцов низкими ценами, а затем выставлять счета по высоким ценам, обещать ложные скидки, не указывать или намеренно занижать условия цены, вводя в заблуждение и пр.

Платформы и продавцы обязаны предоставлять потребителям возможность отмены автоматических списаний, включая бесконтактную (беспарольную) оплату, подключение услуг страхования и других дополнительных услуг, автоматическое продление подписок и пр.

Опыт России

В России Закон о платформенной экономике не регулирует вопросы ценообразования на платформах, однако платформа вправе делать скидку на товар продавца только получив его письменное согласие с указанием цены, количества товаров со скидкой и срока участия в скидке. Без согласия продавца платформа может вводить скидки только за свой счет.

3. Регуляция персональных данных

Опыт США

Агентство Калифорнии по защите конфиденциальности провело консультации по внедрению единого портала «DROP» (по Закону об удалении 2023 г.[23]), если раньше потребители Калифорнии могли отказаться от продажи их данных третьим лицам только в момент сбора их данных компаниями, то теперь создается централизованная государственная платформа, через которую потребители смогут найти брокеров данных, которым компании уже передали их данные, и запросить у них удаление своих данных[24]. DROP брокер данных должен обрабатывать запросы на удаление данных как минимум каждые 45 дней. После обработки запроса требуется уведомить запросившего потребителя: были ли в базе данных брокера найдены данные этого пользователя и удалены. При этом запрещено использовать портал DROP для контактирования с потребителями вне процедуры удаления данных. Таким образом, организация единой платформы для работы брокеров данных в Калифорнии упрощает задачу потребителям в реализации права на удаление данных, оказавшихся у брокеров данных.

В США генеральные прокуроры 37 штатов направили компании Meta[25] письмо в связи с введением в Instagram новой функции по обмену данными о местоположении[26], т.к. отображение точного

[23] https://digitalpolicyalert.org/change/13671-california-privacy-protection-agency-rules-on-data-broker-registration-and-accessible-deletion-mechanism

[24]https://www.skadden.com/insights/publications/2023/12/californias-new-data-deletion-law-imposes

[25] Деятельность компании Meta признана экстремистской и запрещена на территории Российской Федерации

https://digitalpolicyalert.org/event/32796-attorneys-general-of-37-states-announced-investigation-into-instagram-over-location-sharing-feature

[26] https://illinoisattorneygeneral.gov/News-Room/Current-News/Protect%20Instagram%20User%20Privacy%20Multistate%20AG%20Letter.pdf?language_id=1

местоположения пользователей в режиме реального времени на карте увеличивает риск их преследований и домогательств, особенно несовершеннолетних. Компании рекомендуется ограничить использование этой функции для несовершеннолетних, ввести предупреждения для взрослых о рисках трансляции местоположения, обеспечить возможность отказа от использования функции.

Опыт Австрии

В августе 2025 г. суд в Австрии [27] признал нарушение австрийской медиагруппой Der Standard требований Регламента ЕС по защите персональных данных (GDPR) в отношении сбора согласия через механизм «плати или соглашайся» («Pay or OK»)[28]. Данная практика платы за доступ к контенту рассматривалась в предыдущем выпуске Мониторинга[29].

Ранее Управление по защите данных по обращению правозащитной организации Noyb выявило, что новостное издание Der Standard вынуждало пользователей либо соглашаться на все цели обработки данных, включая автоматизированный анализ данных, таргетированную рекламу, доступ к социальным сетям, нажатием одной кнопки «ОК», либо оплатить подписку на издание для доступа к контенту платформы. В Суде Der Standard доказывало право собирать данные пользователей, ссылаясь на исключение для свободы СМИ (п. 2 ст. 85 GDPR)[30]. Однако Суд указал, что механизмы пакетного согласия нарушают нормы GDPR (принцип ясности согласия (ст. 5), условие законности обработки на основе согласия (ст. 6)), поскольку пользователь должен иметь возможность выбрать, для каких конкретных целей он дает согласие. Нажатие одной кнопки «ОК» не является добровольным, так как не оставляет пользователю возможности выбора цели обработки данных и поэтому является недействительным. Исключение GDPR для журналистики в данном случае не применимо, поскольку обработка данных осуществлялась для таргетированной рекламы, которая не может считаться журналистской деятельностью. Суд потребовал прекратить обработку ранее собранных данных и удалить их.

Однако возник вопрос, какие данные Der Standard должна удалить? Суд подтвердил, что удалению подлежат все поведенческие пользовательские данные, в том числе так называемые «строки прозрачности и согласия» – записи о выборе пользователя при предоставлении согласия (например, настройки cookie-файлов). Суд считает такие данные персональными, поскольку в сочетании с адресами интернет-протокола ТС-строки позволяют идентифицировать пользователей.

Опыт России

В августе Минцифры представило проект требований к сбору и обработке персональных данных операторами данных[31]. Цель поправок – расширить контроль субъектов в отношении их собранных данных путем предоставления возможности отслеживания через «Госуслуги», кто и каким образом обрабатывает их данные.

Субъект данных получает возможность предоставлять согласие на обработку данных по типовой форме, разработанной Роскомнадзором, и управлять согласием через «Госуслуги» (например, получать информацию об обработке данных или обжаловать действия оператора данных в Роскомнадзор). Это обязывает операторов данных передавать сведения, запрашиваемые субъектом персональных данных, в систему «Госуслуги». В результате предлагаемые нормы должны установить централизованный механизм публичного контроля над отношениями между физическими лицами и компаниями в части обработки их данных.

4. Развитие открытых ИИ-моделей и прав на ИИ-контент

Опыт ОЭСР

В августе 2025 г. ОЭСР представила отчет об «открытости» ИИ: как в странах может внедряться институт свободно

[27] https://digitalpolicyalert.org/event/32858-federal-administrative-court-issued-ruling-against-publishers-of-derstandardat-over-pay-or-consent-mechanism-violations
[28] https://noyb.eu/sites/default/files/2025-08/20250818145608738p_Redacted.pdf
[29] См. Мониторинг №7 (19) (Июль 2025).
[30] Согласно п. 2 ст. 85 GDPR государства-члены ЕС на уровне национального законодательства должны предусматривать для журналистской деятельности исключения из требований к защите ПД
[31] https://regulation.gov.ru/projects/159652

распространяемых элементов моделей ИИ. ОЭСР рекомендует регуляторам детализировать понятие «open-source ИИ» или «ИИ с открытым исходным кодом»[32] в регулировании ИИ за счет внедрения в законодательство уровней открытости систем ИИ[33]. ОЭСР отмечает, что термин «open-source ИИ» неточно описывает, какие компоненты ИИ открыты: веса[34] модели, код или данные. Например, раскрытие только весов может считаться «open-source», но фактически ничего не даёт без исходного кода. Раскрытие этих компонентов - ключевой инструмент прозрачности: третьи лица могут проверять качество и риски модели, находить ошибки и искажения, лучше объяснять выводы системы. ОЭСР предлагает описывать уровни открытости по доступности компонентов: «открытая модель» (веса и базовое описание), «открытые инструменты» (добавляются коды обучения и оценки, ключевые датасеты), «открытая наука» (раскрыт весь цикл разработки и материалы).

Важно внедрять в регулирование «открытые лицензии», позволяющие свободно использовать объекты интеллектуальной собственности (в том числе системы ИИ). Лицензии различаются по цели. Например, разрешительные допускают использование открытых элементов ИИ при указании разработчика. Они ускоряют разработку и внедрение: можно свободно экспериментировать и продавать решения при соблюдении условий. Но возникает риск злоупотреблений, поэтому их нужно дополнять проверками: не распространяется ли вредоносное ПО, не нарушаются ли авторские права, не используются ли неправомерно данные. Другой вид - copyleft-лицензии: тот, кто использует в продукте элементы ИИ из открытого доступа, обязан распространять свой продукт на тех же условиях.

ОЭСР, внедряя такие лицензии, подчёркивает, что регулятор должен обеспечивать законность и безопасность публикуемых компонентов ИИ и данных. Рекомендуются требования к описаниям: какие элементы публикуются и какие источники данных использованы. Компоненты должны проверяться на безопасность и соответствие заявленным свойствам.

Опыт США

В августе 2025 г. в штате Арканзас вступил в силу закон[35] о правах на ИИ-контент. По умолчанию, если человек даёт инструкции генеративной системе, передаёт данные и получает контент (текст, изображение, код и т.д.), право на результат принадлежит ему. Если он предоставляет данные для обучения, владельцем обученной на их основе версии становится он. Данные должны быть получены законно и права не переданы по договору разработчику/провайдеру. В случае с работниками, если работа с ИИ входит в их обязанности, то права на контент принадлежат работодателю.

Закон уточняет: нельзя присвоить то, что нарушает чужие авторские и иные права. Если при запросе или передаче данных использованы чужие объекты авторских прав или персональные данные, у лица не возникает прав ИС (интеллектуальной собственности) на сгенерированный контент. Открытым остаётся вопрос, кто владелец модели, обученной на данных многих лиц: закон это не решает.

Закон снимает спор о праве на итог генерации (контент), сам запрос, предоставленные данные и обученную на них модель. Если компания законно предоставляет данные для обучения, она получает право собственности на обученную модель. Закон снижает риск конфликтов в совместных проектах: стороны могут заранее установить иной порядок владения - действуют условия договора. Например, при дообучении модели поставщика на данных заказчика можно разделить права: «веса» и их обновления остаются у поставщика, заказчик получает лицензию для внутреннего использования.

[32] Общепринятого определения «open-source ИИ» нет, обычно под этим понимаются модели ИИ, у которых ключевые части опубликованы в открытом доступе и разрешены к свободному использованию: исходный код (как модель обучают и как она работает), обученные «веса» и сведения о данных.

[33] https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/08/ai-openness_958d292b/02f73362-en.pdf

[34] «Веса» - это числовые параметры модели ИИ, которые она «выучивает» во время обучения. Модели с открытыми весами - это модели ИИ, у которых можно свободно скачать и запускать веса, но не обязательно открыт весь остальной «набор»: данные обучения, часть кода или инструменты могут быть закрыты

[35] https://arkleg.state.ar.us/Bills/Detail?id=HB1876&ddBienniumSession=2025/2025R

Пользователь обладает авторскими правами на контент, если использованные данные принадлежат ему на законном основании. Это решает вопрос прав на ИИ-контент при нарушении авторских прав пользователем. Права ИС на такой контент не возникают, а фрагменты (например, текста или кода), схожие с чужим объектом ИС, будут принадлежать правообладателю при доказанном нарушении.

Опыт России

В России внедрены некоторые меры стимулирования развития open-source ИИ. Например, расходы на разработку платформ для «умных помощников» с открытым кодом могут учитываться в двойном размере для снижения налога на прибыль организаций. Однако нормы, учитывающие специфику режима открытых лицензий на ИИ, в России не приняты. При их формировании стоит обращать внимание на рекомендации ОЭСР по требованиям к описаниям распространяемых по открытой лицензии частей ИИ, а также к указанию источников данных и обеспечению возможности проверки таких частей на безопасность.

В России нет и специального регулирования интеллектуальных прав на сгенерированный ИИ контент и модели ИИ, обученные на принадлежащих третьим лицам данных. Обсуждение таких вопросов в ГД РФ запланировано на осень 2025 г.[36] При обсуждении следует обращать внимание на следующие вопросы: на чьих данных обучена модель ИИ, сгенерировавшая контент; предоставляет ли собственные данные пользователь, который сформировал запрос для ИИ на генерацию контента.

5. Данные в конкуренции

Опыт Китае

Верховный суд представил подборку дел в сфере конкуренции, связанных с использованием данных[37]. Так, в одном из дел компания А (ответчик) скопировала из приложения компании Б (истец) более 50 тыс. видеороликов, которые содержали код приложения компании Б, никнеймы пользователей и их аватары. Компания А фактически использовала размещенные на платформе Б данные и перенесла их на собственную платформу для публичного распространения. Компания А сослалась на отсутствие у компании Б прав интеллектуальной собственности на контент пользователей, поэтому такой перенос не нарушает права компании Б.

Суд решил, что компания Б осуществляла агрегирование данных, размещённых пользователями, которые загружали свои видеоролики на основе пользовательского соглашения по правилам платформы и через ее техническую поддержку. Поэтому загруженные пользователями данные обладают высокой коммерческой ценностью. Кроме того, компания Б вложила существенные ресурсы (людские, финансовые) в формирование и накопление данных и привлекла пользовательский трафик, что придало совокупности данных дополнительную экономическую ценность. Поэтому коммерческий интерес компании В, связанный с владением и коммерческой эксплуатацией совокупности данных, подлежит правовой защите даже если компания Б не обладает правами ИС в отношении таких данных. Суд признал нарушение конкуренции, так как перенос данных с платформы Б на платформу А привел к идентичности предлагаемого пользователям контента, то есть компания А попыталась «заменить» услуги платформы компании Б, чем нарушило ее хозяйственный интерес.

В другом деле компания А (истец) управляла сайтом для соискателей по поиску работы, в том числе предоставляла возможность работодателям осуществлять поиск работников по резюме, скачивать, пересылать резюме и пр. При этом компания Б (ответчик) предоставляла услуги по обработке резюме и управлению наймом для работодателей и пр. На сайте компании Б можно было привязывать внешние аккаунты, например, аккаунт на сайте компании А или на других сайтах, чтобы работодатели могли централизованно обрабатывать резюме со всех сайтов. Для этого работодатель должен был авторизоваться, введя логин и пароль от своего аккаунта на сайте А (или других сайтов), после чего системы автоматически

[36] https://iz.ru/1944845/2025-08-29/v-gosdume-khotiat-zakrepit-avtorskoe-pravo-na-proizvedeniia-s-ii

[37] https://eastlawlibrary.court.gov.cn/court-digital-library-search/page/portal/newsDetail.html?id=44aad9946d2b414a9ee1b59b965192e6&utm

синхронизировались, и резюме с сайта А попадали в личный аккаунт работодателя на сайте Б для дальнейшей обработки. Однако за счет связывания аккаунтов двух платформ резюме с сайта компании А попадали в информационные системы компании Б. В результате против компании В был подан иск о недобросовестной конкуренции, связывая аккаунты, компания Б использовала логины и пароли работодателей, обходила механизмы защиты данных компании А (например, капчи) и автоматически получала, сохраняла и использовала резюме, собранные компанией А.

Однако Суд признал отсутствие акта недобросовестной конкуренции, признав подобное поведение вопросом права работодателя на перенос собранных им данных (в т.ч. резюме) с одной платформы на другую. Кроме того, перенесенные резюме сохранялись исключительно в аккаунтах работодателей и не попадали в общую базу данных резюме компании Б.

Опыт России

В России на данный момент вопрос использования данных в антиконкурентных практиках не регулируется[38]. Однако ФАС учитывает вопрос доступа к данным крупных платформ, например, при определении доминирующего положения. Так, ФАС оценивала данный фактор в расследовании против HeadHunter 2019 г.[39], где компания создавала труднопреодолимый барьер для входа на рынок других платформ, которым необходимо обеспечить наличие большой базы соискателей и работодателей.

[38] Например, в рамках Принципов взаимодействия участников цифровых рынков»[38] 2022 г.

[39] https://br.fas.gov.ru/ca/upravlenie-regulirovaniya-svyazi-i-informatsionnyh-tehnologiy/8e4961ce-3f9c-4b37-9f4b-b2804deeec88/