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

- **Защита потребителей иммерсивных технологий**
- **Криптовалюты как товары**
- **Обманные практики онлайн**
- **Ответственный ИИ в бизнесе и власти**
- **Доступ автовладельцев к данным своих машин**
- **Регулирование управления данными**

Мониторинг №9 (21) (Сентябрь 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.

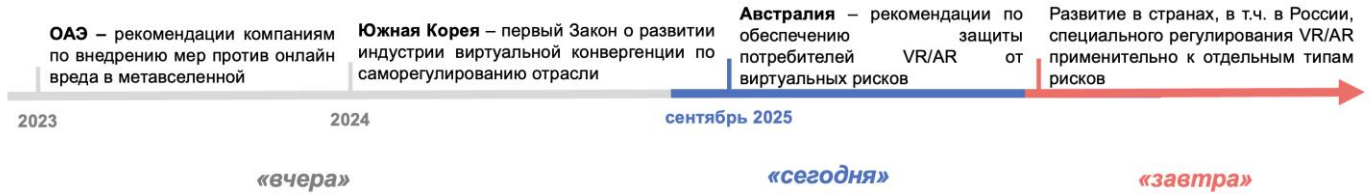
«Опять сентябрь, как тьму времен назад,
и к вечеру мужает юный холод.
Я в таинствах подозреваю сад:
все кажется — там кто-то есть и ходит.»
Б. Ахмадулина

В сентябре 2025 г. можно выделить 6 событий, которые определяют тренды развития регулирования цифровой экономики в мире.

Тренд № 1. Защита потребителей иммерсивных технологий

В сентябре 2025 г. Австралия выпустила обзор[1] рисков иммерсивных технологий, например, чрезмерная реалистичность иммерсивных сред, что увеличивает воздействие опасного онлайн-контента на детей.

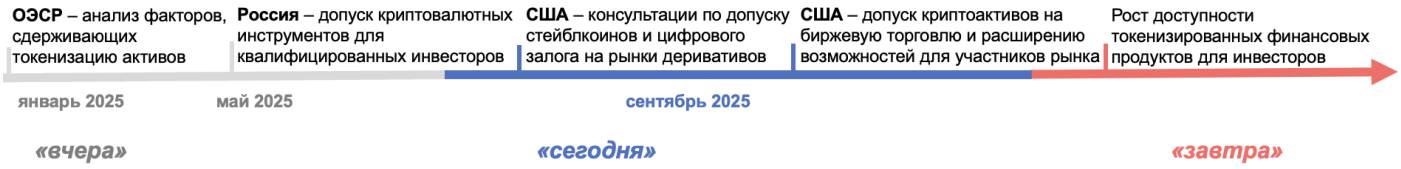
Тренд
Защита потребителей иммерсивных технологий



Тренд № 2. Криптовалюты как товары

В сентябре 2025 г. в США Комиссия по торговле товарными фьючерсами вынесла на обсуждение вопрос использования токенов как обеспечения по сделкам с деривативами. Это приведет к росту количества токенизированных активов в мире.

Тренд
Криптовалюты как товары



Тренд № 3. Обманные практики онлайн

В сентябре 2025 г. в Китае антимонопольная служба опубликовала обзор судебной практики о распространении блогерами обманной онлайн-рекламы. В США против Uber был подан иск о дискриминации инвалидов при перевозках.

Тренд
Обманные практики онлайн

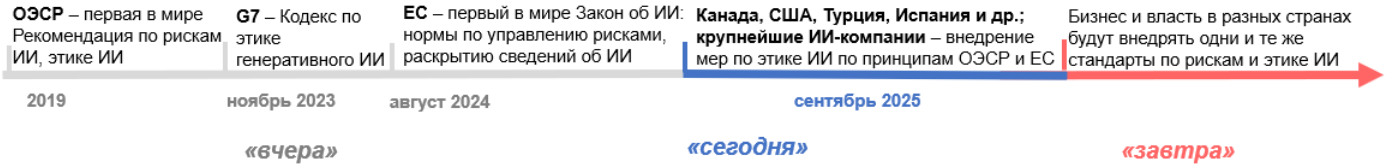
[1] https://dp-reg.gov.au/sites/default/files/documents/2025-09/DP-REG%20-%20Examination%20of%20Technology%20-%20Immersive%20Technologies_0.PDF

Тренд № 4. Ответственный ИИ в бизнесе и власти

В августе 2025 г. ОЭСР определила тренд: и компании, и государства следуют одним и тем же международным стандартам этики и управления рисками ИИ, которые заложены ОЭСР и ЕС. В будущем эти практики превратятся в схожее в различных странах законодательство.

Тренд

Ответственный ИИ в бизнесе и власти

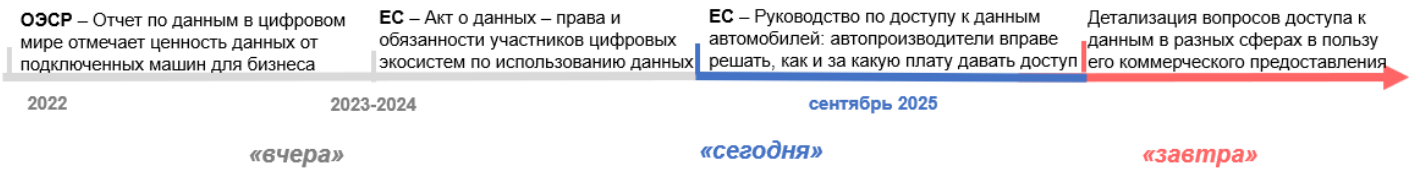


Тренд №5. Доступ автовладельцев к данным своих машин

В сентябре 2025 г. ЕС выпустил правила предоставления производителями доступа к данным автотранспортных средств для их владельцев.

Тренд

Доступ автовладельцев к данным своих машин

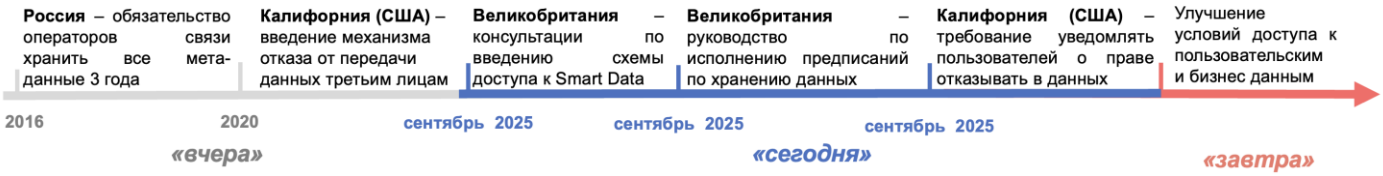


Тренд №6. Регулирование управления данными

В сентябре 2025 г. в Великобритании обсуждался вопрос о необходимости введения схемы Smart Data – схемы управления частными данными для пользователей и компаний, а также правил продления хранения данных. В Калифорнии (США) компании обязаны уведомлять пользователей о возможности отказаться от передачи собираемых данных третьим лицам.

Тренд

Регулирование управления данными



Также в сентябре 2025 г. Министерство транспорта (Минтранс) подготовило **законопроект об ответственности за ДТП с участием беспилотных автомобилей** (ВАТС[2]) и определении лиц, ответственных за их эксплуатацию[3]. Впервые попытка разработать такой законопроект была предпринята еще в 2021 г.

Минтранс предлагает считать следующих ответственных за эксплуатацию ВАТС:

- изготовитель ВАТС, если авария произошла из-за неправильной работы системы управления ВАТС;
- владелец – при несоблюдении правил эксплуатации или внесении несанкционированных изменений в конструкцию
- авторизованный сервисный центр несёт ответственность за ДТП, вызванное некачественным техобслуживанием, ремонтом или невыполнением обновлений ПО;
- оператор дистанционной поддержки[4] – при неисполнении своих обязанностей.

[2] Высокоавтоматизированное транспортное средство.
[3] https://www.vedomosti.ru/technology/articles/2025/10/01/1143267-mintrans-opredelilsya-s-otvetstvennostyu
[4] Лицо, обеспечивающее удалённый мониторинг и техническую помощь при эксплуатации ВАТС, не вмешиваясь в его непосредственное управление.

В законопроекте также устанавливаются требования к сертификации, техобслуживанию и допуску ВАТС на дороги.

Определение ответственности стало одним из ключевых вопросов, поскольку действующее законодательство не учитывает случаи, когда автомобилем управляет система ИИ. В таких ситуациях ответственность нужно определять в зависимости от того, произошло ли ДТП из-за действий водителя или из-за ошибки системы управления автомобилем, и если виновата система – выяснять, кто допустил этот сбой.

Ключевые аспекты

1. Защита потребителей иммерсивных технологий

Опыт Австралии

В сентябре 2025 г. Австралия выпустила обзор[5] рисков при использовании иммерсивных технологий. Технологии позволяют пользователям взаимодействовать с цифровым контентом в Интернете на уровне восприятия (в 3D), который может ощущаться почти как реальный мир, но уровень погружения в «искусственный» может отличаться.

Выделяются технологии: виртуальной реальности (VR[6] как очки виртуальной реальности, шлемы); дополненной реальности (AR[7] как приложения «примерки» товара к интерьеру); смешанной реальности (MR[8] как создание виртуальных аватаров человека). В мире прогнозируется[9] увеличение размера рынка VR/AR технологий: на 33,16% (с 20,43 млрд в 2025 г. до 85,56 млрд долл. к 2030 г.).

Иммерсивные технологии создают риски:

1) неправомерного сбора большого массива персональных данных (особенно чувствительных). Основной риск нарушения – сложность дать осмысленное согласие на их сбор, так как пользователь может не осознавать, какая информация собирается (например, данные об особенностях движения тела, физических реакциях, психографические данные и т.д.)[10], что может использоваться для идентификации пользователя без его ведома. Австралия предлагает интегрировать меры защиты при создании устройств, приложений: механизм контроля согласия на сбор[11], возможность отключать отдельные функции (как обмен информацией о местоположении или отслеживание движения глаз) до тех пор, пока пользователь не включит их, возможность удалять данные (функция «удалить аватар» со стиранием всех данных);

2) нарушения стандартов безопасности в Интернете (особенно детей). Технологии могут обеспечивать анонимность (например, путем замены реального человека его цифровой копией – аватаром), и могут использоваться злоумышленниками для вовлечения детей в сексуализированное насилие за счет эмоционального воздействия. Закон Австралии о безопасности в интернете 2021 г. разделил контент по уровню опасности на «материал 1-го класса» (деструктивный контент, запрещенный к показу), «материал 2-класса» (контент, ограниченный по возрасту). Контент (например, MR-приложений) может относиться и к классу 1, что потребует от поставщиков ограничить доступ к нему, предоставлять ежегодные отчеты о мерах предотвращения распространения такого контента[12];

3) нарушения прав потребителей через манипулирование поведением из-за чрезмерной реалистичной и эмоциональной интенсивности контента. Например, дипфейки в виде 3D аватаров знаменитостей могут вводить в заблуждение пользователя, провоцируя его сделать покупку товара или вложиться в какую-то финансовую лотерею.

Опыт России

Задача развития VR/AR технологий в России поставлена еще в Дорожной карте развития «сквозной» цифровой технологии «Технологии виртуальной и дополненной реальности» 2019 г. В рамках национального проекта «Цифровая экономика» ставится задача по разработке стандартов обработки массивов больших данных, стандартов информационной безопасности в системах VR/AR. При этом в России остаются

---

[5] https://dp-reg.gov.au/sites/default/files/documents/2025-09/DP-REG%20-%20Examination%20of%20Technology%20-%20Immersive%20Technologies_0.PDF

[6] Такие технологии создают эффект полного погружения в искусственную среду, например, специальные симуляторы для обучения врачей или пилотов.

[7] Такие технологии позволяют накладывать отдельные искусственные цифровые объекты на реальный мир.

[8] Такие технологии объединяют виртуальную и дополненную реальность: то есть создается и цифровой объект, который накладывается на реальность, а также система позволяет с ним взаимодействовать.

[9] https://www.mordorintelligence.com/industry-reports/virtual-augmented-and-mixed-reality-market

[10] Например, виртуальные шлемы могут собирать данные о движении глаз, мимике, поведенческих особенностях и пр.

[11] К примеру, уведомлять пользователя перед началом сбора данных о том, что начинается такой сбор (например, может выпадать интерфейс: приложение использует данные о движениях головы, разрешаете ли вы производить такой сбор?).

[12] Промышленные стандарты 2024 г. по безопасности в Интернете.

нерешенными вопросы необходимости соблюдения в метавселенных законодательства о персональных данных, защите детей, регулировании имущественных отношений и пр.

В России с развитием технологии также могут вводиться меры регулирования отрасли (как в Южной Корее и ОАЭ), в первую очередь саморегулирования, включая вопросы защиты данных, эмоционального влияние технологии на детей, распространения незаконного контента в иммерсивных средах и пр.

2. Криптовалюты как товары

Опыт США

В сентябре 2025 г. Комиссия по торговле товарными фьючерсами (CFTC) начала обсуждение вопроса использования токенизированных активов[13] и стейблкоинов[14] в качестве обеспечения на рынках деривативов.

Деривативом могут быть фьючерсы на нефть, опционы на акции Apple и др. Владение деривативом означает право на заключение соглашения о покупке или продаже нефти или акций по определенной цене в будущем. Такие сделки сопряжены с риском, поэтому требуют обеспечения. CFTC обсуждает:

1) какие пилотные проекты по использованию токенов в качестве обеспечения можно запустить[15];

2) какие правила по работе с залогом нужно обновить, чтобы токены признавались допустимым видом обеспечения;

3) какие шаги уже предпринимают компании для внедрения токенизированного обеспечения по сделкам с деривативами.

Сформированы критерии приемлемости такого обеспечения. По итогам консультаций определены меры официального признания стейблкоинов и токенов допустимым залогом при расчётах и торговле деривативами[16].

Реализация инициативы на рынке потенциально может существенно изменить криптоэкономику: на конец 2024 г. в обеспечении по различным сделкам использовались различные активы на сумму 0,9 трлн долл.[17], их токенизация может увеличить рынок криптоэкономики на треть (3,7 трлн долл., на 10 октября 2025)[18]. Положительное решение вопроса также может позволить разнообразить рынок обеспечения за счет токенизации материальных активов, «расщепления» права владения на них.

Также в сентябре 2025 г. CFTC и Комиссия по ценным бумагам заявили о выработке порядка допуска к биржевой торговле криптоактивами на спотовом рынке (рынок, где сделки проводятся практически сразу, например, продавец в момент сделки передает криптовалюту и получает фиат). [19]

Регуляторы подтвердили, что действующие правила уже позволяют организовывать торговлю криптовалютами (как Bitcoin, Ethereum) в качестве товаров при соблюдении требований к защите инвесторов и прозрачности торгов. Дополнительно регуляторы обозначили практические вопросы, которые участникам рынка необходимо проработать: как устанавливаются и поддерживаются требования маржинальности, каким образом организованы клиринг и расчёты, как налажен обмен данными между площадками (для мониторинга базовых рынков[20] и предотвращения манипуляций).

Реализация инициативы окажет влияние на криптобиржи по всему миру, так как в юрисдикцию CFTC теперь попадут не только сами криптовалюты, но и биржи, на которых они торгуются. CFTC уже выступили с инициативой регулировать право иностранных криптобирж предоставлять услуги американским резидентам (такое право с конца 1990-х годов действует в отношении классических товарных бирж). Зарубежные криптобиржи смогут

[13] Цифровая форма залога, представляющая права на реальные активы и используемая для расчётов и гарантий по сделкам.
[14] Токены, стоимость которых привязана к стабильному активу (например, доллару или золоту).
[15] Например, Coinbase планирует пилотный проект, где USDC будет выступать как залог в расчётах по фьючерсам.
[16] Производные финансовые инструменты (фьючерсы, опционы)
[17] https://www.fia.org/sites/default/files/2025-06/FIA%20-%20Tokenisation%20-%20Accelerating%20the%20velocity%20of%20collateral.pdf
[18] https://coinmarketcap.com
[19] https://www.sec.gov/newsroom/speeches-statements/sec-cftc-project-crypto-090225
[20] Наблюдение и анализ сделок, цен и объёмов торгов на рынках, где обращаются базовые активы, чтобы выявлять манипуляции, аномалии и риски, которые могут повлиять на связанные с ними деривативы.

обслуживать клиентов из США, если их юрисдикция соответствуют сопоставимым стандартам регулирования[21].

Опыт России

В России пока нет решений аналогичных инициативам в США, однако Банк России в мае 2025 г.[22] разрешил финансовым организациям предлагать квалифицированным инвесторам инструменты с доходностью, зависящей от цен криптовалют (деривативы, ценные бумаги, ЦФА) при консервативной оценке рисков (полное покрытие капиталом и лимиты в 1% капитала, о которых мы рассказывали в Мониторинге №8 (20)). При этом ЦБ подчёркивает, что не поддерживает прямые инвестиции в криптовалюты, считая их высокорискованными.

В перспективе российский финансовый рынок также рассмотрит возможность использования токенизированных активов (например, ЦФА[23]) в качестве обеспечения, учитывая их потенциал для ускорения и упрощения расчётов.

3. Обманные практики онлайн

Опыт Китая

В сентябре 2025 г. антимонопольная служба Китая опубликовала практику расследований ложной рекламы в электронной коммерции. Так, госпиталь Дэсинь в Шанхае для рекламы медицинских услуг в коротких видео (shorts) нанял 169 блогеров, которые рассказывали о качестве услуг, которыми якобы сами пользовались. В другом кейсе компания продвигала проекты виртуальной реальности через блогеров, которые публиковали видео использования VR-приложений. Однако выяснилось, что ни в одном из дел блогеры реально не пользовались услугами компаний. Участники расследований получили штрафы от 100 до 200 тыс. юаней (от 1,15 до 2,3 млн руб.) за обман, использование дипфейков.

Стоит отметить, что Китай и другие страны ужесточают регулирование рекламы блогеров, требуя, например, предоставления достоверной информации об опыте использования блогером продукта, требование делать пометку, что продукты, о которых рассказывают блогеры, являются рекламой. Наиболее строгое регулирование за последнее время ввели ОАЭ – блогеры должны получать лицензию при распространении рекламы.

Опыт США

В сентябре 2025 г. в США против Uber подан иск за дискриминацию пассажиров с инвалидностью[24]. Минюст США обвинил Uber в том, что водители отказывают в обслуживании пассажирам со служебными собаками и складными инвалидными колясками. При этом в Uber существует система «кредитов» - форма компенсации, когда, например, поездка была отменена, водитель повёл себя неправильно, или произошло списание денег по ошибке, то Uber начисляет на счёт пользователя определённую сумму в виде кредитов. Но есть лимит. И из-за большого количества отказов водителей пассажиры с инвалидностью достигали лимита, и Uber переставал предоставлять им компенсации или возмещать убытки за отменные заказы.

Кроме того, взимался незаконный сбор за уборку после служебных собак, водители нередко оскорбляли пассажиров, не предоставляли возможностей для удобства перемещения, например, не разрешали человеку с ограниченной подвижностью сесть спереди (так, одна пассажирка не смогла сидеть сзади из-за протеза ноги). При этом Uber не проводил специализированные обучения водителей, которые перевозят пассажиров с инвалидностью.

Несмотря на то что часто пассажиры сталкивались с дискриминацией со стороны водителей, Uber также несет прямую ответственность, так как является лицензируемым поставщиком транспортных услуг (наравне с таксопарками) и обязан соблюдать законодательство о защите инвалидов от дискриминации – обеспечивать провоз в транспорте служебных животных, не взимать дополнительные сборы, связанные с инвалидностью пассажира и пр.

[21] https://finance.yahoo.com/news/cftc-may-approve-foreign-crypto-150409711.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAD-3E2EI2fsEeUHT4x2jLNveV4yCA-s6V187idtDduJkPXImrm3AcuOxxv5E1Z8CXgkl07HP3MqW8rylj7vVdAg4M75faeL13EhPJBb_El4t4M_9rwacm4A_d4t7xjBK8dHNuDquYcqJkUyHhga4ONtR6izdRnIDorpy4js1a4bP

[22] https://cbr.ru/press/event/?id=24647

[23] Цифровой финансовый актив

[24] https://www.justice.gov/usao-ndca/media/1414021/dl?inline

Опыт России

В России также наблюдается тренд на ужесточение регулирования рекламы, в том числе блогеров. Так, с 1 сентября 2025 г. запретили рекламу в запрещенных социальных сетях, таких как Instagram[25]. Это может привести к уходу рекламного рынка «в тень», к снижению прозрачности и доходов рынка онлайн-рекламы, уменьшению поступлений налогов от рекламы в бюджет.

Если говорить о социальной ответственности платформ, то в России не регулируется вопрос обеспечения прав инвалидов при использовании платформ (есть требования только для перевозчиков, т.е. таксопарков, и водителей). Хотя, например, платформы такси как Яндекс такси внедрили специальные функции для пользователей с ограниченными физическими возможностями, а также имеют политики по перевозке таких людей. Вероятнее всего, регулирование социальной ответственности платформ будет развиваться за счет саморегулирования платформ и обучения водителей.

4. Ответственный ИИ в бизнесе и власти

Опыт ОЭСР

В сентябре 2025 г. ОЭСР опубликовала обзор первых отчётов компаний в рамках Хиросимского процесса по ИИ – инициатива стран G7 по формированию универсальных правил развития и использования систем ИИ. Исследовались практики компаний по 7 направлениям:[26]

1) выявление и оценка рисков организации[27]. Для этого компании, например, Microsoft, Google, OpenAI, IBM и др. проводят испытания ИИ с имитацией нападений: команды пытаются «обмануть» модель, чтобы понять, где есть риски неправильной работы системы;

2) управление рисками через процедуры и технические меры. Сначала ИИ тестируется внутри компании, потом для ограниченного круга доверенных пользователей, и только затем выводится в широкий доступ. Реализуются технические меры: очистка и отбор обучающих данных, «доводка» модели под конкретные задачи и проверка результатов запросов до того, как их увидит человек;

3) раскрытие сведений о прозрачности систем ИИ. Например, если ИИ-продукты предназначены для массовой аудитории, то компании публикуют «паспорта» моделей и отчёты о прозрачности: что умеет система, где слабые места, как её тестировали. Продавцы B2B-решений, закрепляют обязательства о раскрытии информации в договорах;

4) управление инцидентами. При инцидентах есть прописанные сценарии: кто следит, кто фиксирует, кто отвечает – компании имеют команды специалистов. Создаются горячие линии для сообщений о проблемах ИИ (у KYP.ai и Rakuten), специальные процедуры пересмотра работы высокорисковых систем ИИ;

5) создание механизмов аутентификации и отслеживания ИИ-контента. Компании внедряют маркировку сгенерированного ИИ контента (как водяные знаки) и иными способами информируют пользователя, что он взаимодействует с ИИ;

6) инвестирование в безопасность ИИ. Больше всего компании вкладывают средств в кибербезопасность, в повышение доверия к информации (например, Google разрабатывает инструменты обнаружения фейков), а также выявления дискриминационного поведения ИИ (например, Fujitsu, OpenAI проверяют модели ИИ на предмет дискриминации);

7) вклад систем ИИ в достижение общественно важных целей. Крупные компании ведут исследования по устойчивости, честности, прозрачности работы моделей и подтверждению происхождения контента (у Microsoft - сеть AI & Society и лаборатория AI Frontiers). Многие проекты нацелены на здравоохранение, образование, доступность и климат, поддерживают ЦУР ООН.

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

[26] https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/09/how-are-ai-developers-managing-risks_fbaeb3ad/658c2ad6-en.pdf

[27] Компании ориентируются либо на положения Рекомендации ОЭСР по ИИ 2019 г., либо на категории рисков по Закону ЕС об ИИ, реже – на стандарты Национального института стандартов и технологий США .

Также ОЭСР опубликовала обзор использования ИИ для госуправления[28]. Как и компании органы власти ориентируются на Рекомендацию ОЭСР по ИИ, правила Хиросимского процесса и пр. Например, в Канаде действует обязательная оценка воздействия алгоритмов для всех автоматизированных решений в госуправлении. Чаще всего (45 из 200 рассмотренных кейсов) ИИ внедряют в госуслугах – например, в Греции ИИ «читает» и анализирует документы на регистрацию недвижимости, что ускорило оценку таких сделок с нескольких месяцев до 10 минут. На втором месте по популярности – ИИ в открытом правительстве и взаимодействии государства с гражданским обществом. Например, в Архив Европарламента внедрили ИИ для помощи в поиске и анализе документов из архива. Также, ИИ часто используется в судебной деятельности, например, в Бразилии Верховный суд внедрил ИИ для первичного рассмотрения заявлений на предмет того, соответствуют ли они требованиям, и можно ли смотреть заявления по содержанию (например, подан ли достаточный пакет документов). Время рассмотрения заявлений в итоге сократилось с более чем 40 минут до нескольких секунд.

Опыт России

В России этические принципы разработки и внедрения систем ИИ заложены на уровне «мягкого» регулирования для отдельных отраслей. В Мониторинге № 7 (19) мы уже рассказывали о Кодексе этики ИИ на финансовом рынке Банка России. Также Альянс в сфере ИИ (входят Яндекс, VK, Сбер и др.) разработал добровольные кодексы: общий Кодекс этики ИИ, Кодекс этики в медицине, Декларацию по генеративному ИИ и др. Перечисленные документы частично повторяют Руководство ОЭСР по ИИ 2019 г.

Также в 2025 г. Правительство РФ инициировало эксперимент по применению генеративного ИИ в госуправлении: Минцифры разработает методические рекомендации и правила его проведения (включая критерии к сервисам и ограничения по сценариям применения), участие предусмотрено для федеральных и региональных органов.[29] Представляется, что в ближайшие 1-2 года Россия перейдет от мягкого регулирования к базовым обязательным требованиям для ИИ в госуправлении и в отдельных секторах (например, транспорт, финансы, медицина). На базе эксперимента по генеративному ИИ Минцифры может оформить типовые методики: испытания систем ИИ перед выпуском на рынок, процедуры управления инцидентами, механизмы рассмотрения жалоб. Могут также внедряться отраслевые рекомендации (чек-листы для управления рисками систем ИИ по аналогии с финансовыми услугами, например, в сфере транспорта).

5. Доступ автовладельцев к данным своих машин

Опыт ЕС

В сентябре 2025 г. Еврокомиссия опубликовала руководство к Акту ЕС о данных 2023 г.[30] в отношении доступа к данным, накапливаемым автопроизводителями, возникающим при эксплуатации автомобиля и предоставлении связанных цифровых услуг. Речь идёт об автомобилях, которые собирают сведения о своём использовании (например, данные о скорости движения, температуре, пробеге, уровне топлива или заряда и неисправностях) и способны передавать их третьим лицам, а также о цифровых услугах, без которых автомобиль не сможет работать (например, удаленное зажигание, отпирание дверей, самодиагностика). Услуга признаётся «связанной», когда между автомобилем и поставщиком идёт двусторонний обмен данными, влияющий на работу машины (например, системы оптимизации маршрута). При этом беспилотные автомобили данным руководством не охватываются.

Производитель не обязан обеспечивать постоянный и непрерывный доступ пользователя к данным в любой момент времени, он вправе предоставлять данные, когда сам решит, что это «релевантно и технически возможно». Эти правила развивают политику ЕС по управлению данными, в рамках которой

[28] https://www.oecd.org/en/publications/governing-with-artificial-intelligence_795de142-en.html
[29] https://www.garant.ru/products/ipo/prime/doc/56928658
[30] https://digital-strategy.ec.europa.eu/en/library/guidance-vehicle-data-accompanying-data-act

Еврокомиссия стремится расширить возможности потребителей и компаний по контролю над данными, которые генерируют подключенные к цифровым сетям устройства.

Также производители вправе делиться данными с другими компаниями за «разумную компенсацию».

Опыт России

Специального закона, дающего пользователю и выбранным им сервисам право требовать собираемые транспортными средствами данные, в России нет. Вопросы передачи данных с частных транспортных средств производителю регулируются общими нормами о персональных данных. Из позиции Роскомнадзора по вопросу допустимости сбора поведенческих данных пользователей, включая вождение автомобиля, следует, что данные, позволяющие идентифицировать пользователя автомобиля, не могут собираться без его согласия. В ближайшее время могут появиться разъяснения со стороны регуляторов по сбору и использованию телематических данных с автомобилей и праву владельца на доступ к ним, как недискриминационный доступ независимых сервисов, осуществляющих техобслуживание подключенных автомобилей, к данным при согласии владельца.

6. Регулирование управления данными

Опыт Великобритании

В сентябре 2025 г. в Великобритании обсуждалась идея введения института доступа к пользовательским и бизнес данным «Smart Data Scheme». Smart data – любые данные пользователей и бизнеса, которые по поручению пользователя получают от компаний-держателей пользовательских данных специальные уполномоченные третьи лица (authorized third party provider, далее – ATP). В качестве ATP могут выступать финтех-стартапы, онлайн-платформы, аналитические сервисы, агрегаторы тарифов и др.

Пользовательские данные копятся у компаний, при этом пользователи не могут сами распоряжаться собственными данными, так как это технически сложно: нужно сначала запросить свои данные, потом их получить в машиночитаемом формате, затем передать другой компании (например, у которой пользователь хочет получить услугу). В рамках Smart Data Scheme пользователи могут поручить ATP получить у компаний накопленные данные (например, о банковских операциях, тарифах, энергопотреблении или подписках). Далее, когда ATP получает доступ к данным пользователя у других компаний, он может анализировать сырые пользовательские данные, создавая персонализированные цифровые продукты для самого пользователя. Например, ATP может быть поставщиком финансовых услуг и использовать данные о банковских операциях для составления финансовой консультации для пользователя.

Другое направление схемы Smart Data касается бизнес-данных. Исполнительные органы власти могут запрашивать у бизнеса раскрытие неперсональных данных, аккумулированных в бизнес-процессах: информацию о товарах, услугах, цифровом контенте, условиях их поставки, наличии, цене, качестве, о пользовательском опыте. Если данные публично раскрываются одной компанией, то другие участники рынка смогут их использовать для сравнения, анализа и улучшения своих товаров и услуг.

Технически схема Smart Data предполагает создание единых стандартов форматов данных и интерфейсов (API), через которые информация может передаваться беспрепятственно, быстро и безопасно среди участников оборота данных.

Также в Великобритании выпущено Руководство по правилам хранения данных после достижения цели их обработки. Единственная допустимая цель хранения – это сохранение данных несовершеннолетнего пользователя при расследовании его смерти. Хранение таких данных допускается только по поручению Уполномоченного органа в области информации Ofcom[31][32]. Для сравнения в

[31] Data Preservation Notices

[32] https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/consultation-on-data-preservation-notices/consultation-on-data-preservation-notices.pdf?v=402980

России действует требование к операторам связи по хранению мета-данных пользователей в течение 3 лет, однако такое требование применяется всегда и ко всем (а не для конкретной цели), что создает для компаний издержки на хранение данных, которые могут и не пригодиться госорганам.

Опыт США

В сентябре 2025 г. в Калифорнии были приняты нормы в отношении механизма opt-out – т.е. отказа от предоставления данных[33]. Теперь поставщики браузеров обязаны уведомлять пользователей о возможности отказаться от предоставления своих данных поставщикам цифровых услуг, к которым пользователь обращается через браузер, и информировать каким образом это сделать.

Опыт России

В России субъекты персональных данных по-прежнему ограничены в распоряжении своими данными, поскольку закон не предусматривает права на перенос данных между операторами. На фоне зарубежных инициатив, таких как Smart Data Scheme, это усиливает разрыв между возможностями российских и иностранных пользователей. Отсутствие инструментов вроде механизма отказа от предоставления данных способствует развитию серого рынка персональных данных и ослабляет защиту прав пользователей в цифровой экономике.

Перспективы цифровизации экономики зависят в значительной мере от качества вовлечения пользовательских данных в экономические процессы, т.е. от того, насколько осознанно и активно пользователи распоряжаются собственными данными. Поэтому в целях поддержки национального цифрового бизнеса регуляторы могут представить поправки в законодательство о персональных данных, например, в части закрепления права человека предоставлять свои необезличенные персональные данные для неопределенных общественно-значимых целей, т.е. на альтруистических началах.

[33] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202520260AB566