

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

Исключение рисков при использовании ИИ в правоохранительной
деятельности, защита прав интеллектуальной собственности при обучении
генеративного ИИ

Мониторинг №5 (Май 2024)

Мониторинг подготовлен коллективом экспертов Института экономической политики имени
Е. Т. Гайдара (Института Гайдара):

Левашенко А.Д., с.н.с. лаборатории анализа лучших международных практик Института Гайдара;

Гирич М.Г., н.с. лаборатории анализа лучших международных практик Института Гайдара;

Ермохин И.С., н.с. лаборатории анализа лучших международных практик Института Гайдара;

Магомедова О.С., н.с. лаборатории анализа лучших международных практик Института Гайдара;

Малинина Т.А., с.н.с. лаборатории анализа лучших международных практик Института Гайдара

При частичном или полном использовании материалов ссылка на источник обязательна.

«Великие, истинные дела всегда просты и скромны»

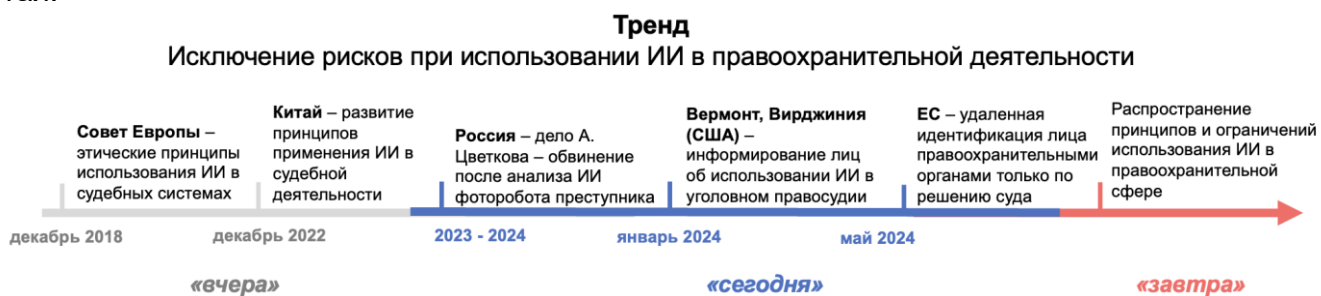
Л.Н. Толстой

В мае 2024 г. можно выделить 2 события, которые определяют тренды развития регулирования цифровой экономики.

Тренд №1. Исключение рисков при использовании ИИ в правоохранительной деятельности

В России резонансное уголовное дело против А. Цветкова, рассматриваемое в 2023–2024 гг., показало риски, которые могут возникнуть при применении искусственного интеллекта (ИИ) в правоохранительной деятельности. Специальное регулирование в этой сфере отсутствует, а инструкции МВД, касающиеся использования подобных технологий, закрыты.

В мае 2024 г. в ЕС был принят закон, который относит используемый в правоохранительной деятельности искусственный интеллект к высокорисковому, в том числе допускает его использование с разрешения суда для биометрической идентификации подозреваемых в реальном времени в общественных местах. Кроме того, системы ИИ для уголовного судопроизводства также отнесены законопроектами штатов США к высокорисковым. Советом Европы еще в 2018 г. были приняты основные положения использования ИИ в судебной деятельности: ИИ не может подменить судей, участники должны быть информированы о его применении, данные для обучения ИИ должны быть получены из легальных источников и обрабатываться понятным образом. Аналогичные положения приняты в 2022 г. Верховным судом Китая.



Тренд №2. Защита прав интеллектуальной собственности при обучении генеративного ИИ

В мае 2024 г. Китай опубликовал проект Базовых требований к безопасности генеративного ИИ, заложив требования к его операторам по мерам пресечения нарушений прав интеллектуальной собственности (далее – прав ИС). Например, если в наборе данных, на которых обучается ИИ, содержатся литературные, художественные и научные произведения, провайдер обязан провести проверку на предмет нарушений прав ИС в создаваемом ИИ контенте. Принятие этих норм вызвано судебными делами в 2023–2024 гг. Например, дело Ultraman о запрете использования контента для обучения и для генерирования ИИ без разрешения правообладателей. Аналогичный подход в ЕС и Франции, которые требуют от поставщиков услуг реализации модели «достаточно подробного резюме» – раскрытие информации об ИС, используемых для генерации контента и обучения ИИ.





Ключевые аспекты

1. Исключение рисков при использовании ИИ в правоохранительной деятельности

Опыт Европы

В правоохранительной деятельности ИИ использовался в ЕС как минимум с середины 2010-х годов, в том числе для наблюдения в общественных местах во время определенных событий (например, саммита G20 в Гамбурге)¹. Границы такого вмешательства в права людей вызвали озабоченность, в том числе депутатов Европарламента².

В мае 2024 г. в ЕС принят Закон об ИИ³, который узаконивает возможность уже для постоянного наблюдения в режиме реального времени и в любом публичном пространстве более чем за 6 тысячами человек, которые разыскиваются по европейскому ордеру за преступления.

Закон относит ряд систем ИИ, используемых в правоохранительной деятельности к «высокорисковым», что предполагает **повышенные требования** к таким системам: обеспечивать автоматическую запись событий на протяжении жизненного цикла системы ИИ; применять систему управления рисками, включая тестирование и пр.

Так, использование удаленной биометрической идентификации подозреваемых в реальном времени в общественных местах (отслеживание с помощью ИИ по камерам наблюдения) в правоохранительной деятельности запрещено, но допустимо по предварительному разрешению судебного органа в отношении некоторых особо опасных преступлений (терроризм, торговля людьми, оборот наркотиков и пр.). Список преступлений достаточно широкий.

Также разрешено профилирование лиц правоохранительными органами при уголовном расследовании, однако требуется обеспечить надзор человека за работой ИИ.

Таким образом, в ЕС возможно использование ИИ при уголовных расследованиях с соблюдением определенных требований к высокорисковым системам ИИ. Так, Закон признает риски дискриминации и нарушения фундаментальных прав при применении систем ИИ (например, на безопасность – не опасаться ареста только потому, что камера с ИИ на улице сигнализировала о совпадении изображения с преступником). Для снижения таких рисков Закон вводит требования к высокорисковому ИИ – к качеству данных, анализу рисков, человеческому мониторингу работы и решений, возможности донастройки систем ИИ.

Будет ли соблюдение этих требований достаточным, чтобы не создавать искажения, остается под вопросом. Так, если система обучена даже на репрезентативных данных, показывающих, что, например, кражи совершают люди из одной страны или одного пола, то создаются риски дискриминации – система ИИ, обучаясь на таких данных, может указывать в первую очередь именно на этих людей в качестве подозреваемых.

В ЕС предпринята попытка соблюсти баланс рисков и пользы ИИ через предъявление к высокорисковому ИИ для правоохранительной деятельности специальных требований⁴. Однако, например, Австрия считает эти меры недостаточными для гарантий прав граждан, по ее мнению, правоохранителям даются слишком большие полномочия⁵.

¹ https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf.

² <https://www.patrick-breyer.de/en/ai-act-threatens-to-make-facial-surveillance-commonplace-in-europe/>.

³ https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:PE_24_2024_INIT.

⁴ Решения исключительно на основе автоматизированной обработки персональных данных для предотвращения и

расследования преступлений или исполнения уголовных наказаний, кроме случаев, когда обеспечены гарантии вмешательства контролера-человека, были ранее запрещены Директивой ЕС 2016/680 (<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680>).

⁵ <https://data.consilium.europa.eu/doc/document/ST-9645-2024-ADD-1-REV-1/X/pdf>.

Стоит отметить, что **Совет Европы**⁶ еще в 2018 г. разработал и принял этические принципы использования ИИ в судебных системах⁷, которые легли в основу регулирования этой сферы в ЕС. В частности, в списке принципов присутствуют требования к качеству и безопасности систем, информированности пользователей и др.

Опыт США

В США отсутствует регулирование ИИ в правоохранительной сфере. Это создает проблемы соблюдения полицией прав подозреваемых и усложняет их защиту, например, в 2020 г. человек был арестован по подозрению в краже, поскольку ИИ показал его соответствие фото преступника, но кражи он не совершал⁸.

Законопроекты штатов Вермонт⁹ и Вирджиния¹⁰ (январь 2024 г.), относят системы ИИ, существенно влияющие на доступ к уголовному правосудию, к высокорисковому. Это значит, что предъявляются особые требования по управлению рисками и к данным, на которых обучен ИИ.

Подход этих штатов отличается от подходов, принятых в ЕС, по двум основным вопросам:

1) не запрещается использовать ИИ, например, для оценки риска совершения преступлений человеком только на основе его профилирования;

2) не требуется контроль человека за работой ИИ, но требуется обязательно проинформировать лиц, в отношении которых принимается решение на основе ИИ, о применении такой системы и ее целях, а в Вермонте и о том, как она работает.

В результате прозрачность систем ИИ, влияющая на право подозреваемых на защиту, обеспечивается общими требованиями к высокорисковому ИИ (о качестве используемых данных, управлением рисками), а также правом

подозреваемого получить информацию о работе ИИ.

Опыт Китая

Специальное регулирование использования ИИ в правоохранительной деятельности отсутствует. Однако в 2022 г. Верховный суд Китая выпустил аналогичные Совету Европы принципы применения ИИ в судебной деятельности¹¹. При этом в Китае заложены специальные принципы, как:

- ИИ не должен заменять судью в принятии решений;
- ответственность за вынесенное решение лежит на принимающем его лице, а не ИИ;
- право пользователя (судья, подсудимый и пр.) отказаться от продуктов ИИ при вынесении решений.

Опыт России

В России отсутствует специальное регулирование использования ИИ в уголовном процессе. При этом среди основных функций МВД России есть задача по внедрению ИИ в информационно-аналитическую систему¹², но методические рекомендации использования этих сервисов в открытом доступе отсутствуют. Закрытость такой информации усложняет анализ и оспаривание решений, принятых с использованием ИИ в системе МВД, в том числе защиту подозреваемых и обвиняемых по уголовным делам.

В 2023 г. человек был обвинен в убийствах на основании решения нейросети, что он похож на фоторобот преступника на 55% (дело против А. Цветкова)¹³. Дела, обстоятельства обвинения в которых схожи с делом А. Цветкова, в открытых источниках отсутствуют, однако в условиях недоступности данных о применении ИИ в системе МВД это может означать отсутствие не таких дел, а их огласки. С учетом существующего характера судебно-правовой системы (избрание мер пресечения, низкая

⁶ Council of Europe – международная организация, не входящая в структуру ЕС.

⁷ <https://www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment>.

⁸ <https://www.techpolicy.press/senators-explore-ai-in-criminal-investigations-and-prosecutions>

⁹ <https://legislature.vermont.gov/Documents/2024/Docs/BILLS/H-0710/H-0710%20As%20Introduced.pdf>.

¹⁰ <https://lis.virginia.gov/cgi-bin/legp604.exe?241+ful+HB747H1>.

¹¹ <https://www.court.gov.cn/fabu/xiangqing/382461.html>.

¹² Пункт 12.62 приказа от 15 июня 2021 г. № 444.

¹³ <https://www.bfm.ru/news/547759?ysclid=lw7e27jlqh27755622>.

доля оправдательных приговоров) это усугубляет риски преследования невиновных лиц и ведет к размыванию ответственности за принятые в ходе расследования решения. Возможность предъявления обвинения в результате процедуры с непрозрачным механизмом применения ИИ затрудняет установление ответственного за обвинение и защиту обвиняемого.

В России возможно:

1. Установить требования к системам ИИ, предназначенным для использования в расследовании преступлений, касающиеся используемых данных, в том числе для обучения и тестирования, управления рисками, прозрачности, контроля человеком;

2. Обеспечить правовые гарантии, что решение, сгенерированное при участии ИИ, не может быть принято без участия человека. С одной стороны, это означает, что за любое решение в итоге несет ответственность человек, с другой – привлечение его к ответственности – вопрос правоприменения.

2. Защита прав интеллектуальной собственности при обучении генеративного ИИ

Генеративный ИИ позволяет создавать новый контент (текст, компьютерный код, изображения, аудио- и видео) в ответ на запрос пользователя. Обучение такого ИИ часто происходит на открытых данных, которые могут содержать охраняемые правами ИС объекты. Это ведет к риску создания произведений, схожих с защищаемыми произведениями других авторов.

Поэтому в мае 2024 г. в Китае и ЕС были приняты первые правила о защите прав ИС при обучении генеративного ИИ, что было вызвано рядом судебных дел, когда правообладатели подавали жалобы на обучение ИИ на основе их работ без их разрешения.

Опыт Китая

В мае 2024 г. Китай опубликовал проект «Базовых требований к безопасности

генеративного ИИ»¹⁴. **Поставщики услуг генеративного ИИ должны:**

1) назначить лицо, ответственное за соблюдение прав ИС при использовании ИС системой и в генерируемом контенте;

2) иметь стратегию обеспечения соблюдения прав ИС, включая перечень рисков нарушения прав ИС;

3) при нарушении прав ИС – не использовать наборы данных с нарушением для обучения ИИ, провести проверку нарушения;

4) обеспечить механизм подачи жалоб от пользователей поставщику о нарушениях прав ИИ генеративным ИИ.

Что касается необходимости получения разрешения от правообладателей на используемый контент для обучения ИИ, в феврале 2024 г. Суд в Гуанчжоу привлек к ответственности владельца сайта, на котором предоставлялась услуга генерации контента за деньги. Суд пришел к выводу, что система работала таким образом, что по запросу пользователя создавалось изображение, которое было схоже до степени смешения с объектом интеллектуальной собственности истца. Практика суда показывает, что **ИИ, который позволяет пользователю сделать запрос о генерации контента, предполагающий копирование ИС или его отдельных элементов, будет трактоваться как нарушение законодательства о ИС.** В данном случае применяется общее правило о запрете на коммерческое использование ИС без **лицензии правообладателя**¹⁵.

При этом суд в Китае признает авторские права пользователя ИИ на сгенерированные ИИ произведения. В ноябре 2023 г. Суд Пекина принял решение по делу о нарушении авторских прав на изображение, созданное с использованием Stable Diffusion. Изображения, сгенерированные ИИ, являются «произведениями» по закону об авторских правах, так как относятся к области литературы, искусства, являются оригинальными и представляют результат интеллектуальной деятельности человека.

¹⁴ <https://www.tc260.org.cn/upload/2024-03-01/1709282398070082466.pdf>

¹⁵ Ст. 23 Закона об авторских правах https://www.most.gov.cn/ztlz/gjxjxjldh/jldh2017/jldh17xgwj/201801/t20180104_137482.html

Автором признается истец, который ввел запрос ключевых слов (вид изображения, изображаемый объект, окружение и стиль) и далее корректировал запрос. Суд исключил авторство разработчиков системы ИИ на сгенерированное изображение.

Опыт ЕС, Франции, Италии

Принятый в мае 2024 г. Закон ЕС по ИИ устанавливает обязанность провайдеров генеративного ИИ:

1) внедрять комплаенс выполнения законодательства о защите авторских прав (например, проверять используемые ИИ данные на наличие защищенных объектов ИС);

2) опубликовать подробное **описание (резюме) о контенте**, используемом для обучения модели ИИ (ч.1 ст.53), например, перечисление основных наборов данных, включая указание на крупные частные или общедоступные базы данных или архивы. Планируется разработать форму такого резюме.

В ЕС существует право использовать ИС без разрешения правообладателей в научных целях исследовательскими организациями и учреждениями культурного наследия. Аналогично ст. 23 Закона об авторских правах Китая¹⁶.

Среди стран ЕС **Франция первая** в сентябре 2023 г. представила Законопроект № 1630¹⁷ об обязательном получении согласия правообладателей при использовании объектов ИС для систем ИИ в том числе при обучении систем генеративного ИИ. **Без разрешения автора** возможно использование только в **некоммерческих** целях. Это снижает риски неправомерного коммерческого использования объектов ИС и при сохранении возможности свободного использования таких объектов для социально полезных целей.

Если произведение создается ИИ «без прямого вмешательства человека», то правообладателями являются авторы или правообладатели произведений, которые сделали возможным создание данного

произведения (ст. 2). Однако остается неясным, как должны определяться конкретные произведения, ставшие основой для генерации, каким образом должно распределяться авторское право на произведение, сгенерированное ИИ?

Законопроектом Франции предлагается внедрить коллективное управление сгенерированными ИИ произведениями через организации коллективного управления (для сбора роялти). Законопроект не решает проблему использования для обучения произведений, авторов которых не было возможности установить. Такое предложение несет в себе риски неправильного определения авторов произведения, нарушения прав авторов на имя и на вознаграждение за использование их произведений.

Также Франция предлагает обязать делать пометки, что произведение сгенерировано системой ИИ – аналогичная норма была предложена проектом закона об ИИ **Италии** (апрель 2024 г.). Необходимо использовать знак или маркировку с аббревиатурой «IA» (intelligenza artificiale)¹⁸. Что касается использования охраняемой ИС для обучения ИИ, Италия, в отличие от ЕС и Франции, предложила другой подход – право на свободное использование данных, к которым имеется законный доступ, для обучения систем ИИ, если такое использование прямо не запрещено правообладателями.

Опыт США

В США специальное регулирование не установлено. По общему правилу применяется доктрина «добросовестного использования» защищенных авторским правом данных – возможно использование объектов ИС без лицензии в обстоятельствах, определяемых:

1) целью (например, образовательной);

2) характером использования (некоммерческим). Это не значит, что любое некоммерческое использование признается добросовестным, а коммерческое – недобросовестным. Например,

¹⁶ П.14 Преамбулы Директивы ЕС № 2019/790 об авторском праве.

¹⁷https://www.assemblee-nationale.fr/dyn/16/textes/16b1630_proposition-loi

¹⁸ <https://www.senato.it/service/PDF/PDFServer/DF/437373.pdf>

«преобразующее использование» (добавление чего-то нового) вероятно будет считаться добросовестным. Использование комбинации изображения и текста для обучения ИИ является по сути «преобразующим» по сравнению с исходными данными, что теоретически признается добросовестным использованием;

3) природой самих данных: чем больше выражен творческий элемент, тем ниже шансы на признание добросовестного использования;

4) объемом использованных данных источника;

5) влиянием на рынок и стоимость защищенных данных – наносит ли нелегальное использование вред существующему (например, вытесняя продажи оригинала) или будущему рынку (оригинал станет менее используемым).

В 2023 г. в США были поданы иски американских писателей против OpenAI за использование их текстов для обучения ChatGPT и копирования работ без разрешения; иск художников против Stability AI, Deviantart и Midjourney за неразрешенное использование для обучения ИИ изображений, защищенных авторским правом, для получения большего количества произведений того же типа без согласия авторов оригинальных изображений. Жалобы приняты к рассмотрению, однако решения пока не вынесены.

Опыт России

В России отсутствует регулирование ИС для обучения ИИ.

Однако возможно применение ст. 1274 ГК РФ – право использовать обнародованное произведение или его часть без согласия правообладателя и без выплаты вознаграждения для информационных, учебных или культурных целей. Требуется указать имя автора и источник. То есть при соблюдении перечисленных условий использование объектов ИС может

квалифицироваться как цитирование, а объекты ИС могут использоваться для обучения генеративного ИИ в коммерческих целях, что влечет нарушение ИС правообладателей.

Таким образом, можно выделить 3 подхода стран к использованию данных для обучения ИИ:

1) требование к поставщикам услуг ИИ по комплаенсу для защиты ИС и публикации информации о данных, используемых для обучения ИИ (ЕС, Франция и Китай). При чем по общему правилу требуется обязательное получение разрешения от правообладателей на коммерческое использование ИС, без разрешения – только в некоммерческих целях.

Суды Китая и законопроект во Франции предлагают распространить общее правило о получении разрешения от правообладателей о коммерческом использовании ИС для обучения ИИ;

2) отсутствие специальных требований к операторам ИИ (США) при возможности добросовестного использования ИС для обучения ИИ без лицензии;

3) возможность свободного использования ИИ без разрешения правообладателей, исключение – прямой запрет правообладателя на использование (Италия).

Российский подход в части права использования произведений для обучения ИИ без разрешения схож с подходами ЕС и Франции. При этом в России нет механизмов защиты правообладателей от неправомерного использования объектов ИС для обучения систем генеративного ИИ.

Для создания таких механизмов возможно дополнить часть 4 ГК РФ нормами о:

- праве автора/ правообладателя запретить использование произведения для обучения систем ИИ / алгоритмов;
- маркировки произведений, созданных с использованием ИИ/алгоритмов.