



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

ИИ в здравоохранении, борьба с антиконкурентным поведением поставщиков ПО для смартфонов, защита персональных данных в блокчейне
Мониторинг №6 (Июнь 2024)

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

Авторы: Гирич М.Г., н.с.; Ермохин И.С., н.с.; Левашенко А.Д., с.н.с.; Магомедова О.С., н.с.; Малинина Т.А., с.н.с.

При частичном или полном использовании материалов ссылка на источник обязательна.

«Рукописи не горят»

М. А. Булгаков

В июне 2024 г. можно выделить 3 события, которые определяют тренды развития регулирования цифровой экономики.

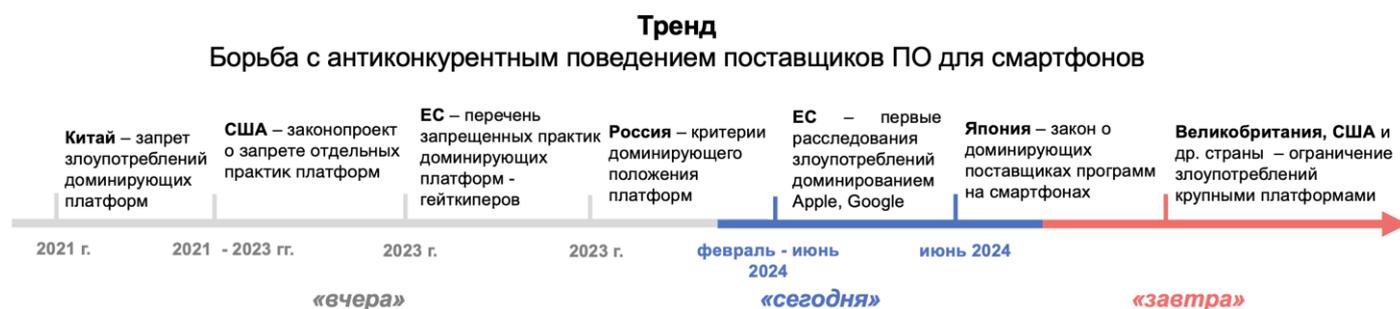
Тренд №1. ИИ в здравоохранении

В июне 2024 г. в Калифорнии (США) уточнен законопроект, закрепляющий обязанность медучреждений информировать пациентов об использовании генеративного искусственного интеллекта (ИИ) для создания сообщений о состоянии их здоровья. Подписанный также в июне Закон ЕС признал такие системы ИИ высокорисковыми. Самое строгое регулирование в этой сфере было введено в 2022 г. в Китае, где были установлены ограничения на замену врача системой ИИ в телемедицине, иной подход был предложен в США в январе 2024 г. – наделение ИИ компетенциями врача.



Тренд №2. Борьба с антиконкурентным поведением поставщиков ПО для смартфонов

В июне 2024 г. Япония ввела запрет на злоупотребления доминирующим положением поставщиками услуг операционных систем, магазинов приложений и браузеров в смартфонах. Закон направлен на олигополистов – Google и Apple. Во многом регулирование повторяет законодательство ЕС. Также в июне 2024 г. ЕС начал расследование в отношении антиконкурентной практики Apple по ограничению возможности разработчиков уведомлять пользователей об альтернативных каналах покупки приложений или услуг (из другого магазина приложений или с собственного сайта разработчика).



Тренд №3. Защита персональных данных в блокчейне

В июне 2024 г. ЕС опубликовал отчет по лучшим практикам применения блокчейн-технологий и защите персональных данных, включая определение участников, которые несут ответственность за сохранность данных, и виды данных, подпадающие под режим защиты. При этом еще в 2018 г. Франция впервые сделала попытку определить какие данные в блокчейне могут считаться персональными и какие обязанности появляются у участников.

Тренд Защита персональных данных в блокчейн-сетях





Ключевые аспекты

1. ИИ в здравоохранении

Опыт США

В июне в Калифорнии (США) рассматривался законопроект об использовании ИИ при общении с пациентами¹. Ранее в США (в 2023–2024 гг.) были рассмотрены предложения по регулированию использования ИИ в сфере здравоохранения. Можно выделить следующие подходы:

1) Наделение ИИ компетенцией врача:

- возможность выписывать рецепты на лекарственные препараты. ИИ фактически приравнивается к практикующему врачу при условии, что (1) технология разрешена штатом для назначения конкретного препарата и (2) одобрена FDA² (федеральный законопроект США³);
- 2) **Ограничение использования ИИ:**
- запрет на принятие решений в сфере здравоохранения (наряду со страхованием и социальным обеспечением) исключительно на основе результатов, сгенерированных ИИ (законопроект штата Джорджия⁴). Любое такое решение должно содержательно рассматриваться человеком. Планируется создать для этого правила;
- запрет для медучреждений заменять независимые оценки лицензированных специалистов по уходу за пациентами на рекомендации или решения ИИ (штат Иллинойс⁵). Например, если медсестра определила процедуры для восстановления пациента после операции, учреждение не вправе

предписывать ей изменить их на основе рекомендаций ИИ.

Некоторые штаты не внедряют специальное регулирование систем ИИ в здравоохранении, однако они признаются «высокорисковыми» (штаты Вермонт⁶, Вирджиния⁷, Колорадо⁸). В этих 3 штатах предусмотрена обязанность разработчиков и пользователей высокорисковых систем ИИ принимать меры для избежания алгоритмической дискриминации при доступе человека к медицинским услугам, пользователей – уведомлять об использовании ИИ при оказании услуг. Существует обязанность разработчиков разъяснять пользователям возможность и способы мониторинга.

В Калифорнии в июне 2024 г. уточнена обязанность медучреждений, использующих генеративный ИИ для создания письменных или устных сообщений о состоянии здоровья пациентов⁹:

- информировать, что сообщение создано с помощью ИИ, и что такое сообщение было проверено человеком – поставщиком услуги;
- предоставлять инструкции, как пациенту связаться с человеком – поставщиком услуги.

Кроме того, с 2023 г. в Массачусетсе рассматривается законопроект об использовании ИИ в области психического здоровья¹⁰:

- лицензированный специалист в этой сфере должен получить одобрение лицензирующего органа на использование ИИ;
- ИИ должен постоянно контролироваться специалистом;

¹ https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=202320240AB3030

² Управлением по пищевым продуктам и лекарствам (Food and Drug Administration)

³ <https://www.congress.gov/bill/118th-congress/house-bill/206/text>

⁴ <https://www.legis.ga.gov/legislation/65973>

⁵ <https://www.ilga.gov/legislation/fulltext.asp?DocName=&SessionId=112&GA=103&DocTypeId=SB&DocNum=2795&GAID=17&LegID=&SpecSess=&Session=>

⁶ <https://legislature.vermont.gov/Documents/2024/Docs/BILLS/H-0710/H-0710%20As%20Introduced.pdf>

⁷ <https://lis.virginia.gov/cgi-bin/legp604.exe?241+ful+HB747H1>

⁸ https://leg.colorado.gov/sites/default/files/2024a_205_signed.pdf

⁹ Информация о состоянии здоровья пациента, она не включает административные вопросы, в том числе, планирование визитов и выставление счетов

¹⁰ <https://malegislature.gov/Bills/193/H1974>

- пациент предоставляет информированное согласие на получение лечения у специалиста, который будет использовать ИИ. Получение информированного согласия пациента – необходимое условие любого медицинского вмешательства. Но при применении ИИ требуется согласие после информирования о том, как работает ИИ.

Опыт ЕС

В ЕС в июне 2024 г. был подписан Закон об ИИ¹¹, который признает ИИ высокорисковым при его использовании:

1) для обеспечения безопасности медицинского устройства, используемого, например, для диагностики *in vitro*¹²;

2) при оценке органами власти права лица на доступ к госуслугам здравоохранения (например, в рамках медицинского страхования);

3) для оценки и классификации экстренных вызовов от физических лиц, например установления приоритета в направлении служб неотложной первой помощи и получении медицинской помощи.

К высокорисковому ИИ предъявляются специальные требования, включая требования анализа рисков, обеспечения человеческого контроля за ИИ и пр.

Подход ЕС аналогичен подходам штатов США – Вермонта, Вирджинии, Колорадо, но есть и отличия. В ЕС требуется контроль человеком при использовании высокорискового ИИ (в названных штатах такое требование отсутствует), но не предусмотрена обязанность информировать людей о применении ИИ. Это связано с желанием снять любую ответственность с потребителей медицинских услуг. В отличие от Колорадо, у ЕС не установлена возможность требовать пересмотра человеком неблагоприятного решения ИИ. С точки зрения развития технологий подход Колорадо имеет преимущества:

пересмотренные решения дают обратную связь и могут быть использованы для улучшения работы ИИ.

Опыт Китая

Национальная комиссия Китая по здравоохранению в 2022 г. заявила, что существующему ИИ в медицинской сфере не хватает данных и прозрачности работы алгоритмов для медицинского обслуживания¹³. Неясно, как определять ответственность за причиненный вред пациентам в результате действий ИИ. Поэтому в Китае установлены ограничения при использовании ИИ в медицине¹⁴:

1) медицинское учреждение не может использовать ИИ, выдавая его за врача или заменяя врача, имеющего право оказывать услуги по диагностике и лечению лично (ст. 13).

2) рецепты на лекарства должен выписывать сам лечащий врач, использование ИИ или других методов автоматического формирования рецептов строго запрещено (ст. 21).

Опыт России

В России действует 2 экспериментальных правовых режима для тестирования медицинских технологий с ИИ, а также принят ГОСТ Р 59921.2–2021 «Системы искусственного интеллекта в клинической медицине».

Однако отсутствует специальное правовое регулирование применения систем ИИ в здравоохранении. Тем не менее ИИ может использоваться как часть ПО в медицинском изделии (Приказ Минздрава России от 06.06.2012 N 4н). Такое ПО отнесено к категории ПО с высокой степенью риска, для которых предусмотрены специальные условия использования и лицензирования. Правила регистрации таких систем определены Постановлением Правительства РФ от 27.12.2012 № 1416.

Для применения ИИ во врачебной практике в России необходимо внедрять

¹¹https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:PE_24_2024_REV_1.

¹² выполнения экспериментов, когда опыты проводятся «в пробирке»

¹³ <http://www.cn-witmed.com/list/13/9702.html>

¹⁴ Уведомление об издании подробных правил надзора за интернет-диагностикой и лечением, 2022 г. <http://www.nhc.gov.cn/yzygj/s3594q/202203/fa87807fa6e1411e9afef82a4211f287.shtml>

системы выявления и управления рисками, а также устанавливать требование человеческого контроля за решениями, принятыми ИИ. Это позволит использовать ИИ в медицине – например, – применение ИИ для постановки диагноза может сократить расходы на лечение до 50%¹⁵. При этом человеческий контроль снизит риски ошибок в диагнозе или при назначении лекарств.

2. Борьба с антиконкурентным поведением поставщиков ПО для смартфонов

В июне 2024 г. в Японии был принят закон, ограничивающий злоупотребления доминированием на рынке ПО, используемого в смартфонах¹⁶. Закон фактически направлен на Apple (46,6% рынка) и Google (53,4%) – олигополистов на рынке базовых операционных систем для смартфонов, браузеров и магазинов приложений. А в ЕС в июне началось расследование о злоупотреблении Apple своим доминирующим положением на рынке магазинов приложений¹⁷.

Регулирование Японии распространяется только на поставщиков 4 типов приложений в смартфонах¹⁸: базового операционного ПО (операционные системы и драйверы), магазины приложений, браузеры и поисковые системы.

Комиссия по справедливой торговле (антимонопольный орган Японии) планирует разработать количественные критерии для определения доминирующего положения перечисленных 4 типов поставщиков ПО, включая оценку количества сделок или рыночную долю поставщика в отношении каждого типа ПО. Комиссия определит конкретный перечень операторов (поставщиков услуг), которые занимают доминирующее положение.

Во многом закон Японии схож с Законом ЕС о цифровых рынках, однако он

секторальный и направлен только на конкретные практики злоупотребления доминирующим положением поставщиков ПО для смартфонов. Одна из причин – размер рынка приложений для смартфонов, например, более 90% развлекательного контента потребляется именно через смартфоны¹⁹.

В Японии определены и запрещены характерные для рынка ПО для смартфонов практики злоупотребления:

1) использование данных, накопленных бизнес-пользователями (сторонние поставщики ПО, разработчики приложений в магазинах приложений), для конкурирования с ними, а также передача этих данных дочерним компаниям или другим своим сервисам. Например, данные о продажах приложений сторонних разработчиков, которые продаются через магазин приложений доминирующего поставщика (количество скачиваний, регион, стоимость и пр.);

2) введение технических ограничений. Например, доминирующие операторы базового операционного ПО не могут вводить ограничения для установки магазинов приложений сторонних поставщиков или браузеров. Apple не может ограничить возможность установить Google Play вместо App Store;

3) введение ограничений по использованию платежных услуг. Например, введение условия, что пользователь не может использовать платежные системы других поставщиков, кроме рекомендованных или заложенных в систему оплаты этого магазина приложений;

4) запрет предоставления преимуществ собственным сервисам. Например, при поиске в магазине приложений предлагать сначала собственные сервисы, а уже потом сервисы конкурентов;

¹⁵ https://www.hsph.harvard.edu/ecpe/programs/ai-for-health-care-concepts-and-applications/?gclid=cjwkcjwx46tbhbheiwara_djpivzt43u3rvveax4p7j3gjz4rknn-99z-4adr_3cniltqubnkrdbocqi0qavd_bwe

¹⁶ <https://www.sangiin.go.jp/japanese/joho1/kousei/gian/213/pdf/s0802130622130.pdf>

¹⁷ https://ec.europa.eu/commission/presscorner/detail/en/IP_24_3433

¹⁸ смартфон – это терминал, который:

- имеет такой размер, что его можно носить с собой и использовать в любое время;
- имеет установленное программное обеспечение, которое можно использовать;
- с помощью терминала можно пользоваться телефоном и Интернетом.

¹⁹ <https://www.kantei.go.jp/jp/singi/digitalmarket/kyosokaigi/dai7/siryou01.pdf>

5) установление ограничений для отображения цен на сервисы, продаваемые в магазине приложений, а также отображения ссылок на другие сайты для скачивания (например, другой магазин приложений или собственный сайт поставщика ПО), чтобы пользователь мог скачать ПО через сторонние площадки.

Именно такая практика послужила поводом для нового разбирательства ЕС против Apple в июне 2024 г. Apple ограничила возможность разработчиков, распространяющих приложения через App Store, иметь возможность бесплатно информировать своих клиентов об альтернативных, более дешевых возможностях покупки приложений, а также оставлять ссылки для покупателей на альтернативные каналы покупки, например, на собственные сайты разработчиков, сторонние магазины приложений. Разработчики могли оставлять ссылки не в App Store, а внутри приложения, но тогда Apple взимала с разработчиков плату по 0,50 € - комиссия за то, что пользователь покупает приложение не в App Store, а в другом магазине, перейдя по ссылке разработчика.

В настоящее время Комиссия признала нарушение ст. 6(4) Закона ЕС о цифровых рынках. Риск наказания для Apple – штраф до 10% от общего мирового оборота, разбирательство в процессе рассмотрения.

В Японии за нарушение перечисленных запретов штрафы могут достигать до 20% оборота предприятия в Японии.

Стоит отметить, что в Японии доминирующие операторы обязаны внедрять практики, которые будут уравнивать конкуренцию:

1) раскрывать систему управления данными. Например, магазины приложений должны раскрывать данные о продаже ПО сторонних поставщиков, об условиях приобретения и использования такого ПО;

2) обеспечивать право на переносимость данных с одного устройства / сервиса пользователя на другое устройство / сервис, например, переносить фотографии или сообщения из одного приложения в другое;

3) обеспечивать право пользователя изменять настройки по умолчанию, удалять ПО, предустановленное доминирующим поставщиком.

Перечисленные выше практики и запреты также используются и в ЕС (аналитика представлена в выпуске [№ 3 Мониторинга \(март 2024 г.\)](#)). Однако есть отличие – Япония выделяет группу мер, связанных с изменением спецификаций или условий в отношении конкретного ПО. Например, если доминирующий поставщик операционной системы изменяет спецификации к ПО (например требования к программам, которые можно устанавливать), если условия использования системы или доминирующий магазин приложений отказывается от сотрудничества с отдельными разработчиками ПО, либо браузер отказывается отображать веб-страницу, то такие действия необходимо согласовать с Комиссией по справедливой торговле.

Опыт России

В России ст. 10.1 Закона о защите конкуренции устанавливает запрет на монополию платформ, занимающих доминирующее положение. Также есть руководство ФАС, но оно не касается практик, связанных с использованием данных, интероперабельностью, как это сделано в Японии или ЕС.

Однако ФАС проводила расследования схожие с делом Apple в ЕС в отношении злоупотреблений на рынке ПО, в том числе для смартфонов.

Например, в 2015 г. проводилось расследование в отношении Google, так как операционная система Android (более 50% рынка) осуществляла обязательную предустановку приложений Google, ограничив установку приложений альтернативных поставщиков. В аналогичном расследовании 2020 г. было признано, что Apple (100% рынка магазинов приложений на операционной системе iOS) устанавливала технические ограничения для приложений сторонних поставщиков, продвигая собственные.

По итогам расследований было признано доминирование Google и Apple и на

них были наложены штрафы за злоупотребления положением.

3. Защита персональных данных в блокчейне

Технология блокчейн представляет собой цепочку блоков с базами данных, в том числе персональных. В июне 2024 г. Европейская блокчейн-песочница выпустила отчет о применении европейского законодательства к технологии, включая вопросы защиты персональных данных²⁰. Еще в 2018 г. Франция дала рекомендации по соблюдению европейского законодательства о персональных данных при использовании блокчейн-технологий²¹.

Важно отметить, что рекомендации о применении законодательства о персональных данных в первую очередь разработаны для частных блокчейн-сетей (например, Ethereum Enterprise), регуляторы отмечают, что применение рекомендаций к публичным блокчейн-сетям (например, Bitcoin) требует дальнейшей проработки.

Опыт ЕС и Франции

Персональные данные – это данные, которые позволяют прямо или косвенно идентифицировать конкретное физическое лицо. ЕС и Франция выделяют следующие аспекты, влияющие на защиту персональных данных в блокчейне:

1. Виды данных, которые считаются персональными:

- приватные ключи (позволяют подтвердить транзакцию или действие в блокчейне), которые принадлежат конкретному физическому лицу. Например, пароль от криптокошелька;

- хешированные данные о транзакциях/действиях (любые данные, обработанные функцией шифрования в блокчейне). Например, данные о передаче криптоактивов или других сведений между криптокошельками;

- данные, содержащиеся в блокчейне, которые связаны с учетными или данными пользователя, расположенными вне

блокчейна (например, такие данные входа в аккаунт на блокчейне, как логин и пароль);

- данные в блокчейне, связанные с конкретными продуктом, которые могут не признаваться персональными, однако связаны с лицом, которого можно определить. Например, данные об IP-адресе пользователя.

Перечисленные выше виды данных, которые могут использоваться в блокчейне, становятся персональными, если позволяют оператору данных идентифицировать лицо, которому они принадлежат. Например, оператор может определить, кому принадлежит хэш (идентифицирует лицо, оставившее запись (создавшее хэш) и время), либо, которому принадлежит приватный ключ, используемый в блокчейне. Это возможно за счет использования функции «коммитента» в блокчейне, которая позволяет «замораживать» (хешировать) данные таким образом, что распознать зашифрованные данные возможно при наличии дополнительной информации (например данных из других баз).

В деле Брейер 2016 г. суд ЕС уже признавал, что IP-адрес относится к персональным данным, если провайдер платформы имеет технические средства для идентификации конкретного лица, которому принадлежит IP-адрес, в том числе используя данные от третьих лиц, как интернет-провайдеры.

2. Участники блокчейн-системы, которые должны выполнять нормы по защите персональных данных.

В блокчейне участники, которые определяют цели и записывают данные в цепочке или принимают решение о направлении данных для валидации майнерами, являются контролерами в рамках закона о персональных данных ЕС. Например, нотариус (как физическое лицо), который вносит запись в блокчейне для регистрации сделки, определяя, что данные записываются во исполнение такой сделки. Или банк (как юридическое лицо), который вводит данные своих клиентов в блокчейн

²⁰ <https://ec.europa.eu/digital-building-blocks/sites/display/EBSISANDCOLLAB/Best+practices+report+2023+-+Part+B?preview=/753860727/753860735/European%20Blockchain%20Sa>

<ndbox%20-%20Best%20practices%20report%20-%20Part%20B%20-%20Jun.2024.pdf>

²¹ https://www.cnil.fr/sites/cnil/files/atoms/files/la_blockchain.pdf

(осуществляет регистрацию данных третьих лиц в системе). В то же время лицо не может иметь статус контролера в отношении своих же данных. Например лицо, которое покупает или продает биткойн от своего имени.

Будут признаваться обработчиками персональных данных в значении закона ЕС майнеры, так как имеют доступ к данным о транзакциях (включая хэш), которые могут включать персональные данные, а также разработчик смарт-контракта, который обрабатывает персональные данные, полученные от лица, собирающего такие данные (контролер). Например, когда разработчик смарт-контракта для сделки получает данные от нотариуса, а майнер валидирует и записывает эту транзакцию в блокчейн.

В то же время к обработчикам данных не относятся:

- стороны смарт-контракта, так как лица не считаются обработчиками собственных данных;
- разработчики алгоритма смарт-контракта, если не имеют доступ к персональным данным, а только технически разрабатывают ИТ-решения.

3. Обеспечение права на удаление данных из блокчейна (ЕС, Франция).

Право субъекта персональных данных на их удаление означает право потребовать у контролера уничтожения собранных данных. Право на удаление персональных данных в блокчейне реализуется, когда происходит удаление приватного ключа или хэша, которые могут содержать персональные данные, в том числе зашифрованные через хэш.

Опыт России

В России отсутствуют специальные нормативно-правовые акты органов власти о защите персональных данных в блокчейне, что создает риски нарушения законодательства. Также в отличие от ЕС и Франции статус контролера данных и обработчика данных не различается. Это значит, что на практике в России любые участники блокчейна, которые имеют отношение к работе с данными, подпадают под определение оператора данных в рамках российского законодательства (например, майнеры). Но на практике каждый участник блокчейна может соблюдать требования к операторам персональных данных только в той части, которая входит в их функции как участника системы блокчейн. Например, разработчик смарт-контракта может обеспечивать меры безопасности обработки данных, но не может контролировать законность оснований для сбора персональных данных, записанных в блокчейне (например, наличие согласия субъекта этих данных).

