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

ИИ в здравоохранении, борьба с антиконкурентным поведением поставщиков ПО в смартфонах, защита персональных данных в блокчейне

Мониторинг №6 (Июнь 2024)

«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 ИИ для создания сообщений о состоянии их здоровья. Подписанный также в июне Закон ЕС об ИИ 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, хотя в США в январе 2024 г. был предложен иной подход – наделение ИИ компетенциями, схожими с врачом.

Тренд №2. Борьба с антиконкурентным поведением поставщиков ПО в смартфонах

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 начала 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.

Ключевые аспекты

1. ИИ в здравоохранении

Опыт США

В июне в Калифорнии (США) рассматривался законопроект об использовании ИИ при общении с пациентами[1]. В США ранее в 2023–2024 гг. были предложены инициативы по регулированию использования ИИ в сфере здравоохранения. Можно выделить следующие подходы:

1) Наделение ИИ компетенцией **врача**:

- Возможность назначать лекарства по рецептам. ИИ фактически приравнивается к практикующему врачу при условии, что (1) технология разрешена штатом для назначения конкретного препарата и (2) одобрена FDA[2] (федеральный законопроект США[3]);

2) **Ограничение использования ИИ**:

- запрет принятия решений в сфере здравоохранения (наряду со страхованием и социальным обеспечением) исключительно на основе результатов, сгенерированных ИИ (законопроект Джорджии[4]). Любое такое решение должно содержательно рассматриваться человеком. Планируется создать для этого правила;
- запрет для медучреждений принимать политики, заменяющие независимые оценки лицензированных специалистов по уходу за пациентами на рекомендации или решения ИИ (Иллинойс[5]). 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 для ИИ в здравоохранении, однако такие системы ИИ признаются **«высокорисковыми»** (Вермонт[6], Вирджиния[7], Колорадо[8]). 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 предоставить пользователям разъяснения, как человек может осуществлять мониторинг.

В Калифорнии в июне 2024 г. уточнена обязанность медучреждений, использующих генеративный ИИ для создания письменных или устных сообщений о состоянии здоровья пациентов[9]:

- 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 здоровья[10]:

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

[1] https://leginfo.legislature.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 ИИ[11], 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 в части мониторинга работы, включая требования анализа рисков, обеспечения человеческого контроля за ИИ и пр.

Подход ЕС аналогичен подходам штатов США – Вермонта, Вирджинии, Колорадо, но есть отличия. В ЕС требуется контроль человеком при использовании высокорискового ИИ (в этих 3 штатах – нет), 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 обслуживания[13]. Неясно, как определять ответственность за причиненный вред пациентам в результате действий ИИ. Поэтому в Китае установлены ограничения при использовании ИИ в медицине[14]:

1) медицинское учреждение не может использовать ИИ, выдавая 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).

В Китае сегодня установлены самые строгие ограничения.

Опыт России

В России запущено 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 использования 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.

[11] https://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/fa87807fa6e1411e9afeb82a4211f287.shtml

В случае разработки в России возможности использования ИИ во врачебной практике важно внедрять 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 в смартфонах

В июне 2024 г. в Японии был принят закон, ограничивающий практики злоупотребления доминированием на рынке ПО, используемого в смартфонах[16]. 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 приложений[17].

Регулирование Японии распространяется только на поставщиков 4 типов приложений в смартфонах[18]: 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 доминирующего положение.

Во многом закон Японии похож на Закон ЕС о цифровых рынках, однако он секторальный и приземляет конкретные практики злоупотребления доминирующим положением на поставщиков ПО для смартфонов. Одна из причин – размер рынка приложений для смартфонов, например, более 90% развлекательного контента потребляется именно через смартфоны.[19]

Итак, Япония определяет характерные для рынка ПО для смартфонов практики злоупотребления, которые запрещены:

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 сторонним собственным сервисам. Например, при поиске в магазине приложений предлагать сначала

[15] https://www.hsph.harvard.edu/ecpe/programs/ai-for-health-care-concepts-and-applications/?gclid=cjwkcajwx46tbhbheiwara_djpivzt43u3rvveax4p7j3gjz4rknn-99z-4adr_3cniltlqubnkrdbocqi0qavd_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: такого размера, 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/siryou1.pdf

собственные сервисы, а уже потом сервисы конкурентов.

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 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 направления 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.

На данный момент 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% от 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 продаж ПО сторонних поставщиков, 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 (за март 2024 г.). Однако есть отличие – Япония выделяет группу мер, связанных с изменением спецификаций или условий в отношении конкретного ПО. Например, доминирующий поставщик операционной системы изменяет спецификации к ПО (например, требования к программам, которые можно устанавливать), 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, которое при этом не охватывает практики, связанные с использованием данных, интероперабельностью, как это сделано в Японии или ЕС.

Между тем ФАС проводила схожие с делом Apple в ЕС расследования в отношения злоупотреблений на рынке ПО, в т.ч. для смартфонов.

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

сторонних поставщиков, продвигая собственные.

Было признано доминирование Google и Apple с наложением штрафов за злоупотребления положением.

3. Защита персональных данных в блокчейне

Технология блокчейн представляет собой цепочку блоков с базами данных, в т.ч. персональных. В июне 2024 г. Европейская блокчейн-песочница выпустила отчет о применении европейского законодательства к технологии, включая вопросы защиты персональных данных[20]. Еще в 2018 г. Франция дала рекомендации по соблюдению европейского законодательства о персональных данных при использовании блокчейн-технологий[21].

Важно отметить, что рекомендации о применении законодательства о персональных данных в первую очередь разработаны для приватных блокчейн-сетей (напр. Ethereum Enterprise), регуляторы отмечают, что применение рекомендаций к публичным блокчейн-сетям (напр. 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:

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

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

3) данные, содержащиеся в блокчейне, которые связаны с учетными или данными пользователя, расположенными вне блокчейна (например, данные входа в аккаунт на блокчейне, как логин и пароль);

4) 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 лицо, которому принадлежит приватный ключ, используемый в блокчейне. Это возможно за счет использования функции «коммитмента» в блокчейне, которая позволяет «замораживать» (хэшировать) 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 т.ч. обращаясь к данным 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 значении 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

[20] https://ec.europa.eu/digital-building-blocks/sites/display/EBSISANDCOLLAB/Best+practices+report+2023+-+Part+B?preview=/753860727/753860735/European%20Blockchain%20Sandbox%20-%20Best%20practices%20report%20-%20Part%20B%20-%20Jun.2024.pdf

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

сделки. Или банк (как юридическое лицо), который вводит данные своих клиентов в блокчейн (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.

Майнеры, т.к. 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), будут признаваться обработчиками персональных данных в значении закона ЕС. 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 запросить у контролера уничтожение собранных данных. Право на удаление персональных данных в блокчейне реализуется, когда происходит удаление приватного ключа или хэша, которые могут содержать персональные данные, в т.ч. зашифрованные через хэш.

Опыт России

В России отсутствуют специальные заявления 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 по смыслу 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.