ИНСТИТУТ ЭКОНОМИЧЕСКОЙ ПОЛИТИКИ имени Е.Т. ГАЙДАРА

Лаборатория анализа лучших международных практик

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

Передача персональных данных из ЕС в США, обманные практики с данными, использование ИИ в судах

Мониторинг №7 (Июль 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.

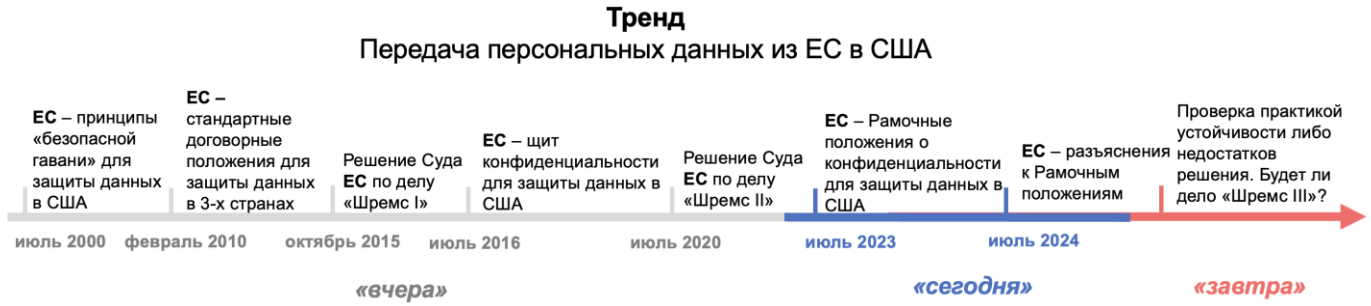
«...крупными буквами печатались слова совершенно несущественные, а все существенное изображалось самым мелким шрифтом.»

М. Салтыков-Щедрин

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

Тренд № 1. Передача персональных данных из ЕС в США

В июле ЕС опубликовал разъяснения к Рамочным положениям о конфиденциальности при передаче данных из ЕС в США, принятым еще в 2023 г. Механизмы реализации этих положений направлены на сокращение рисков избыточного доступа спецслужб США к данным, передаваемым из ЕС. Правда, есть сомнения, что это будет работать.



Тренд №2. Обманные практики с данными

В июле сразу 3 штата США ввели запрет для онлайн-платформ на использование обманных («темных») практик с данными. По исследованию FTC[1], ICPEN[2], GPEN[3] пользователи более 1000 сайтов хотя бы 1 раз сталкивались с одной из «темных практик» на 97% ресурсах. Интернет-ресурсы принуждают пользователей соглашаться на незащищенные способы обработки данных, обманом собирают больше данных, чем нужно и пр.

[1] Федеральная торговая комиссия США.
[2] Международная сеть по защите прав потребителей и правоприменению.
[3] Глобальная сеть по обеспечению конфиденциальности.

Тренд №3. Использование ИИ в судах

В июле Верховный Суд Российской Федерации заявил, что использование ИИ при подготовке документов в судах снизит количество ошибок при вынесении приговоров. В это же время Окружной суд Западного округа Северной Каролины США заявил об осторожности при использовании ИИ судами и сторонами: каждое заявление и ссылка на законы, судебные решения, содержащиеся в документе, должны быть проверены. С июня 2023 г. суды ряда стран (Канада, Новая Зеландия, Австралия) уже вынесли предупреждения об ответственности за использование сторонами ИИ в суде.

Тренд

Ограничение использования ИИ в судах

1. Передача персональных данных из ЕС в США

Персональные данные (далее – ПД) передаются из ЕС компаниям в США, в том числе для обеспечения международной торговли (например, услуг авиакомпаний) и потребностей рынка труда (например, при найме в США специалиста из ЕС). По общему правилу ПД из ЕС могут передаваться в страны с адекватной защитой ПД, что может признаваться решениями Еврокомиссии или обеспечиваться определенными инструментами, например, стандартными договорными положениями (подписываются компаниями, передающими и получающими ПД)[4]. Поскольку регулирование ПД в США менее строгое, чем в ЕС, США по умолчанию не считалась страной с адекватной защитой ПД. Решения Еврокомиссии об адекватности защиты ПД в США облегчают их трансграничную передачу.

В числе документов, на основе которых Еврокомиссия принимала решения об адекватности защиты, – Рамочные положения о конфиденциальности данных ЕС–США. В июле 2024 г. Европейским советом по защите данных опубликованы разъяснения к этим положениям[5], уточняющие технические моменты передачи ПД (например, передача ПД компаниям, дочерним по отношению к присоединившимся к указанным рамочным положениям, обязанность информирования субъектов данных о том, кому в США передаются данные).

Решение Еврокомиссии об адекватности защиты ПД в США по Рамочным положениям[6,7] было принято в июле 2023 г., при этом ранее действовали 2 аналогичных по форме и смыслу решения Еврокомиссии (решение по принципам «безопасной гавани» 2000 г.[8] и решение о «щите конфиденциальности» 2016 г.[9]), которые были признаны недействительными Судом ЕС[10] в рамках дел «Шремс I» (2015 г.)[11] и «Шремс II» (2020 г.)[12,13].

В основе принципов «безопасной гавани», «щита конфиденциальности» и рамочных положений о конфиденциальности данных лежат принципы информирования, подотчетности при дальнейшей передаче данных, безопасность передачи, целостность данных и пр.[14] Небольшие различия есть в принципах «безопасной гавани» и «щитом конфиденциальности». Последний шире, например, в части ответственности при передаче ПД для обработки подрядчикам[15] и того, в каких случаях и о чем необходимо уведомлять субъектов ПД, в том числе о требовании раскрыть ПД в ответ на законные запросы органов власти для обеспечения национальной безопасности.

Еще одно различие между тремя рассматриваемыми решениями Еврокомиссии состоит в механизмах защиты прав субъектов ПД. Так, Суд ЕС в деле «Шремс I» (которое отменило решение по «безопасной гавани») постановил, что принципы «безопасной гавани» (2000 г.) предоставляют недостаточную правовую защиту для субъектов ПД. Поэтому в рамках следующего решения – «щита конфиденциальности» была предусмотрена функция омбудсмена, чтобы власти ЕС могли через него подавать запросы от имени субъектов ПД, передаваемых из ЕС, в том

[4] При отсутствии таких решений и инструментов ПД могут передаваться из ЕС в третьи страны в качестве исключения: например, при выраженном согласии субъекта ПД после его информирования о рисках.

[5] https://www.edpb.europa.eu/system/files/2024-07/edpb_dpf_faq-for-businesses_en.pdf

[6] https://eur-lex.europa.eu/eli/dec_impl/2023/1795/oj

[7] Решение означает, что адекватность защиты данных обеспечивается Рамочными положениями, т.е. действует только для компаний из США, заявивших о соблюдении этих положений и включенных на этом основании в список Министерства торговли США, а не для США в целом. То же верно для принципов «безопасной гавани» и «щита конфиденциальности».

[8] https://eur-lex.europa.eu/eli/dec/2000/520/oj

[9] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.ENG

[10] Court of Justice of the European Union (CJEU).

[11] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362

[12] https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62018CJ0311

[13] Отметим, что правового вакуума это не создало, так как решение Еврокомиссии по стандартным договорным положениям (2010 г., см. ниже) оставалось действующим.

[14] Их 7: информирование; выбор; подотчетность при дальнейшей передаче; безопасность; целостность данных и ограничение целей; доступ субъектов; защита прав, инфорсмент и ответственность. Принципы публикуются Министерством торговли США и сопровождаются переговорами между ЕС и США об условиях (включающих также механизмы реализации принципов), на которых может быть признана адекватность защиты данных, т.е. решения Еврокомиссии не являются односторонними.

[15] Например, Facebook передает данные пользователей из ЕС на свои серверы в США; если Facebook в США нанимает, условно, компанию А для обработки этих данных, то А – подрядчик.

случае если разведка США создает риски нарушения ПД (например, осуществляет массовый сбор ПД).

Решения Еврокомиссии на основе принципов «безопасной гавани» и «щита конфиденциальности» признаны Судом ЕС недействительными по причинам:

1) несоразмерности доступа разведывательных органов США к ПД европейцев (например, массовый сбор ПД по Закону США о наблюдении в целях внешней разведки);

2) отсутствия эффективной правовой защиты от вмешательства госорганов США. При этом введение функции омбудсмена на эффективность правовой защиты не повлияло, так как он, по сути, не является судом.

Решение Еврокомиссии об адекватности защиты, обеспечиваемой стандартными договорными положениями (включают, например, обязательства экспортера и импортера данных в отношении друг друга и субъектов данных), принятое в 2010 г.[16], в рамках дела «Шремс II» в суде не было отменено, так как эти положения, не являясь обязательными для властей третьих стран, в том числе США[17], тем не менее обеспечивают приостановку/запрет передачи ПД в третью страну, если получатель не соблюдает или не может соблюдать их защиту.

Стоит отметить, что Решение Еврокомиссии по Рамочным положениям о конфиденциальности данных 2023 г. было принято после подписания в США в 2022 г. указа № 14086 об усилении гарантий безопасности в деятельности разведки[18], чтобы ограничить несоразмерный доступ разведки США к ПД европейцев. Отличие этого решения от двух предыдущих заключается в создании в США двухуровневого механизма[19] для рассмотрения жалоб субъектов ПД, чьи данные переданы из ЕС в США, по поводу их сбора и использования разведкой:

- на 1-ом уровне жалобы рассматриваются должностным лицом (в отличие от омбудсмена – в разведывательном сообществе, а не в структуре Госдепартамента США);
- на 2-ом – специально созданным судом по надзору за защитой данных, в котором решение 1-го уровня можно обжаловать. Это призвано усилить защиту от вмешательства разведки.

Эти меры критикуются как формальные: соразмерность является предметом оценочных суждений, а независимость, прозрачность и беспристрастность суда по надзору за защитой данных ставится под сомнение, так как субъекты данных не имеют к нему прямого доступа. В связи с этим г-н Шремс готовится к очередному делу в Суде ЕС[20]. При этом в наличии действующего решения об адекватности защиты ПД в США заинтересованы и ЕС, и США: для компаний обоих оно сокращает издержки при внешнеторговых операциях.

Опыт России

В России согласно п. 2 ст. 12 Закона о ПД Роскомнадзор утвердил перечень стран, обеспечивающих адекватную защиту прав субъектов ПД: 89 стран[21], в том числе все 27 стран ЕС, но США в этом перечне отсутствует[22]. Это означает, что ПД не могут передаваться в США до решения Роскомнадзора о возможности их передачи. Операторы вправе передавать ПД в страны из перечня до рассмотрения уполномоченным органом уведомления о трансграничной передаче данных, а в остальные страны – по результатам такого рассмотрения.

Подход РФ строже предусмотренного в ЕС, где передача ПД в третьи страны допустима без разрешения надзорного

[16] https://eur-lex.europa.eu/eli/dec/2010/87/oj

[17] В отличие от рассмотренных выше это решение ориентировано на передачу ПД во все третьи страны, но в деле «Шремс II» речь шла о передаче ПД именно в США.

[18] https://www.federalregister.gov/documents/2022/10/14/2022-22531/enhancing-safeguards-for-united-states-signals-intelligence-activities

[19] https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752

[20] https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu

[21] 55 стран, являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке ПД, и 34 – нет. Последние включаются в перечень, если нормы права и меры по обеспечению конфиденциальности и безопасности ПД в них соответствуют положениям этой конвенции.

[22] В редакциях приказа Роскомнадзора от 15.03.2013 № 274 США отсутствовали.

органа даже при отсутствии решения об адекватности защиты в этих странах (например, на основе обязывающих корпоративных правил или согласия субъекта ПД после его информирования о рисках). Обеспечивает ли он большую защиту ПД, зависит от тщательности рассмотрения уполномоченным органом условий в уведомлениях о трансграничной передаче данных.

2. Обманные практики с данными

Опыт США

В июле 2024 г. в 3-х_ штатах США вступили в силу поправки в законы о данных – в Техасе[23], Флориде[24] и Колорадо[25]. Указанные штаты закрепили понятие «темных практик» (dark pattern) – практик манипулирования пользовательским интерфейсом для нарушения автономии пользователя, т.е. способности свободно принимать решения или делать выбор в отношении использования данных. Например, согласие на операции с ПД, полученное обманным путем; практики, направленные на сбор информации от детей сверх того, что требуется для получения услуги, или предложение отказаться от защиты данных в игре или социальной сети.

Кроме того, установлено право Федеральной торговой комиссии определять перечни запрещенных практик, применение которых рассматривается как нарушение законодательства о ПД.

Опыт международных организаций и ЕС

В июле 2024 г. опубликовано исследование FTC США совместно с ICPEN[26], GPEN[27], где изложены результаты проверки более 1000 сайтов и приложений на предмет использования «темных практик»[28].

Ранее похожие исследования проводились в 2022 г. ОЭСР[29] и ЕС.[30] «Темные практики» используются в дизайне сайта для манипулирования мнением потребителей, например:

1. Заставляют предоставлять больше личной информации, чем необходимо для получения продуктов или услуг;
2. Заставляют соглашаться на использование менее защищенных методов обработки данных;
3. Препятствуют пользователю получить информацию о защите его данных.

Оценивались следующие практики:

1) сложный и запутанный язык – технические или чрезмерно длинные правила конфиденциальности, которые трудно понять. 89% изученных ресурсов содержали либо чрезмерно длинные политики конфиденциальности (более 3000 слов), либо технические и запутанные формулировки, затрудняющие чтение;

2) вмешательство в интерфейс – элементы дизайна, влияющие на восприятие и понимание пользователями их действий, связанных с ПД. Выявлено на 43% изученных ресурсах. Примеры практик:

- ложная иерархия визуальное выделение одних элементов интерфейса и сокрытие других, направляя пользователей к менее защищенным операциям по защите ПД. Например, предлагается способ, который обеспечивает меньшую защиту данных, выделяется цветовым контрастом;
- выбор вариантов обработки данных «по умолчанию», обеспечивающих меньшую защиту данных;
- использование фраз, которые могут вызвать чувство вины у потребителя. 29% сайтов отговаривали пользователей удалять аккаунты через предупреждение, например,

[23] https://capitol.texas.gov/tlodocs/88R/billtext/html/HB00004F.htm
[24] https://flsenate.gov/Session/Bill/2023/262/BillText/er/HTML
[25] https://leg.colorado.gov/sites/default/files/2021a_190_signed.pdf
[26] Международная сеть по защите прав потребителей и правоприменению (международная организация).
[27] Глобальная сеть по обеспечению конфиденциальности (международная организация).
[28] https://www.privacyenforcement.net/system/files/2024-07/GPEN%20Sweep%202024%20-%20%27Deceptive%20Design%20Patterns%27_0.pdf

[29] Отчет ОЭСР о «Темных коммерческих практиках» https://one.oecd.org/document/DSTI/CP(2021)12/FINAL/en/pdf
[30] Руководящие принципы № 3/2022 по «Темным практикам в интерфейсах платформ социальных сетей» https://www.edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf

фразой «если Вы нажмете «Удалить учетную запись пользователя», Вы потеряете свои VIP-привилегии».

ЕС также выделила практику манипулирования эмоциями потребителей. Например, просьба назвать свое местоположение, чтобы якобы его смогли найти другие пользователи, и он не был одиноким, хотя на самом деле платформа собирает такие данные для собственных целей;

3) назойливость – неоднократные просьбы к пользователям предпринять определенные действия, которые могут снизить защиту данных, например, просьбы включить уведомления или предоставить возможность отслеживать геолокацию. Практика использовалась на 41% сайтов.

ЕС также выделяет практику «перегрузки» – пользователю направляется большое количество запросов, пользователь устает и соглашается на все предлагаемые опции с ПД и дает непреднамеренное согласие на действия, на которые не хотел бы ранее давать. Например, постоянное направление просьбы указать номер телефона или предоставить доступ к контактам, в результате чего пользователю проще согласиться предоставить информацию, чем постоянно отказываться;

4) создание препятствий, например, предоставление возможности регистрации учетной записи, но отсутствие инструментов удаления аккаунта или необходимость выполнения неудобных действий (заполнение длинной формы или отправка письменного запроса в организацию), чтобы удалить аккаунт; принуждение делать множество кликов, чтобы получить информацию об использовании их ПД. Практика использовалась на 39% ресурсов;

5) принудительное использование – требование предоставить больше данных для доступа к услуге, чем необходимо для ее получения. Например, создание учетной записи через использование сторонних социальных сетей, чтобы получить доступ к данным пользователя об использовании этой соцсети. Такие практики использовались на 26% ресурсов. ОЭСР выделяет практику требования информации, например, о контактах пользователей для дальнейшей рассылки спама контактам потребителя, в том числе якобы от имени потребителя.

Опыт России

В России не закреплено понятия «темных практик» или иных аналогов для обозначения практик злоупотреблениями при сборе данных. Однако введение пользователей в заблуждение относительно условий конфиденциальности их данных может быть основанием для принятия санкций. Например, по решению Московского города суда платформа LinkedIn была заблокирована в России в 2016 г. за нарушение требования локализации персональных данных. Суд установил, что LinkedIn собирала поведенческие данные с помощью cookie-файлов, но не соблюдала в отношении собранных данных требования локализации, а в пользовательском соглашении устанавливало условие о праве платформы передавать все собранные данные третьим лицам[31]. В России предусмотрены нормы, предупреждающие введение пользователей в заблуждение в рамках законодательства о защите прав потребителей и в рамках законодательства о персональных данных.

Роскомнадзору целесообразно на основе общих нормативных положений и с учетом судебной практики разработать чек-лист признаков «темных практик» на цифровых платформах и сформировать открытый банк примеров, выявляемых на русскоязычных платформах. Открытый банк примеров может пополняться из материалов, присылаемых пользователями, в целях информирования их о рисках и мотивации платформ корректировать свою политику сбора данных пользователей до разбирательств Роскомнадзором.

3. Использование ИИ в судах

В Мониторинге №5 мы уже рассматривали вопрос использования ИИ в правоохранительной деятельности. Между тем формируется новый тренд – ограничение использования ИИ в судебном процессе. Суды стали получать жалобы на заключения

[31] https://mos-gorsud.ru/mgs/services/cases/appeal-civil/details/19d661b0-6b14-48eb-b753-9adbf19fe32a

адвокатов или доводы сторон, сгенерированные ИИ, содержащие ссылки на несуществующие судебные дела, нормы права или неподтвержденные аргументы.

Например, в 2023 г. Окружной суд Нью-Йорка наложил штраф в 5 тыс. долл. на стороны и их представителей за подачу письменных представлений, сгенерированных ChatGPT, включающих цитаты из минимум 6 несуществующих судебных решений[32]. Другой пример – решение Трибунала Налоговой палаты в Великобритании 2023 г. – в споре об уплате налогов сторона защиты использовала как минимум 4 ссылки на расследования налоговой службы, которых не существовало[33].

Поэтому в июле 2024 г. Окружной суд Западного округа Северной Каролины США[34], ограничил использование ИИ для формирования адвокатами заключений[35]. Установлено, что фактические и юридические ссылки в судебных документах, подготовленных с использованием ИИ, должны быть проверены сторонами, подающими документы. К любому представленному в Суд документу должно прилагаться заключение, что:

- при подготовке документа не использовался ИИ, за исключением ИИ, встроенного в стандартные онлайн источники юридических баз данных (как Westlaw, Lex1s);
- каждое заявление и ссылка на источники в документе должны быть проверены на предмет точности.

Аналогичные руководства были приняты и другими судами в США, например, в Манитобе[36], Юконе[37] и пр., а также судами в ряде других стран, например, в Великобритании (по использованию чат-ботов)[38], Новой Зеландии[39], Австралии[40] и др.

Устанавливается, что стороны и представители при использовании инструментов с ИИ в ходе судебных разбирательств должны:

- понимать, как работают инструменты. Например, качество сгенерированного юридического ответа зависит от данных, на которых обучался чат-бот, а также качества запроса самого пользователя;
- соблюдать правила конфиденциальности: любая личная информация, введенная в чат-бот, сохраняется и может быть использована в запросах других пользователей;
- если стороны представляют себя в суде самостоятельно (без юристов) – уведомлять суд о применении ИИ в документах, чтобы участники знали о рисках;
- проверять достоверность сведений, если при формировании документов использовался ИИ.

Текст, сгенерированный ИИ, следует проверять, чтобы:

1) не использовалась версия ИИ, которая обучена на устаревших данных, не включающих более позднюю судебную практику или изменения законодательства;

2) сформированная информация была полной и точной (не содержала ссылки на выдуманные судебные дела или нормы);

3) использованная практика была применима к юрисдикции, а не взята из других юрисдикций с иными материальными законами и процедурными требованиями.

Опыт России

В июле 2024 г. на сайте Верховного Суда Российской Федерации появилось его заявление о возможностях использования

[32] https://storage.courtlistener.com/recap/gov.uscourts.nysd.575368/gov.uscourts.nysd.575368.54.0_2.pdf

[33] Felicity Harber v The Commissioners for HMRC https://caselaw.nationalarchives.gov.uk/ukftt/tc/2023/1007

[34] Юрисдикция распространяется на суды Западного округа Северной Каролины.

[35] https://www.ncwd.uscourts.gov/sites/default/files/Standing%20Order%20In%20Re-%20Use%20of%20Artificial%20Intelligence2.pdf

[36] Суд королевской скамьи Манитобы, Практическое указание от 23 июня 2023 года «Использование ИИ при подаче заявлений в суд» https://www.manitobacourts.mb.ca/site/assets/files/2045/practice_direction_-_use_of_artificial_intelligence_in_court_submissions.pdf

[37] Верховный суд Юкона, Использование инструментов ИИ https://www.yukoncourts.ca/sites/default/files/2023-06/GENERAL-29%20Use%20of%20AI.pdf

[38] https://www.judiciary.uk/wp-content/uploads/2023/12/AI-Judicial-Guidance.pdf

[39] https://www.courtsofnz.govt.nz/going-to-court/practice-directions/practice-guidelines/all-benches/guidelines-for-use-of-generative-artificial-intelligence-in-courts-and-tribunals/

[40] https://www.supremecourt.vic.gov.au/forms-fees-and-services/forms-templates-and-guidelines/guideline-responsible-use-of-ai-in-litigation

ИИ при подготовке к судебному разбирательству[41]. Кроме того, рассматривается идея подключения ИИ к ГАС «Правосудие»[42,43].

Тем не менее Верховному Суду рекомендуется разработать требования при использовании ИИ в российских судах, включая:

1) уведомление суда и участников процесса, если для подготовки документов, используемых в ходе судебного заседания, применялся ИИ;

2) требование проверки достоверности всех ссылок на законодательство, судебную практику и иные источники.

[41] https://www.vsrf.ru/press_center/mass_media/33763/

[42]ГАС "Правосудие" – территориально распределенная автоматизированная информационная система, предназначенная для формирования единого информационного пространства судов общей юрисдикции и системы Судебного департамента при Верховном Суде.

[43] https://rg.ru/2023/05/25/robot-pomozhet-rassudit.html