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

Борьба с антиконкурентными практиками онлайн, использование технологиями персональных данных

Мониторинг №9 (Сентябрь 2024)

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., ст. науч. сотр. Малинина Т.А.

«Небывалая осень построила купол высокий,
Был приказ облакам этот купол собой не темнить.
И дивилися люди: проходят сентябрьские сроки,
А куда провалились студеные, влажные дни?».
А. Ахматова

В сентябре 2024 г. можно назвать 2 события, которые определяют тренды развития регулирования цифровой экономики в мире.

Тренд № 1. Борьба с антиконкурентными практиками онлайн

В сентябре 2024 г. опубликованы очередные результаты антимонопольных расследований деятельности Google в Великобритании и в Италии, Amazon в Германии. Все расследования касаются вопросов злоупотребления платформами доминирующим положением. Кроме того, в Китае с 1 сентября вступили в силу Временные положения о борьбе с недобросовестной конкуренцией в интернете, которые направлены, в том числе на отказ от обеспечения совместимости сервисов доминирующей платформы с сервисами других поставщиков.

Тренд № 2. Использование технологиями персональных данных

В сентябре 2024 г. регуляторы 4-х стран ЕС приняли решения о принципах использования компаниями персональных данных для обучения ИИ, создания баз данных и применения файлов cookie. Например, в Германии принято регулирование для «служб управления согласием» на использование файлов cookie, которое позволяет получить согласие лишь один раз для последующего использования цифровых услуг. Это избавит пользователей цифровых услуг от повторяющихся запросов на использование файлов cookie и сократит число возможных нарушений. Необходимость соблюдения баланса между развитием цифровой экономики и правами субъектов персональных данных в перспективе приведет к расширению прав регуляторов по уточнению и реализации законодательных требований к использованию персональных данных.

Кроме того, важным событием в сентябре 2024 г. стало подписание в Вильнюсе **Рамочной конвенции Совета Европы об искусственном интеллекте (ИИ) и правах человека,**

демократии и верховенстве права[1,2]. Конвенция является первым юридически обязывающим международным соглашением об ИИ. Периметр ее действия шире, чем у Закона об ИИ ЕС, так как ее могут подписать (и уже подписали) страны за пределами ЕС[3].

Отметим, что определение системы ИИ в Конвенции (ст. 2) совпадает с обновленным в марте 2024 г. определением ОЭСР (см. Мониторинг № 3). Конвенция содержит ряд концепций, уже закрепленных в Законе об ИИ ЕС, в частности подход, основанный на рисках, и возможность введения запретов для систем ИИ.

Положения Конвенции имеют общий характер, обусловленный необходимостью гибкого применения в быстро меняющейся среде, когда детали реализуемых мер (в частности, по защите конфиденциальности и персональных данных, информированию людей о том, что они взаимодействуют с ИИ, оспариванию людьми решений, принятых с использованием ИИ) оставлены на усмотрение подписавших сторон. При этом каждая сторона в течение 2-х лет с момента подписания Конвенции должна представить отчет с мерами по ее реализации (п. 1 ст. 24). В целом Конвенция может способствовать распространению в странах мира подходов к регулированию ИИ, закрепленных в принятом в 2024 г. Законе об ИИ ЕС.

Россия не является членом Совета Европы с марта 2022 г.[4], таким образом, она пока не может присоединиться к Конвенции.

В сентябре 2024 г. в России также произошло значимое событие в сфере регулирования цифровой экономики – **предложены законопроекты для регулирования дипфейков, включая использование голоса для создания дипфейка:**

1. Использование дипфейков для совершения уголовных преступлений.

Законопроектом № 718538-8[5] предложено в рамках Уголовного кодекса наказывать за преступления, совершенные с использованием изображения или голоса (в том числе фальсифицированных или искусственно созданных – включая дипфейки), а так же с использованием биометрических персональных данных потерпевшего или иного лица, включая клевету, кражу, мошенничество, вымогательство, причинение имущественного ущерба путем обмана или злоупотребления доверием. Кроме того, предлагается ввести ответственность за использование биометрических персональных данных с целью мошенничества в сфере компьютерной информации для хищения чужого имущества путем ввода, удаления, блокирования, модификации компьютерной информации и пр.

Следует отметить, что уголовное наказание за кражу или иное преступление с использованием дипфейков не отменяет ответственности в рамках законодательства о персональных данных. Это значит, что, например, мошенник получит не только срок за кражу с использованием дипфейка, но и штраф за незаконную обработку персональных данных в рамках административной ответственности;

2. Регулирование права на голос, включая обработку голоса.

Законопроектом 718834-8[6] предполагается внесение изменений в Гражданский кодекс (ст. 152.3) с целью признать «право на охрану голоса» (аналогичное уже принято в отношении изображения лица). Предлагается закрепить положение, что обнародование (в том числе в интернете) и использование голоса гражданина (например, в виде записи), в том числе с

[1] https://rm.coe.int/1680afae3c.

[2] От имени ЕС Конвенцию подписала Еврокомиссия (https://digital-strategy.ec.europa.eu/en/news/commission-signs-council-europe-framework-convention-artificial-intelligence), также ее подписали Андорра, Грузия, Исландия, Норвегия, Молдова, Сан-Марино, Израиль, Великобритания и США (https://www.coe.int/en/web/portal/-/council-of-europe-opens-first-ever-global-treaty-on-ai-for-signature).

В разработке Конвенции Комитетом по ИИ Совета Европы в качестве стран-наблюдателей участвовали Аргентина, Австралия, Канада, Коста-Рика, Ватикан, Израиль, Япония, Мексика, Перу, США и Уругвай (https://rm.coe.int/1680afae67

[3] Конвенция открыта для подписания странами – членами Совета Европы и иными странами, участвовавшими в ее разработке (п. 1 ст. 30). Впоследствии при получении согласия стран-членов к ней будет предложено присоединиться всем прочим странам (п. 1 ст. 31).

[4] https://www.coe.int/en/web/portal/46-members-states.

[5] https://sozd.duma.gov.ru/bill/718538-8#bh_histras

[6] https://storage.consultant.ru/site20/202409/17/pr_170924_834.pdf

помощью специальных технологий (например, ИИ для создания дипфейков) допускается только с согласия этого гражданина, а после его смерти – с согласия супруга, детей, родителей. Аналогичная норма существует для изображения гражданина, однако отличие состоит в том, что предлагаемые нормы использования голоса более современные, так как включают в том числе «специальные технологии», что подразумевает применение дипфейков и любых других технологий синтеза голоса. Фактически закрепляется 3 важных аспекта: (1) личное право лица на голос; (2) имущественное право, включая возможность передать свой голос наследникам, в том числе право его использования для объектов интеллектуальной собственности; (3) запрет на создание дипфейков без согласия лица.

Согласие при этом не требуется, если:

- голос используется в государственных, общественных или иных публичных интересах;
- голос записан при видео- или аудиозаписи, которая воспроизводится в местах свободного посещения, публичных мероприятиях (собраниях, конференциях, концертах и пр.);
- запись голоса производилась за плату.

Если голос гражданина был получен без его согласия и распространен в интернете, то возможно предъявлять требования об удалении записи и прекращении ее использования и распространения. В целом предлагаемые нормы могут снизить риски создания дипфейков для незаконного использования, фактически дипфейк можно создать только с согласия обладателя личных и имущественных прав на голос.

Во многом данный подход близок к регулированию дипфейков в США (анализировался авторами в Мониторинге №2), где в январе 2024 г. опубликован законопроект No AI Fraud Act[7]. В США предложено установить право собственности лица на свой голос и изображение (подобие), т.е. фактически имущественные права. Такое право приравнивается к праву интеллектуальной собственности и может свободно передаваться по наследству, и не прекращается после смерти еще в течение 10 лет независимо от того, использовались ли такие права физическим лицом при его жизни. Лицо может передать свое изображение или голос для создания цифрового изображения[8] или копии голоса[9] путем заключения письменного соглашения.

В России предлагаются схожие нормы – установление имущественных прав на голос, включая возможность его использования для создания объектов интеллектуальной собственности с учетом того, что дипфейк также может выступать объектом прав интеллектуальной собственности. При этом в России напрямую не закреплена норма об использовании голоса в рамках интеллектуальной собственности, однако эта норма подразумевается, так как право на голос становится в том числе имущественным правом.

В России следует уточнить такие правовые вопросы, как:

1) необходимо ли согласие лица в письменном виде, например, если такое использование планируется в коммерческих целях. Такое согласие подтвердит право третьего лица использовать голос, в том числе для создания объектов интеллектуальной собственности;

2) возникают ли в данном случае права интеллектуальной собственности на голос, в том числе возможность передачи таких прав наследникам. В данном случае необходимо установить срок действия интеллектуальных прав.

[7] https://www.congress.gov/bill/118th-congress/house-bill/6943/text?s=1&r=3

[8] Цифровое изображение (digital depiction) – точная копия, имитация или приближенное изображение человека (живого или умершего), которое создано или изменено полностью или частично с использованием цифровых технологий.

[9] Цифровая голосовая копия (digital voice replica) – аудиозапись, которая создана или изменена полностью или частично с использованием цифровых технологий и зафиксирована в звукозаписи или аудиовизуальном произведении, которое включает повторения, имитации лица, которые на самом деле лицо не озвучивало.

/ Ключевые аспекты

1. Борьба с антиконкурентными практиками онлайн

В Мониторинге №3 мы анализировали нормы регулирования в отдельных странах различных практик злоупотребления доминирующим положением платформ. Теперь рассмотрим применение этих норм в конкретных расследованиях.

Опыт ЕС и Великобритании

В сентябре 2024 г. проведен ряд антимонопольных расследований против Google и Amazon в Великобритании, Германии и Италии.

В деле против Google (Великобритания)[10] Управление по конкуренции и рынкам заявило о злоупотреблении Google доминирующим положением в трех частях цепочки стека рекламных технологий[11]: Google управляет инструментами покупки рекламы (Google Ads и DV360) и сервером DFP для публикации объявлений рекламодателями, а также рекламной биржей AdX.

Рекламные биржи проводят аукционы рекламных мест, сводя запросы от рекламораспространителей (сайтов, где публикуются объявления) и ответные ставки от рекламодателей (с ценами, по которым они готовы купить рекламное место). Затем проводится аукцион, где взимается комиссия за аукцион – 20% от суммы ставки. Все 3 платформы принадлежат Google, которая доминирует на рынке.

В сентябре началось расследование против компании Google, которая предоставляла преференции собственным сервисам:

- обеспечивала бирже Google AdX эксклюзивный доступ к рекламодателям;
- манипулировала ставками рекламодателей так, чтобы они имели более высокую стоимость при отправке на аукцион AdX, чем при отправке на аукционы конкурирующих бирж;
- биржа Google AdX могла первой подавать заявки на аукционах рекламных мест для их покупки, что фактически давало преимущественное право на участие в аукционе по сравнению с другими биржами.

К настоящему времени в отношении Google еще не вынесено решение, расследование продолжается.

В Италии в сентябре генеральный адвокат опубликовал оценку злоупотреблений Google доминирующим положением на рынке операционных систем[12]. Google разработала операционную систему с открытым исходным кодом Android. С 2015 г. запущен Android Auto – приложение для связи приложений с мобильных устройств и дисплеев автомобилей. Сторонние разработчики могут создавать собственные приложения, совместимые с Android Auto, используя шаблоны Google. Компания Enel X сообщила, что Google отказалась подключать ее приложение JuicePass с функций для электромобилей, так как приложение не совместимо с Android Auto (Enel не использовала специальный шаблон Google для совместимости).

Интересно, что генеральный адвокат для оценки положения Google на рынке использовал критерии «Броннера»[13] – практика, когда доминирующее предприятие отказывает в доступе к инфраструктуре, разработанной этим доминирующим предприятием для своей деятельности. При этом такой отказ приводит к устранению конкуренции на соответствующем рынке, так как нет альтернативной инфраструктуры, предоставляемой другими предприятиями. Однако адвокат признал критерии «Броннера» неприменимыми, так как платформа (Android Auto) была разработана доминирующим Google не для собственного

[10] https://www.gov.uk/government/news/cma-objects-to-googles-ad-tech-practices-in-bid-to-help-uk-advertisers-and-publishers

[11] Рекламный стек состоит из посредников, оказывающих услуги, направленные на покупки и продажи рекламных мест и рекламного пространства онлайн. Например, к таким посредникам относятся рекламные серверы для рекламораспространителей (продают места на своих сайтах для размещения рекламы); сервисы покупки рекламы (используются рекламодателями для приобретения рекламного места у рекламораспространителя); рекламные биржи (проводят аукционы в режиме реального времени для покупки и продажи рекламы)

[12] https://curia.europa.eu/jcms/upload/docs/application/pdf/2024-09/cp240132en.pdf

[13] judgment of the Court of Justice of 26 November 1998 in Case C-7/97 Bronner

исключительного использования, а для подключения приложений сторонних разработчиков.

Стоит отметить, что в России проводилось расследование против Apple[14] в 2020 г., когда Apple внедрила технические ограничения iOS с точки зрения настройки профиля конфигурации, что заставило «Лабораторию Касперского» ухудшить функциональность приложения Safe Kids (необходимо было удалить некоторые технологические компоненты, иначе доступ в App Store был запрещен). ФАС признала злоупотребление доминирующим положением Apple, использовав критерии, схожие с критериями «Броннера» – App Store была единственным каналом распространения приложений на iOS, при этом App Store – единственная возможность получить доступ сторонним разработчикам приложений на устройства с iOS.

Тем не менее в Италии действия Google признаны злоупотреблением, так как отказ приложению Enel не был объективно оправданным. Такой отказ мог бы быть «объективно оправдан», если бы доступ к платформе Android Auto был технически невозможен или влиял бы на ее производительность. Однако отказ из-за необходимости разработки специального шаблона для программы Enel не приводит к указанным техническим рискам, а требует только временных и финансовых затрат от Google.

Фактически ФАС России признала App Store единственной платформой для доступа к устройствам iOS, использовав критерии «Броннера», тогда как в Италии адвокат занял иную позицию (сослался на технические возможности платформы), хотя Android Auto, как и App Store для iOS, является единственной возможностью для получения доступа поставщиков приложений к машинам на Android. При этом в обоих случаях платформы создавались не только для собственной деятельности компаний по размещению приложений, а для подключения к устройствам сторонних приложений.

На данный момент в Германии в отношении Amazon проводится 2 расследования (начались в 2022 г.)[15]:

1) в связи с осуществлением Amazon контроля с помощью алгоритмов за ценами, которые устанавливались сторонними продавцами на маркетплейсе. В результате Amazon может блокировать или ограничивать продажи товаров от таких продавцов, если товары продаются по завышенными ценам;

2) в отношении системы «брендгейтинга»: Amazon создает реестр брендов и их дистрибьюторов, которые могут подтвердить свои интеллектуальные права на продажу товаров с соответствующим товарным знаком. Это необходимо, чтобы исключать с площадки продавцов, которые не имеют интеллектуальных прав на товарный знак продаваемых товаров. Антимонопольным органом планируется провести проверку условий допуска или исключения продавцов с площадки Amazon с учетом наличия у них прав на использование бренда (товарного знака).

В сентябре 2024 г. антимонопольный орган Bundeskartellamt запустил онлайн-опрос 2000 сторонних ритейлеров для изучения влияния цен Amazon на доступ к платформе.

Опыт Китая

С 1 сентября 2024 г. в Китае вступают в силу Временные положения по борьбе с недобросовестной конкуренцией в интернете[16], которые определяют запрещенные практики:

1) использование ложной и вводящей в заблуждение рекламы: распространение недостоверной информации о транзакциях, рейтингах продавцов и их товаров, о трафике; введение в заблуждение за счет предложения скидок для потребителей только за положительные отзывы;

2) фальсификация отзывов пользователей и иные практики с отзывами, например, использование изображений для маскировки отрицательных отзывов, размещение положительных оценок в начале списка отзывов и пр.;

3) нанесение ущерба деловой репутации конкурентов, например,

[14] https://docs.cntd.ru/document/565727153

[15] https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2022/14_11_2022_Amazon_19a.html

[16] https://scjgj.beijing.gov.cn/ztzl/gpjzyqjc/zjyq/202405/t20240524_3693717.html

распространение предупреждений о ложных рисках, писем с жалобами и пр.;

4) действия по вставке ссылок, в том числе для принудительного перехода по ним, чтобы мешать работе продуктов других поставщиков;

5) создание продуктов, несовместимых с продуктами других поставщиков;

6) скупка продавцом своих же товаров, чтобы оставить положительные отзывы или понизить рейтинг других поставщиков;

7) злоумышленные действия по завладению (добавление в корзину на маркетплейсе или бронирование) товарами в течение короткого периода времени без оплаты;

8) оптовые закупки с последующим возвратом или отказом в получении товара и пр.;

9) использование частых всплывающих окон, которые невозможно закрыть и пр.;

10) нарушение нормальной работы продуктов других поставщиков, например, путем запуска других приложений вопреки желанию пользователя, непредставление функций удаления приложений и пр.

Опыт России

К настоящему времени ФАС разработала свод практик для рынка, который определяет злоупотребления на цифровых рынках[17]. Однако в отличие от подхода Китая или стран ЕС такие принципы не содержат перечня злоупотреблений, связанных с антиконкурентным использованием накапливаемых платформами данных или с отказом от интероперабельности со сторонними сервисами и пр.

2. Использование технологиями персональных данных

Персональные данные – значимый ресурс для развития цифровой экономики, но при этом они принадлежат лицам, которые имеют право на конфиденциальность. В сентябре 2024 г. регуляторы ряда стран ЕС по результатам расследований приняли решения по правилам использования персональных данных для обучения ИИ, создания баз данных и применения файлов cookie.

Опыт стран ЕС

4 сентября 2024 г. Комиссия по защите данных Ирландии[18] завершила разбирательство в отношении компании X (бывший Twitter), которое начала в Высоком суде[19] 8 августа[20]. Поводом стала обработка компанией X в период с 7 мая по 1 августа 2024 г. персональных данных из публичных постов европейцев для обучения своей системы ИИ Grok[21]. Комиссия[22] подала в суд на компанию X, с требованием в срочном порядке обязать компанию приостановить, ограничить или запретить их обработку. Это было сделано впервые.

8 августа 2024 г. компания X согласилась приостановить оспариваемую обработку персональных данных. В итоге судебное разбирательство было прекращено на основании согласия X постоянно придерживаться принятых обязательств, конкретное содержание которых Комиссия не раскрывает.

При этом Комиссия запросила у Европейского совета по защите данных[23] в соответствии с п. 2 ст. 64 GDPR[24] разъяснение, в каких пределах персональные данные могут обрабатываться для разработки и обучения ИИ, и правовые основы такой обработки. Разъяснения пока не опубликованы.

Это дело показывает, что на текущем этапе регулирование использования персональных данных имеет пробелы, восполнение которых на практике зависит от договоренностей между регулятором и обработчиком данных.

Также в сентябре 2024 г. Управление по защите персональных данных Нидерландов[25] наложило штраф в размере

[17] https://fas.gov.ru/p/protocols/1666
[18] Data Protection Commission.
[19] Irish High Court.
[20] https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-welcomes-conclusion-proceedings-relating-xs-ai-tool-grok
[21] https://www.dataprotection.ie/en/news-media/press-releases/dpc-welcomes-xs-agreement-suspend-its-processing-personal-data-purpose-training-ai-tool-grok
[22] Data Protection Act 2018, https://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html
[23] European Data Protection Board.
[24] Общие положения о защите данных (Регламент ЕС 2016/679), https://eur-lex.europa.eu/eli/reg/2016/679/oj
[25] Autoriteit Persoonsgegevens.

30,5 млн евро на американскую компанию Clearview AI[26].

Clearview AI – коммерческая компания, не имеющая представительства в Европе, предлагает услуги по распознаванию лиц разведывательным и следственным службам. Клиенты компании предоставляют ей изображения, чтобы выяснить личность людей на снимках. Для этой цели у компании есть база данных с более чем 30 млрд фото людей, которые она автоматически собирает из интернета, а затем создает из них уникальный биометрический код для каждого лица без ведома и согласия на это людей.

Таким образом, любой человек, фото которого есть в интернете, может оказаться в этой базе данных. Отметим, что автоматический сбор и хранение информации из интернета (scraping) частными компаниями и лицами в Нидерландах обычно недопустимо[27]. Кроме того, по мнению Управления компания Clearview AI нарушила GDPR в части: 1) обработки биометрических персональных данных, так как компания не подпадает под исключения из общего запрета в законе (например, когда субъект данных дал ясное согласие на их обработку или обработка необходима для защиты жизненных интересов субъекта данных); 2) информированности субъектов данных, поскольку не сотрудничает по запросам о доступе к данным. Если компания не прекратит нарушения, то помимо основного штрафа должна выплатить дополнительный в размере до 5,1 млн евро.

В 2022 г. в отношении Clearview AI органом по защите данных Греции уже выносилось решение о штрафе в размере 20 млн евро за аналогичные нарушения GDPR[28], что не изменило практику компании. В связи с этим Управление по защите персональных данных Нидерландов ищет способы воздействия на компанию, в том числе исследуя возможности возложить ответственность на ее директоров, которые знали о нарушениях, но в рамках своих полномочий не препятствовали им. Таким образом, это дело подтверждает практику в деле г-на Дурова и Telegram: если европейские регуляторы не могут «дотянуться» до компании, они пытаются воздействовать на ее управляющих.

6 сентября 2024 г. Управлением по защите данных Бельгии[29] было принято постановление по незаконному применению компанией Mediahuis баннеров с уведомлением об использовании файлов cookie на 4 сайтах прессы, например, газеты Антверпена[30,31]. Управление получило от пользователя жалобу, что на сайтах нет достаточно быстро различимой кнопки «отклонить все» и используются обманные практики (вводящие в заблуждение цвета кнопок), а также отозвать согласие на использование файлов cookie непросто. Управление пришло к выводам, что:

1) согласие не может считаться данным свободно (как требует GDPR), если выбор «принять/отклонить все» не предлагается на одном уровне, например, кнопки рядом. Оно также не является однозначным, так как пользователь не знает, что кнопка «отклонить все» находится на следующем шаге;

2) на рассматриваемых сайтах кнопка «принять все» выделена ярким цветом, что побуждает нажать ее. Так нарушается предписанный GDPR принцип справедливости, в связи с чем согласие недействительно;

3) отзыв согласия возможен только после нескольких кликов, тогда как на согласие достаточно одного, что является нарушением GDPR.

Управление по защите данных дает компании 45 дней на корректировку этих недостатков, в том числе путем настройки кнопки отказа от файлов cookie и неиспользования вводящих в заблуждение цветов кнопок. По истечении этого срока на компанию будет налагаться штраф в размере 25 тыс. евро в день за каждый недостаток на каждом из сайтов. Компания может обжаловать это решение в суде[32].

[26] https://www.autoriteitpersoonsgegevens.nl/actueel/ap-legt-clearview-boete-op-voor-illegale-dataverzameling-voor-gezichtsherkenning
[27] https://www.autoriteitpersoonsgegevens.nl/actueel/ap-scraping-bijna-altijd-illegaal
[28] https://www.edpb.europa.eu/news/national-news/2022/hellenic-dpa-fines-clearview-ai-20-million-euros_en
[29] Gegevensbeschermingsautoriteit.
[30] Gazet van Antwerpen.
[31] https://www.gegevensbeschermingsautoriteit.be/burger/gba-neemt-maatregelen-tegen-mediahuis-voor-onrechtmatig-gebruik-van-cookiebanners-op-perssites
[32] Marktenhof.

Стоит отметить, что в Мониторинге №7 мы уже разбирали обманные практики, связанные с незаконным сбором данных.

Дело компании Mediahuis показывает, что использование персональных данных даже компаниями, деятельность которых открыта неограниченному числу лиц (СМИ), может существенно нарушать действующее законодательство, что дает повод для поиска альтернативных решений.

Так, в Германии создается альтернатива баннерам с уведомлением об использовании файлов cookie: 4 сентября 2024 г. правительством Германии было принято Постановление о создании служб управления согласием[33]. Эти службы сохраняют настройки пользователя, когда он первый раз использует цифровую услугу, и дают ему возможность пересмотреть решение в любое время, а поставщики цифровых услуг, добровольно присоединившиеся к сервису, по запросу будут получать информацию о решении пользователей. Предполагается, что этот новый, в том числе и в рамках ЕС, инструмент должен избавить пользователей цифрового контента от повторяющихся запросов на использование файлов cookie, дать возможность улучшить дизайн сайтов за счет сокращения баннеров и снизить поток файлов cookie. Успех подхода зависит от появления на рынке провайдеров услуг согласия, которые будут пользоваться спросом у пользователей и поставщиков цифровых услуг. Эффективность подхода планируется оценить через 2 года после вступления Постановления в силу.

Пользователи вправе в любое время сменить службу управления согласием, для чего последние должны сохранять настройки в машиночитаемом формате и бесплатно передавать их другой службе по выбору пользователя.

Для повышения доверия службы управления согласием должны быть признаны федеральным уполномоченным по защите данных и свободе информации[34], который включает их в публичный реестр. Для этого они должны предоставить в электронной форме уведомление со сведениями о себе, в том числе наименование, организационно-правовая форма и экономическая структура, включая источники финансирования. К уведомлению требуется приложить заявление, что поставщик услуг управления согласием не будет обрабатывать персональные данные пользователей для иных целей. Требуется также предоставить концепцию безопасности, включающую, в частности, информацию о месте хранения персональных данных, технических и организационных мерах защиты данных и управления рисками. Уполномоченный орган вправе отозвать признание поставщика услуг управления согласием, если он не выполняет установленные требования.

Этот инструмент, сократив поток файлов cookie, может снизить нарушения, связанные с использованием персональных данных.

Опыт России

В России данные из файлов cookie согласно позиции Роскомнадзора тоже признаются персональными данными, т.е. на их обработку требуется получать согласие субъекта, при этом отсутствие информирования об использовании таких файлов относится к числу нарушений[35]. Вместе с тем информация о соответствующих делах, как и о делах, связанных с использованием персональных данных для незаконного создания баз данных и обучения ИИ, в судебной практике отсутствует.

[33] https://bmdv.bund.de/SharedDocs/DE/Pressemitteilungen/2024/073-wissing-wir-wollen-die-cookie-flut-reduzieren.html; https://bmdv.bund.de/SharedDocs/DE/Anlage/K/veordnung-nach-26-absatz-2-tdddg-und-zur-aenderung-der-besonderen-gebuehrenverordnung-telekommunikation.pdf?__blob=publicationFile

[34] Bundesbeauftragte für den Datenschutz und die Informationsfreiheit.

[35] https://29.rkn.gov.ru/news/news340514.htm