



Институт развития
интернета

Еженедельный правовой дайджест
Интернет и информационные
технологии
Выпуск № 129
27.01.2023

Оглавление

Российская Федерация	3
Раздел 1. Законы и законопроекты	3
Раздел 2. Акты и проекты актов Президента	3
Раздел 3. Акты и проекты актов Правительства	4
Раздел 4. Практические кейсы	6
Зарубежные страны	7
Раздел 1. Зарубежное нормотворчество.....	7
Раздел 2. Зарубежные практические кейсы.....	30
Исследования, экспертные мнения, позиции государственных органов, организаций	37



РОССИЙСКАЯ ФЕДЕРАЦИЯ

Раздел 1. Законы и законопроекты

Об информационной поддержке НКО

В Государственную Думу внесён законопроект № [281856-8](#) «О внесении изменений в статью 31-1 Федерального закона "О некоммерческих организациях».

Предусматривается возможность государственным и муниципальным органам предоставлять некоммерческим организациям путём оказания или содействия в оказании услуг по предоставлению вычислительных мощностей.

Минцифры России также сможет содействовать НКО в интеграции их ресурсов с Единым порталом государственных и муниципальных услуг.

Раздел 2. Акты и проекты актов Президента

О государственной культурной политике

Подписан [указ](#) Президента Российской Федерации от 25 января 2023 года № 35 «О внесении изменений в Основы государственной культурной политики, утвержденные Указом Президента Российской Федерации от 24 декабря 2014 г. № 808».

Среди прочего предусматривается:

- формирование безопасной информационной среды путем популяризации информационных ресурсов, с использованием которых распространяется достоверная информация и которые способствуют культурно-историческому просвещению и воспитанию на основе традиционных российских духовно-нравственных ценностей;
- совершенствование российских информационно-поисковых систем как

средства интеллектуального и культурного развития личности;

- формирование государственного заказа на создание информационных материалов, распространяемых в средствах массовой информации, кинематографической и печатной продукции, телерадиопрограмм и интернет-ресурсов, соответствующих целям и задачам государственной культурной политики, а также обеспечение контроля качества выполнения этого государственного заказа;
- нейтрализация деструктивного информационно-психологического воздействия, направленного на размывание традиционных российских духовно-нравственных ценностей.

Раздел 3. Акты и проекты актов Правительства

О классифайдах трансграничной передаче персональных данных

Минцифры России опубликовало:

- [проект постановления](#) Правительства Российской Федерации «Об утверждении Правил взаимодействия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций с оператором связи, владельцем сервиса размещения объявлений, а также Правил ограничения и возобновления доступа к сервису размещения объявлений и информирования о таком ограничении»;
- [проект постановления](#) Правительства Российской Федерации «Об утверждении перечня документов, свидетельствующих о соблюдении владельцем сервиса размещения объявлений требований частей 7 и 8 статьи 10.7 Федерального закона «Об информации, информационных технологиях и о защите информации», а также формы и порядка направления в федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой



информации, массовых коммуникаций, информационных технологий и связи, таких документов».

Взаимодействие владельцев сервисов размещения объявлений с Роскомнадзором будет осуществляться:

- в электронной форме посредством электронной почты, личного кабинета владельца сервиса размещения объявлений на официальном сайте Роскомнадзора 87-fz.rkn.gov.ru

- в бумажном виде, посредством почтовой связи или личного предоставления документов.

Ограничение и возобновление доступа к классифайдам будет осуществляться операторами связи в течение суток с момента получения от Роскомнадзора необходимой информации.

Подтверждать соответствие сервиса размещения объявлений требованиям закона будут следующие документы:

- 1) заявление с реквизитами и контактами владельца классифайда и данными о сервисе, включая количество его российских пользователей в сутки;

- 2) заверенные в соответствии с законодательством иностранного государства копии учредительных документов иностранных юридических лиц с заверенным в установленном законодательством Российской Федерации порядке переводом на русский язык (учредительные документы российских юридических лиц представляются по инициативе заявителя);

- 3) выписка из реестра акционеров (список участников общества с ограниченной ответственностью представляется по инициативе заявителя), а также документ, содержащий в соответствии с законодательством государства регистрации учредителей (участников) юридического лица сведения о количестве голосов, приходящихся на голосующие акции (доли), составляющие уставный капитал юридического лица, с указанием соответствующих учредителей

(участников) юридического лица, имеющих право прямо или косвенно распоряжаться указанными голосами;

4) выписка из торгового реестра государства регистрации или иной эквивалентный документ;

5) копия документа, удостоверяющего личность (для физических лиц);

6) копия документа, свидетельствующего о подаче уведомления о наличии у гражданина Российской Федерации иного гражданства либо вида на жительство или иного действительного документа, подтверждающего право на его постоянное проживание в иностранном государстве (представляется по инициативе заявителя);

7) иные документы.

Раздел 4. Практические кейсы

О создании Национального технологического центра цифровой криптографии

Минцифры России [объявило](#) о создании Национального технологического центра цифровой криптографии, который начнет свою работу в 2024 году.

Целью центра является внедрение и популяризация использования методов криптографической защиты.

В задачи центра входят:

- развитие здоровой конкуренции у отечественных производителей средств криптозащиты;
- производство компонентов средств защиты персональных данных;
- ведение реестра производителей средств криптозащиты;
- практическое обучение специалистов по информационной безопасности;
- определение стандартов в области криптографии и защиты информации.



Об иске МТС к ФАС России

ПАО «Мобильные телесистемы» обратилось в Арбитражный суд города Москвы с иском к ФАС России.

Компания не согласна с [решением](#) регулятора о необоснованном повышении тарифов, вынесенном в октябре 2022 года.

Компания утверждает, что ФАС России выносила свое решение, исходя из некорректного расчёта соотношения прироста выручки и расходов компании в 2022 году.

Заявление по делу № [А40-10774/2023](#) в настоящий момент не принято к производству.

ЗАРУБЕЖНЫЕ СТРАНЫ

Раздел 1. Зарубежное нормотворчество

О массачусетском Билле о правах в Интернете

Билль о правах в Интернете внесен на рассмотрение в Палату представителей штата Массачусетс, США ([HD 3245](#)).

Билль применяется к обработке персональных данных полностью или частично автоматизированными средствами и к обработке не автоматизированными средствами персональных данных, которые являются частью системы учета или должны стать частью системы учета, и предоставляет физическим лицам защиту в отношении обработки персональных данных и свободного перемещения персональных данных.

Кроме того, предусматриваются различные права субъектов данных, включая:

- право на получение информации;

- право на получение подтверждения обработки данных;
- право на исправление без неоправданной задержки персональных данных;
- право на передачу данных;
- право на возражение против обработки персональных данных в маркетинговых целях;
- право не быть объектом решения, основанного исключительно на автоматизированной обработке.

В частности, требуется, чтобы контролеры без неоправданной задержки сообщали субъекту персональных данных о любом нарушении персональных данных и документировали любые нарушения персональных данных, чтобы Генеральный прокурор мог проверить соблюдение требований.

Кроме того, контролер и обработчик обязаны назначить ответственного за защиту данных в случаях, включая государственные органы или учреждения, когда основная деятельность контролера или обработчика состоит из операций по обработке, которые по своему характеру, масштабу или целям требуют регулярного и систематического мониторинга субъектов данных в больших масштабах.

Что касается ответственности, законопроект подразделяет нарушения на уровни:

- нарушения положений, включающих обязанности контроллера и процессора, подлежат административным штрафам в размере до 10 млн долларов (~690 млн рублей) или, в случае предприятия, до 2% от общего мирового годового оборота за предыдущий финансовый год, в зависимости от того, что больше;
- нарушение положений, включая основные принципы обработки и условия для получения согласия, права субъектов данных, передача персональных данных получателю в иностранном государстве, влечет наложение административных штрафов в размере до 20 млн долларов (~1,3 млрд рублей) или, в случае предприятия, до 4% от общего мирового годового оборота за предыдущий

финансовый год, в зависимости от того, что выше.

О правилах трансграничного доступа к электронным доказательствам в ЕС

Совет Европейского Союза **объявил** о достижении соглашения с Европейским парламентом по предложению о **Регламенте** о европейских постановлениях о производстве и сохранении электронных доказательств в уголовном судопроизводстве и исполнении приговоров о лишении свободы после уголовного судопроизводства, а также о предложении о **Директиве**, устанавливающей согласованные правила по назначению назначенных учреждений и назначению законных представителей для целей сбора электронных доказательств в уголовном судопроизводстве.

Предлагаемые Регламент и Директива позволят соответствующим органам направлять судебные распоряжения о предоставлении электронных доказательств непосредственно поставщикам услуг в другом государстве-члене ЕС.

В частности, в Регламенте разъясняется, что поставщиками услуг, наиболее подходящими для сбора доказательств в уголовном процессе, являются поставщики услуг электронных коммуникаций и конкретные поставщики услуг информационного общества, которые облегчают взаимодействие между пользователями.

Соответствующие категории поставщиков услуг включают онлайн-рынки, предоставляющие потребителям и предприятиям возможность общаться друг с другом, и другие услуги хостинга, в том числе в случаях, когда услуги предоставляются посредством облачных вычислений, а также онлайн-игровые платформы и платформы для азартных игр.

Поставщики услуг, как правило, должны будут ответить на постановление о предоставлении данных в течение десяти дней, а в случае несоблюдения требований

налагаются денежные штрафы в размере до 2% от их общего годового оборота по всему миру за предыдущий финансовый год.

Директива является инструментом в применении предлагаемого Регламент, поскольку она устанавливает правила, применимые к назначению законных представителей поставщиков услуг или назначению их уполномоченных учреждений, которые отвечают за получение и реагирование на постановления о производстве и сохранении данных.

О неприкосновенности частной жизни в Нью-Гэмпшире

В Сенат штата Нью-Гэмпшир, США внесен законопроект об ожидании неприкосновенности частной жизни ([SB 255](#)).

В частности, законопроект предусматривает, что потребители имеют право:

- подтвердить, обрабатывает ли контролер персональные данные потребителя, и получить доступ к таким данным, если это не приведет к раскрытию коммерческой тайны;
- исправлять неточности в персональных данных потребителя, принимая во внимание характер персональных данных и цели обработки;
- удалять персональные данные, полученные или предоставленные потребителем;
- на переносимость данных, в той мере, в какой это технически возможно, при которой легко используемый формат позволяет потребителям беспрепятственно передавать данные другому контроллеру;
- на отказ от обработки персональных данных для целевой рекламы, продажи персональных данных или профилирования в поддержку автоматизированных решений, которые приводят к юридическим или значительным последствиям.

Кроме того, предусматривается, что контролеры должны отвечать на запросы субъектов персональных данных в течение 45 дней, но могут продлить срок ответа еще на 45 дней, если это разумно необходимо.

Если контролеры отклоняют запросы субъектов данных, они должны информировать потребителей об обосновании отклонения, а если запросы потребителей являются явно необоснованными, чрезмерными или повторяющимися, контролер может взимать с потребителя разумную плату.

Также вводятся следующие обязанности контроллера:

- ограничение сбора персональных данных тем, что является адекватным, релевантным и разумно необходимым в связи с целью;
- создание, внедрение и поддержание разумных административных, технических и физических методов защиты данных;
- запрет на обработку чувствительных данных без предварительного получения согласия субъекта данных (те же положения применяются к обработке персональных данных несовершеннолетних);
- обеспечение эффективного механизма для субъектов данных для отзыва согласия;
- не обрабатывать персональные данные субъектов данных для целевой рекламы или продажи персональных данных потребителей без согласия, если известно, что субъекту данных не менее 13 лет, но менее 16 лет.

Законопроект также подробно описывает обязанности обработчиков, а именно следование инструкциям контроллера и оказание помощи контролерам в выполнении обязательств, включая:

- соответствующие технические и организационные меры для выполнения обязательств контроллера в отношении запросов субъектов данных;
- оказание помощи контроллеру в выполнении его обязательств по обеспечению безопасности;

- предоставление необходимой информации для того, чтобы контроллер мог проводить и документировать оценки защиты данных.

Отношения между контроллером и обработчиком должны регулироваться договором, которые определяет конкретные обязательства сторон.

О вашингтонской Хартии персональных данных

Законопроект о создании Хартии персональных данных внесен в законодательное собрание штата Вашингтон, США ([HB 1616](#)).

Законопроект предоставляет лицам, проживающим в штате Вашингтон, права по управлению своими персональными данными, включая право знать, иметь доступ, возражать, исправлять и удалять.

Кроме того, устанавливаются требования к политике конфиденциальности, которую должны предоставлять организации, подпадающие под действие Хартии, включая как длинную, так и короткую форму политики конфиденциальности, которая постоянно и на видном месте должна быть доступна.

Разъясняется, что лица в возрасте 13 лет и старше будут считаться компетентными для осуществления всех прав, предоставляемых физическим лицам.

О конфиденциальности студентов и сотрудников в Нью-Йорке

В Ассамблею штата Нью-Йорк, США на рассмотрение внесен законопроект о внесении изменений в трудовое законодательство в связи с «Единым законом о защите конфиденциальности работников и студентов в Интернете» ([A01360](#)).

Предусматривается, что работодатели не могут:

1. требовать, принуждать или просить работника:

- раскрывать информацию для входа в защищенный личный аккаунт в Интернете;

- раскрывать содержимое аккаунта, за исключением того, что работодатель может попросить работника добавить работодателя в список лиц, которым работник предоставляет доступ к содержимому, или не удалять его из него;

- изменять настройки онлайн-аккаунта таким образом, чтобы сделать информацию для входа или содержимое аккаунта более доступными для других;

- получать доступ к учетной записи в присутствии работника таким образом, чтобы работодатель мог наблюдать за информацией о входе для контроля над учетной записью.

2. принимать или угрожать принятием неблагоприятных мер в отношении работника за невыполнение:

- требования работодателя или принудительное действие;
- просьбу работодателя добавить работодателя в список лиц, которым работник предоставляет доступ к содержимому защищенного личного аккаунта, или не удалять его из него.

Законопроект предусматривает аналогичные запреты для защиты информации учащихся.

Предусматриваются исключения из запретов на доступ к информации учащихся, включая:

- доступ к общедоступной информации;
- соблюдение закона или постановления суда;
- требование или запрос, основанный на конкретных фактах, доступа к защищенным личным онлайн аккаунтам учащегося для того, чтобы:

- обеспечить соблюдение закона или неправомерное поведение студента, связанного с обучением;

- защитить от угрозы безопасности, информации учебного заведения или систем коммуникационных технологий.

О требованиях к уведомлению о нарушениях данных в Нью-Йорке

В Сенат штата Нью-Йорк, США внесен законопроект, вносящий поправки в Общий закон о бизнесе (SB 2659).

Предусматривается, что предприятие должно предоставить уведомление о нарушении данных в течение 15 дней.

В список организаций, которые должны быть уведомлены о нарушении данных, затрагивающем любого жителя Нью-Йорка, включен Департамент финансовых услуг.

О конфиденциальности биометрии в Мэриленде

В Сенат штата Мэриленд, США внесен законопроект «Коммерческое право - защита потребителей - конфиденциальность биометрических данных» (SB 169).

Законопроект направлен на регулирование использования биометрических данных частными организациями.

Требуется, чтобы каждая частная организация, владеющая биометрическими данными, разработала письменную политику и сделала ее доступной для общественности, установив график хранения и руководящие принципы для окончательного уничтожения биометрических данных в определенные сроки и с учетом исключений.

Кроме того, устанавливаются требования к хранению, передаче и защите от разглашения всех биометрических данных организациями, на которые распространяется действие закона.

Частным организациям запрещается осуществлять определенные операции, такие как:

- продажа, сдача в аренду или торговля биометрическими данными любого лица; и

- обуславливать предоставление услуги сбором, использованием, раскрытием, передачей, продажей или обработкой биометрических данных, если только биометрические данные не являются строго необходимыми для предоставления услуги.

О регулировании цифровых платформ в Таиланде

В Таиланде принят Королевский указ о предприятиях, предоставляющих услуги цифровых платформ, которые требуют уведомления ([В.Е. 2565](#)).

Указ налагает обязательства на цифровые платформы, которые предоставляют услуги электронных посредников с управлением информацией для создания связи между предприятиями, потребителями и пользователями через компьютерную сеть с целью осуществления электронных транзакций, с оплатой или без оплаты услуг.

Королевский указ требует, чтобы сервисы цифровых платформ уведомляли Агентство по развитию электронных транзакций об определенной информации до начала своей деятельности на ежегодной основе.

Кроме того, сервисы цифровых платформ должны информировать пользователей о правилах и условиях использования платформы до или во время использования.

Указ распространяется на любую платформу цифровых услуг, целью которой является обслуживание пользователей в Таиланде, независимо от местонахождения поставщика платформы цифровых услуг.

Указ вступит в силу 20 августа 2023 года.

О защите потребительских данных на Гавайях

В законодательное собрание штата Гавайи, США внесен законопроект о защите потребительских данных ([SB 1110](#)).



Законопроект предусматривает создание основы для регулирования доступа контролеров и обработчиков к персональным потребительским данным.

Вводятся новые права потребителей, такие как право на доступ, переносимость данных, исправление, удаление и право отказаться от обработки персональных данных в целях целевой рекламы, продажи персональных данных или профилирования в поддержку решений, принятых контролером.

Кроме того, законопроект устанавливает, что нарушение представляет собой нечестный метод конкуренции и обманчивые действия или практику при ведении любой коммерческой деятельности, и предусматривает частный иск для потребителей, чьи права нарушены.

Законопроект уже был принят [в первом чтении](#).

О защите данных детей в социальных сетях в Нью-Джерси

В Сенат штата Нью-Джерси, США внесен законопроект стандартах конфиденциальности и управления данными в социальных сетях для детей и учреждении Комиссии по защите данных детей Нью-Джерси ([S3493](#)).

Подчеркивается, что до того, как новая онлайн-услуга, продукт или функция будет предложена пользователям, проживающим в Нью-Джерси, и к этой онлайн-услуге, продукту или функции, вероятно, будут иметь доступ дети, платформа социальных сетей должна предпринять ряд действий, включая:

- завершение оценки воздействия на защиту данных (DPIA) и ведение документации по оценке;
- документирование любого риска нанесения существенного ущерба детям, выявленного в ходе DPIA, и создание своевременного плана по смягчению или устранению этих рисков до получения доступа детьми;
- расчетный возраст, для которого характеристики подходят детям, исходя из рисков, возникающих в результате практики управления данными, или

применение мер защиты данных, предусмотренных для детей, ко всем пользователям;

- настройка всех параметров конфиденциальности по умолчанию, предоставляемых детям, на параметры, обеспечивающие высокий уровень конфиденциальности, если только организации не смогут продемонстрировать убедительные причины того, что иные настройки отвечают наилучшим интересам детей;

- предоставление очевидного сигнала о том, что за ребенком ведется слежка, если онлайн-активность детей может быть отслежена;

- предоставление любой информации о конфиденциальности, условиях предоставления услуг, политике и стандартах сообщества с использованием ясного языка, который может быть понятен детям;

- предоставление заметных, доступных и оперативных инструментов, помогающих детям или их родителям/опекунам осуществлять свои права на конфиденциальность.

Платформы социальных сетей должны пересматривать все DPIA не реже одного раза в два года.

Кроме того, платформы социальных сетей не должны, среди прочего, использовать персональные данные детей:

- использовать персональные данные детей таким образом, который наносит существенный вред физическому здоровью, психическому здоровью или благополучию;

- составлять профиль детей по умолчанию;

- собирать, продавать, передавать или хранить информацию, которая не является необходимой для предоставления услуг;

- собирать, продавать, передавать или сохранять любую геолокационную информацию детей по умолчанию;

- использовать обманные методы разработки, чтобы побудить или поощрить детей предоставлять больший объем персональных данных, чем это разумно необходимо для предоставления услуг, которые, как известно платформе социальных сетей, наносят существенный вред физическому здоровью, психическому здоровью или благополучию.

В рамках Отдела по делам потребителей Департамента законодательства и общественной безопасности предусматривается создание Комиссии по защите данных детей Нью-Джерси.

О законе о цифровой справедливости в Нью-Йорке

В Сенат штата Нью-Йорк, США внесен законопроект о внесении изменений в Закон об общем бизнесе, Закон об исполнительной власти, Закон о финансах штата и Закон об образовании в связи с принятием Закона о цифровой справедливости ([S3493](#)).

Установлено, что любая организация, которая ведет бизнес в Нью-Йорке и в рамках бизнес-процесса хранит персональные 500 или более лиц, должна предоставить уведомление об использовании персональных данных.

Уведомление должно быть кратким и понятным, размещенным на видном месте и написанным ясным и понятным языком, чтобы сложная информация была понятна обычному пользователю.

Законопроект ограничивает персональные данные, которые могут быть собраны, и требует от организаций, на которые распространяется действие закона, защищать данные от несанкционированного доступа и передавать ее только уполномоченным лицам, которые будут обращаться с персональными данными с такой же осторожностью.

Предусмотрены запреты на обработку биометрической информации и на скрытое наблюдение с помощью потребительских устройств.

Устанавливается, что незаконно обрабатывать персональные данные или целевую рекламу таким образом, чтобы дискриминировать, в частности, в сфере занятости, финансов, здравоохранения, кредитования, страхования, жилья, возможностей получения образования, возраста, пола, инвалидности, сексуальной ориентации, гендерной идентичности или предрасположенных генетических характеристик.

Кроме того, законопроект требует, чтобы все государственные организации, прежде чем приобретать или внедрять автоматизированные системы принятия решений, предоставляли такие системы для аудита, проводимого независимой третьей стороной.

Лица, подвергающиеся автоматизированному принятию решений, которые затрагивают их права человека или свободу, должны получать уведомление о принятом решении, об участии автоматизированного принятия решений, а также возможность оспорить решение и добиться его пересмотра человеком.

Также предусматривается, что Управление по оценке штата Нью-Йорк обновляет учебные программы начального/промежуточного уровня для обучения цифровой грамотности и цифровой конфиденциальности.

Законопроект находится на рассмотрении в Комитете по Интернету и технологиям.

О защите данных потребителей в Индиане

В Генеральную Ассамблею штата внесен законопроект о внесении изменений в Кодекс штата в части защиты данных потребителей ([HB 1554](#)).

Вводятся новые определения и положения, касающиеся:

- прав потребителя в отношении персональных данных;
- роли и ответственности контролеров в отношении персональных данных потребителей;

- требования к оценкам защиты данных, которые должны проводить контролеры;
- требования к обработке деидентифицированных или псевдонимных данных;
- создание, ведение и публикация отделом защиты прав потребителей Генерального прокурора ежеквартального списка адресов электронной почты потребителей, которые просят не продавать их персональные данные; и
- требования к брокерам данных, имеющим отношение к персональным данным потребителей, предоставлять уведомления о нарушениях безопасности и ежегодно регистрироваться в генеральной прокуратуре штата.

В случае принятия новые положения вступят в силу 1 января 2024 года.

О конфиденциальности медицинской информации в Нью-Йорке

В Сенат штата Нью-Йорк, США внесен законопроект о стандартах конфиденциальности для электронных медицинских продуктов и услуг и допустимого посредничества в передаче данных ([SB 185](#)).

Для организации, подпадающей под действие закона, будет незаконным заниматься обработкой данных, геофенсингом (таргетинг, основанный на местоположении пользователя) или посредничеством в передаче данных, если:

- пользователи, к которым относится информация, дали прямое утвердительное согласие на такую обработку данных, и, если такая покрываемая организация будет осуществлять посредничество в передаче данных пользователя, пользователь также должен дать отдельное утвердительное согласие на такую посредническую деятельность;
- такое использование данных является строго необходимым и осуществляется с целью:

- защиты от злонамеренной, мошеннической или незаконной деятельности;
- обнаружения, реагирования или предотвращения инцидентов или угроз безопасности;
- выполнения постановления суда.

Характер любой обработки данных или брокерской деятельности с данными должен быть доведен до сведения в ясных и заметных выражениях таким образом, чтобы обычный клиент заметил и понял эти условия.

В отношении согласия устанавливается, что пользователь может дать согласие на обработку данных или брокерскую деятельность от имени несовершеннолетних, находящихся на его иждивении, и что организации должны предоставить эффективный механизм для отзыва пользователем своего согласия после его предоставления.

Для получения согласия в соответствии с требованиями, организации, подпадающие под действие закона, должны:

- раскрывать пользователям все данные, собранные от них при предоставлении согласия;
- раскрывать пользователям все третьи стороны, которым может быть передана личная медицинская информация и другие данные таких пользователей на основании согласия;
 - цель сбора любых персональных данных;
 - позволять пользователю отозвать согласие в любое время.

О конфиденциальности данных в Массачусетсе

В Палату представителей штата Массачусетс, США внесен проект закона о защите конфиденциальности данных штата Массачусетс ([SD 745](#)).

Законопроект распространяется на организацию или любое лицо, кроме физического, действующее в некоммерческом контексте, которое самостоятельно

или совместно с другими определяет цели и средства сбора, обработки или передачи данных.

Законопроект не распространяется на:

- государственные учреждения или поставщиков услуг для государственных учреждений;
- организацию, которая отвечает следующим критериям:
 - средний валовой доход организации или лица за период не превышал 20 млн долларов;
 - организация или лицо в среднем не собирала и не обрабатывала ежегодно закрытые данные более 75 000 человек, при условии, что все закрытые данные для этих целей были удалены или деидентифицированы в течение 90 дней;
 - ни один компонент ее дохода не поступает от передачи данных в течение любого года (или части года, если организация существует менее одного года), который имеет место в течение периода.

Вводятся запреты:

- сбор, обработка или передача номера социального страхования;
- сбор или обработка конфиденциальных данных, за исключением случаев, когда это строго необходимо для предоставления или обслуживания конкретного продукта или услуги, запрошенной физическим лицом;
- передача конфиденциальных данных физического лица третьей стороне.

О праве собственности на свои данные

В законодательное собрание штата Гавайи, США внесен законопроект о внесении поправки к Конституции штата Гавайи ([SB 21](#)).

Предлагается внести изменения в статью I Конституции штата Гавайи, установив право каждого человека владеть своими данными и иметь

исключительное право собственности на данные, которые он генерирует в Интернете.

Предусматривается, что законодательный орган определит, какие данные подпадают под действие этого положения и каким образом это положение будет внедряться и обеспечиваться.

О хранении персональных данных в Дании

Датский орган по защите данных (Datatilsynet) опубликовал [Руководство](#), целью которого является разъяснение рамок хранения персональных данных контролерами данных исключительно для того, чтобы иметь возможность документально подтвердить согласие в соответствии с правилами защиты данных.

Данное руководство дополняет решение регулятора от 2022 года, в котором он постановил, что пятилетний срок хранения для документального подтверждения действительности полученного согласия противоречит принципу ограничения хранения, предусмотренного статьей 5(1)(e) GDPR.

О дизайне, соответствующем возрасту, в Коннектикуте

В Генеральную Ассамблею штата Коннектикут, США внесен проект закона об установлении в штате Коннектикут кодекса дизайна, соответствующего возрасту детей ([HB 6253](#)).

Законопроект направлен на создание обязательств по обеспечению конфиденциальности и безопасности для поставщиков онлайн-продуктов и услуг, к которым имеют доступ дети.

В случае принятия компании, предоставляющие онлайн-продукты и услуги, доступ к которым могут получить дети младше 18 лет, должны будут принимать меры по обеспечению конфиденциальности и безопасности, включая, но не ограничиваясь этим: стандартные настройки конфиденциальности,

обеспечивающие максимальный уровень конфиденциальности; и четко и кратко сформулированные политики конфиденциальности и условия предоставления услуг.

О конфиденциальности информации о социальной помощи

В законодательное собрание штата Небраска, США внесен проект закона о конфиденциальности информации о социальной помощи ([LB 592](#)).

Предусматривается, что закон будет применяться только к органам власти штата или местного самоуправления, включая государственно-частное партнерство.

Устанавливается, среди прочего, что персонально идентифицируемая информация физического лица или информация о социальной помощи может быть добавлена в закрытую систему данных только в том случае, если физическое лицо:

- дает согласие на ее включение в каждый случай обращения за услугами; и
- сохраняет право в любой момент отозвать согласие.

О массачусетском законе о конфиденциальности и безопасности информации

В Палату представителей штата Массачусетс, США внесен проект закона о конфиденциальности и безопасности информации ([SD 1971](#)).

Закон будет применяться к контроллеру или процессору, который ведет бизнес в штате, или когда деятельность по обработке данных контроллера или процессора, физически не расположенного там, связана с предложением товаров или услуг, предназначенных для частных лиц, или отслеживает поведение частных лиц, когда такое поведение происходит в Массачусетсе.

Контролер будет подпадать под действие закона, если он:

- имеет годовой глобальный валовой доход более 25 млн долларов;
- был брокером данных; или



- определил цели и средства обработки личной информации не менее 100.000 физических лиц, исключая персональные данные, обрабатываемые исключительно с целью завершения кредитной, чековой или наличной транзакции, при которой не сохраняется личная информация о физическом лице, заключающем транзакцию.

Кроме того, устанавливаются общие принципы обработки персональных данных, законные основания для их обработки и меры защиты при обработке конфиденциальной информации.

Физическим лицам предоставляются различные права в отношении обработки их данных, включая право на уведомление о конфиденциальности на этапе сбора данных или до него, право отказаться от обработки данных в целях продажи и таргетированной рекламы, право на доступ и транспортировку, удаление и исправление данных, а также право на отзыв согласия.

Контролеры должны будут установить, внедрить и поддерживать разумную политику, практику и процедуры для выявления, оценки и смягчения разумно прогнозируемых рисков для конфиденциальности и познаваемого вреда, связанных с их продуктами и услугами, а также проводить и документировать оценку рисков до начала такой обработки.

Кроме того, законопроект наделяет Генерального прокурора штата полномочиями по обеспечению соблюдения предлагаемого закона, включая выдачу требования о проведении гражданского расследования, если у Генерального прокурора штата есть разумные основания полагать, что организация совершила, совершает или собирается совершить нарушение закона.

О законопроекте о защите данных потребителей в Айове

В Сенат штата Айова, США внесен проект закона о защите данных потребителей ([SSB 1071](#)).

Закон будет применяться к лицу, ведущему бизнес в Айове или производящему продукты или услуги, предназначенные для потребителей, которые являются жителями Айовы, и которое в течение календарного года выполняет одно из следующих действий:

- контролирует или обрабатывает персональные данные не менее 100.000 потребителей;
- контролирует или обрабатывает персональные данные не менее 25.000 потребителей и получает более 50% валового дохода от продажи персональных данных.

Кроме того, предусматриваются права потребителей, включая право на доступ, получение копии и удаление персональных данных, а также на отказ от целевой рекламы или продажи персональных данных.

Устанавливаются следующие обязанности контролеров данных:

- принятие и внедрение разумных административных, технических и физических методов обеспечения безопасности данных для защиты конфиденциальности, целостности и доступности персональных данных;
- запрет обработки чувствительных персональных данных потребителя без четкого уведомления потребителя и возможности отказаться от такой обработки;
- предоставление потребителям разумно доступного, ясного и содержательного уведомления о конфиденциальности.

Кроме того, предусматриваются обязанности обработчика данных, включая оказание помощи контроллеру данных в выполнении его обязанностей, выполнение обязательств контроллера по реагированию на запросы об осуществлении прав потребителей, а также выполнение обязательств контроллера в отношении безопасности обработки персональных данных и уведомления о нарушении безопасности.

О защите прав потребителей в Нью-Йорке

В Сенат штата Нью-Йорк, США проект закона о внесении поправок в общее деловое законодательство в связи с принятием закона о защите потребителей в Интернете ([SB 2998](#))

Устанавливается, что ни один издатель веб-страницы или рекламная сеть, заключившая договор с издателем, не должны собирать персонально идентифицируемую информацию для целей маркетинга предпочтений в Интернете, если потребители не предоставят своего согласия.

Кроме того, ни один издатель не должен собирать любую другую информацию от потребителя, которая не является персонально идентифицируемой информацией, если потребителю не предоставлена возможность отказаться от использования такой информации для интернет-маркетинга.

Предусматривает, что рекламные сети должны размещать на главной странице своего веб-сайта четкое и заметное уведомление о своей политике конфиденциальности и практике сбора и использования данных.

Также издатели веб-страниц должны, в случае заключения договора с рекламной сетью, размещать четкое и заметное уведомление, описывающее сбор и использование информации рекламной сетью.

Уточняется, что если рекламная сеть занимается маркетингом предпочтений в Интернете, политика конфиденциальности как рекламной сети, так и издателя должна описывать возможность отказа от участия в маркетинге.

Определено, что рекламные сети должны прилагать разумные усилия для защиты собранных или зарегистрированных данных от доставки рекламы и отчетности, а также от потери, неправильного использования, изменения, уничтожения или ненадлежащего применения.

Об итальянском руководстве по интерпретации защиты данных

Итальянский орган по защите данных (Garante) опубликовал [Руководство](#) по интерпретации защиты данных.

Руководство предусматривает, что сотрудники должны иметь возможность знать основные параметры, используемые для программирования или обучения автоматизированных систем, включая механизмы оценки эффективности, а также надежность и кибербезопасность систем.

Кроме того, внедрение систем мониторинга в рабочем контексте всегда должно быть предметом предварительной проверки работодателем условий законности, установленных правилами дистанционного управления, а также оценки рисков для проверки их влияния на права и свободы соответствующих лиц.

Также в отношении инструментов машинного обучения, рейтингов и ранжирования, отмечается, что их использование должно быть оценено с точки зрения соразмерности и возможного противоречия принципам защиты данных и национальными отраслевыми правилами, защищающими свободу, достоинство и частную жизнь работников.

О защите персональных данных в Нью-Йорке

В Ассамблею штата Нью-Йорк, США внесен проект закона о внесении изменений в исполнительное законодательство в связи с принятием закона о защите данных в Нью-Йорке ([AB 2587](#)).

Подчеркивается его применение к государственным организациям и подрядчикам, которые заключают контракты на предоставление персональных данных от имени государственных организаций.

Законопроект предусматривает, что физические лица имеют право на информирование, удаление, отсутствие дискриминации, доступ.

Проект закона уточняет, что для соблюдения права на доступность государственные организации и подрядчики должны предоставить определенный способ подачи запросов на достоверную информацию, включая бесплатный телефонный номер и адрес веб-сайта, а если государственные организации имеют веб-сайт, предоставить инструкции о том, как запросить раскрытие и удаление персональных данных.

Указано, что ни одна государственная организация или подрядчик не должны передавать персональные данные какого-либо лица подрядчику или субподрядчику, если только эта информация не имеет решающего значения для целей, ради которых такая государственная организация или подрядчик заключили контракт на их услуги.

Кроме того, отмечается, что государственные организации и подрядчики не должны продавать персональные данные о лицах, которая была передана государственным организациям.

О запрете загрузки TikTok в США

На рассмотрение Конгресса США представлен законопроект, запрещающий загрузку приложения TikTok на устройства американцев ([No TikTok on United States Devices Act](#)).

Предлагается следующее:

- поручить президенту в течение 30 дней использовать Закон о международных чрезвычайных экономических полномочиях (IEEPA) для блокирования и запрета операций с материнской компанией TikTok - ByteDance, предусмотрев жесткие санкции для организаций, пытающихся обойти эти санкции;
- в течение 120 дней после принятия закона обязать директора Национальной разведки представить отчет и проинформировать Конгресс об угрозах национальной безопасности, исходящих от TikTok, включая:

- способность китайского правительства получить доступ к данным американских пользователей;
- способность китайского правительства использовать данные американских пользователей в разведывательных или военных целях, включая слежку, микротаргетинг, глубокие подделки или шантаж;
- продолжающиеся усилия китайского правительства по наблюдению или манипулированию американцами с помощью данных, полученных через TikTok.

О руководящих принципах вторичного использования данных в Саудовской Аравии

Саудовское управление по данным и искусственному интеллекту (SDAIA) начало публичные консультации по [Руководству](#) по вторичному использованию данных.

Руководство устанавливает правовые рамки для обмена данными в целях исследований, разработок и инноваций.

Раздел 2. Зарубежные практические кейсы

Об антимонопольном иске к Google в США

Министерство юстиции США и восемь штатов (Калифорния, Колорадо, Коннектикут, Нью-Джерси, Нью-Йорк, Род-Айленд, Теннесси и Вирджиния) [обратились](#) в суд с иском к компании Google, обвинив компанию в нанесении ущерба конкуренции своим доминирующим положением на рынке онлайн-рекламы.

В иске утверждается, что Google активно и незаконно поддерживала свое доминирование, участвуя в кампании по пресечению конкуренции, поглощая конкурентов и принуждая рекламодателей использовать собственные рекламные продукты.

Об антимонопольном разбирательстве в отношении PayPal в Германии

Немецким антимонопольным регулятором (Bundeskartellamt) возбуждено антимонопольное [дело](#) в отношении европейского подразделения платежной системы PayPal (PayPal (Europe) S.à r.l. et Cie, S.C.A) ввиду возможного ограничения конкуренции и злоупотребления доминирующим положением.

В частности, ведомство изучает условия использования PayPal в Германии, согласно которым онлайн-продавцы не могут предлагать свои товары и услуги по более низкой цене покупателям, выбравшим отличную от PayPal платежную систему с более низкой комиссией. Кроме того, для онлайн-продавцов установлены более высокие сборы за использование иных способов оплаты, кроме PayPal.

О решении по спору между ирландским регулятором и WhatsApp

Европейский совет по защите данных (EDPB) объявил о публикации своего [обязательного решения](#), которое он вынес 5 декабря 2022 года по спору, представленному Комиссией по защите данных (DPC) Ирландии в отношении WhatsApp Ireland Limited.

В частности, EDPB отметил, что DPC поручено внести изменения в свой проект решения в отношении выводов, касающихся законности обработки и принципа справедливости, а также предусмотренных корректирующих мер.

EDPB постановил, что WhatsApp неправомерно полагался на договор в качестве правовой основы для обработки персональных данных. Поэтому ирландскому регулятору поручено добавить нарушение статьи 6(1) GDPR, а также нарушение принципа справедливости в соответствии со статьей 5(1)(a) GDPR.

Кроме того, EDPB постановил, что DPC должен провести расследование операций по обработке WhatsApp, чтобы определить, обрабатывает ли компания:

- специальные категории персональных данных;

- персональные данные для целей поведенческой рекламы, в маркетинговых целях, а также для предоставления метрик третьим лицам и обмена данными с аффилированными компаниями в целях улучшения сервиса.

Кроме того, EDPB просила DPC включить в свое окончательное решение-предписание для WhatsApp привести свои операции по обработке данных в соответствие с GDPR в определенные сроки.

О контроле госорганов за обработчиками данных

Датский орган по защите данных (Datatilsynet) **объявил** о проведении шести плановых проверок государственных органов за обработчиками данных.

Регулятора запросил список обработчиков данных, которым органы власти доверяют чувствительную и конфиденциальную информацию.

В частности, Datatilsynet проверил Департамент Министерства занятости, Совет по персоналу Министерства обороны, Агентство внутренних путешествий, Налоговое управление, Совет по международному найму и интеграции, Датское агентство данных по здравоохранению.

В рамках проверки госорганам были направлены запросы на предоставление следующей информации:

- имеется ли план по надзору за обработчиками данных;
- осуществляли ли госорганы надзор за обработчиками данных;
- как осуществлялось отслеживание за выполнением любых завершённых проверок обработчиков данных.

В пяти из шести инспекций нарушений обнаружено не было.

В ходе проверки Совета по международному найму и интеграции выявлено нарушение Статьи 5(2) Общего регламента по защите данных (GDPR) за его неспособность адекватно контролировать обработку данных, осуществляемую от его имени двумя обработчиками.

О штрафе Ticketer в Эстонии

Инспекция по защите данных (DPI) Эстонии вынесла [предписание](#) Ticketer OÜ о соблюдении требований за нарушение GDPR и Директивы о конфиденциальности и электронных коммуникациях (Директива ePrivacy).

Ранее DPI инициировала расследование в отношении компании Ticketer, чтобы проверить, соответствует ли ее веб-сайт GDPR.

По итогам расследования DPI установила, что уведомление о конфиденциальности Ticketer не соответствует требованиям GDPR.

Кроме того, было выявлено, что Ticketer размещает сторонние файлы cookie на устройстве конечного пользователя, не спрашивая его согласия. В связи с этим DPI пояснила, что, учитывая отсутствие в Эстонии более точных правил относительно использования cookies, необходимо руководствоваться требованиями Директивы ePrivacy.

Таким образом, DPI постановила, что использование сторонних файлов cookie на сайте Ticketer было незаконным, отметив, что данный вид обработки данных разрешен только в случае получения действительного согласия субъекта данных.

DPI предписал компании Ticketer:

- привести свое уведомление о конфиденциальности в соответствие с условиями, изложенными в статьях 13(1) и 13(2) GDPR;
- удалить со своего сайта файлы cookie третьих лиц или получить добровольное согласие физических лиц на использование таких файлов;
- направить в DPI подтверждение об удалении файлов cookie или доказательство добровольного согласия физических лиц на использование файлов cookie.



Об ошибочной кредитной оценке в Норвегии

Норвежский орган по защите данных **вынес решение** о наложении штрафа в размере 200 000 норвежских крон (~) на компанию Recover AS за нарушение GDPR.

Регулятор сообщил, что заявитель был подвергнут кредитной оценке без каких-либо клиентских отношений или иной связи с Recover.

По окончании проведенного расследования Datatilsynet установил, что компания Recover провела кредитную оценку заявителя из-за ошибки. Recover должна была оценить другого нового клиента, однако перепутала имя нового клиента с именем заявителя, направившего жалобу регулятору.

Таким образом, определено, что компания обрабатывала данные заявителя без законного основания, нарушив статью 6(1)(f) GDPR. Более того, Datatilsynet определил, что компания Recover могла бы избежать данной ошибки путем более тщательной оценки кредитоспособности.

Помимо оплаты штрафа компания обязана улучшить внутренний контроль и процедуры оценки кредитоспособности.

О размещении фотографий пациентов на странице больницы в соцсетях

Датский орган по защите данных (Datatilsynet) **объявил** о начале расследования в отношении региона Центральная Ютландия.

Расследование инициировано в связи с использованием Instagram больницей Орхусского университета, где больница размещала изображения пациентов на своем аккаунте таким образом, что это позволило получить медицинскую информацию о пациентах.

В связи с этим Datatilsynet направил в регион ряд вопросов по использованию Instagram, включая правовую основу, прозрачность, оценку рисков и анализ воздействия.

О раскрытии персональных данных Meta без согласия

Управление комиссара по защите частной жизни (ОПС) Канады [установило](#), что компания Home Depot of Canada Inc. нарушила Закон о защите персональных данных и электронных документов 2000 года (PIPEDA).

Регулятору была направлена жалоба, в которой утверждалось, что Home Depot раскрыла персональные данные заявителя компании Meta Platforms, Inc. (*запрещена в РФ*) без его ведома и согласия.

Кроме того, заявитель утверждал, что, удалив свой аккаунт в Facebook, он узнал, что в Meta хранится информация о большинстве его покупок, совершенных в магазине Home Depot.

По итогам расследования ОПС пришло к выводу, что Home Depot не смогла обеспечить получение согласия на свою практику обмена информацией о клиентах с Meta для целей Home Depot и Meta.

ОПС дало ряд рекомендаций Home Depot, чтобы привести ее в соответствие с PIPEDA, а именно:

- не раскрывать компании Meta персональные данные клиентов, запрашивающих электронную квитанцию, до тех пор, пока она не примет меры по обеспечению действительного согласия;
- внедрить меры по получению явного, предварительного согласия, если компания решит возобновить практику передачи данных о клиентах компании Meta через офлайн-конверсии;
- внести изменения в сообщения о конфиденциальности, чтобы обеспечить прозрачное информирование и значимое согласие на эту практику, путем предоставления ключевой информации заранее, в момент запроса клиентами электронной квитанции, включая:
 - какая информация будет передана компании Meta;

- что она будет использоваться для оценки эффективности рекламных кампаний Home Depot по продвижению услуг Meta на Facebook;
- что информация также будет использоваться Facebook для собственных целей, включая таргетинг;
- что у клиентов есть возможность отозвать согласие в более позднее время;
- включение в заявление о конфиденциальности более подробного объяснения данной практики и способов отзыва согласия.

В ответ на рекомендации Home Depot прекратила использование инструмента конверсии Meta в октябре 2022 года, подтвердив, что если она решит возобновить использование инструмента конверсии, то выполнит рекомендации, изложенные выше.

О доступе к аккаунтам пользователей Twitter

Конгресс США получил жалобу информатора, в которой утверждается о дополнительных проблемах с конфиденциальностью и безопасностью данных в Twitter до и после приобретения компании Илоном Маском.

В жалобе утверждается, что около 4.000 сотрудников Twitter имели доступ к настройкам, которые позволяли полностью завладеть любым частным аккаунтом без согласия пользователя.

О запрете TikTok в ЕС

Европейский комиссар по внутреннему рынку объявил о запрете платформы TikTok в ЕС 1 сентября, если она не примет меры по соблюдению Закона о цифровых услугах (Digital Services Act, [DSA](#)).

Согласно DSA, который компании должны выполнить до 1 сентября, крупные интернет-платформы должны будут соблюдать длинный список правил модерации

контента, либо подвергнуться штрафам в размере до 6% от годового дохода, либо быть запрещенными в странах ЕС.

ИССЛЕДОВАНИЯ, ЭКСПЕРТНЫЕ МНЕНИЯ, ПОЗИЦИИ ГОСУДАРСТВЕННЫХ ОРГАНОВ, ОРГАНИЗАЦИЙ

О блокировке запрещённого контента

Роскомнадзор опубликовал статистику ограничения доступа к некоторым видам противоправной информации.

Так, за 2022 год Роскомнадзор совместно с профильными ведомствами заблокировал либо удалил:

- 70 тысяч материалов, сайтов или их отдельных страниц с **порнографическим контентом** с участием несовершеннолетних, что на 20% больше, чем в 2021 году (58,4 тысячи).
- 98 тысяч материалов, сайтов и их отдельных страниц с информацией о распространении **наркотиков**,
- более 61 тысячи материалов о способах совершения **самоубийства** и с призывами к нему.

В 2017 году РКН запустил собственный мониторинг информационного пространства для выявления детской порнографии и суицидального контента. За 5 лет ведомство зафиксировало:

- 399,8 тысяч нарушений в сфере детской порнографии: 240 тысяч из них нашла служба мониторинга, остальные 159,8 тысячи материалов прислали граждане.
- 493 тысячи материалов в сфере суицидального контента: 402 тысячи из них нашла служба мониторинга, а пятую часть – 91 тысячу – удалось выявить благодаря



обращениям пользователей.

С 2019 года Роскомнадзор самостоятельно отслеживает материалы о наркотиках. За 3 года ведомство пресекло 580 тысяч нарушений: 237 тысяч из них нашла служба мониторинга, остальные 343 тысячи материалов прислали граждане.

В 2022 году в Роскомнадзор **поступило** 12,5 тысяч определений Мосгорсуда и 38 тысяч заявлений правообладателей о защите авторских прав в Интернете

Зарубежные и российские правообладатели стали чаще обращаться в Роскомнадзор за защитой своих прав. По сравнению с 2021 годом количество заявлений выросло на 18%, а предварительные обеспечительные меры были приняты в отношении почти 350 тысяч сайтов с пиратским контентом, что на 17% больше, чем годом ранее.

85% владельцев сайтов самостоятельно удалили нелегальные копии. Доступ к 41 тысяче сайтов был ограничен операторами связи, так как пиратский контент не был удалён вовремя.

В 2022 году на основании 13,5 тысяч определений Мосгорсуда об отмене предварительных обеспечительных мер было разблокировано 38,6 тысячи ресурсов.

Кроме того, по **данным** Генерального прокурора Российской Федерации, надзорное ведомство в 2022 году направило в Роскомнадзор свыше 1,7 тысячи требований о внесудебном ограничении доступа к информации в Интернете, в 2021 году было направлено 650.

На основании указанных требований Роскомнадзор только в 2022 году заблокировал либо удалил публикации более чем со 190 тысяч Интернет-страниц, в том числе распространявших «фейки» о СВО (таких материалов было 125 тысяч).

О маркетплейсах

Tinkoff представил **отчёт** о потребительской и бизнес-активности на маркетплейсах по итогам 2022 года.

Отмечается следующее:

- на 43% выросло количество покупок россиян на маркетплейсах по отношению к 2021 году;
 - на маркетплейсы приходится 8,5% от общей суммы всех трат (онлайн и офлайн), в полтора раза больше, чем годом ранее;
 - ноябрь по-прежнему остается самым активным месяцем, на него пришлось 12% всех онлайн-продаж и больше всего регистраций продавцов-новичков;
 - в 1,5 раза выросло число продавцов в четвертом квартале 2022 года;
 - 60% продавцов торгуют на Wildberries, это самая популярная площадка в России.
- аналитики изучили данные по тратам клиентов Тинькофф: 28 млн физических лиц и более 180 000 предпринимателей, работающих в сфере электронной коммерции.

О темных паттернах в США

Форум Future of Privacy Forum (FPF) опубликовал [пост](#) о текущей позиции регуляторов США в отношении темных паттернов.

В частности, FPF выделил основные тенденции и выводы, объясняющие наиболее значимые правила, которые касаются манипулятивного дизайна в контексте защиты данных в США, а также обсудил возможности и проблемы применения правил анти-манипулятивного дизайна к конкретным секторам бизнеса или практикам.

Отмечается, что большинство законов штатов, направленных на ограничение или запрет использования манипулятивного дизайна в Интернете в США, основаны на предложенном законе Deceptive Experiences To Online Users Reduction Act (DETOUR).



Институт развития
интернета

iri.rf