



Институт развития
интернета

Еженедельный правовой дайджест
Интернет и информационные
технологии
Выпуск № 139
07.04.2023

Оглавление

Российская Федерация	3
Раздел 1. Законы и законопроекты	3
Раздел 2. Акты и проекты актов Президента	4
Раздел 3. Акты и проекты актов Правительства	5
Раздел 4. Практические кейсы	6
Зарубежные страны	7
Раздел 1. Зарубежное нормотворчество.....	7
Раздел 2. Зарубежные практические кейсы.....	8
Исследования, экспертные мнения, позиции государственных органов, организаций	13



РОССИЙСКАЯ ФЕДЕРАЦИЯ

Раздел 1. Законы и законопроекты

Об информационной поддержке НКО

Государственной Думой принят во втором чтении 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.

Об административной ответственности за неисполнение требований к СОРМ

Государственной Думой принят в первом чтении законопроект № [297967-8](#) «О внесении изменений в статью 13.46 Кодекса Российской Федерации об административных правонарушениях».

Несоблюдение оператором связи требований к сетям и средствам связи, используемым для проведения оперативно-розыскной деятельности, повлечёт наложение административного штрафа в размере до 0,3% от годовой выручки, но не менее 1 миллиона рублей.

Об экспериментальных правовых режимах

Минэкономразвития России опубликовало [законопроект](#) «О внесении изменений в Федеральный закон «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации»».

Совершенствуется процедура рассмотрения инициативного предложения и установления экспериментальных правовых режимов (ЭПР): сокращаются сроки установления ЭПР, конкретизируются перечни прилагаемых к инициативному предложению документов, а также требования к инициаторам.

Регламентируется защита установленных ЭПР в случае, если в течение срока его действия вносятся изменения в законодательство, препятствующие такому ЭПР.

Кроме того, предусматриваются механизмы защиты результатов интеллектуальной деятельности, созданных с использованием технологии искусственного интеллекта при реализации ЭПР.

Раздел 2. Акты и проекты актов Президента

О платформе ГосТех

Опубликован [указ](#) Президента Российской Федерации от 31 марта 2023 года № 231 «О создании, развитии и эксплуатации государственных информационных систем с использованием единой цифровой платформы Российской Федерации «ГосТех»».

Создание, развитие и эксплуатация государственных информационных систем с использованием платформы «ГосТех» осуществляется:

- с 1 апреля 2023 года – в отношении федеральных информационных систем;
- с 1 января 2024 года – в отношении региональных информационных систем.

Использование платформы «ГосТех» будет осуществляться по результатам оценки экономической и технологической целесообразности, проведенной в соответствии с методическими рекомендациями и планом, утвержденными в определенном Правительством Российской Федерации порядке.

Раздел 3. Акты и проекты актов Правительства

Об идентификации болельщиков

Минцифры России опубликовало [проект постановления](#) Правительства Российской Федерации «О внесении изменений в постановление Правительства Российской Федерации от 25 июня 2022 г. № 1140».

Упрощается процедура получения персонифицированной карты болельщиков (Fan ID) для инвалидов, пенсионеров и детей.

Дети, не достигшие возраста 14 лет, смогут пройти идентификацию удаленно с использованием Единого портала государственных и муниципальных услуг без необходимости посещения многофункциональных центров.

Для пенсионеров и инвалидов в уполномоченных на выдачу Fan ID организациях будут оборудованы отдельные окна (кабинеты) для первоочередного обслуживания.

Инвалиды также наделяются правом прохождения идентификации с помощью лиц, ответственных за направление групповых заявлений на оформление Fan ID.

О подтверждении страны происхождения телеком-оборудования

Минпромторг России опубликовал [проект постановления](#) Правительства Российской Федерации «О внесении изменений в некоторые акты Правительства Российской Федерации».

Подтверждать производство телеком-оборудования на территории Российской Федерации предлагается по общим правилам для промышленной продукции: наличие специального инвестиционного контракта, наличие оценки или экспертизы Торгово-промышленной палаты Российской Федерации, наличие сертификата о происхождении товара.

Раздел 4. Практические кейсы

О маркетплейсах

Члены Общественного совета при ФАС России **обсудили** вопрос регулирования взаимодействия маркетплейсов и их контрагентов.

Участники заседания пришли к выводу, что целесообразно вывести цифровые торговые площадки из-под действия моратория на проверки аккредитованных ИТ-компаний.

Представители ФАС России отметили, что регулятор проведет анализ рынка цифровых торговых площадок, а также пригласили представителей ИТ-компаний на заседание экспертного совета для совместной проработки предложений по регулированию деятельности маркетплейсов.

О штрафе за удаление «Википедией» противоправного контента

Мировой судья судебного участка № 422 Таганского района города Москвы вынес постановление по делу № [05-0360/422/2023](#) о привлечении компании Wikimedia Foundation, Inc к административной ответственности за удаление противоправного контента по требованию Роскомнадзора.

По части 2 статьи 13.41 Кодекса Российской Федерации об административных правонарушениях компании назначен штраф в размере 800 000 рублей.



ЗАРУБЕЖНЫЕ СТРАНЫ

Раздел 1. Зарубежное нормотворчество

Об уведомлении о нарушении персональных данных в ЕС

Европейский совет по защите данных опубликовал обновленное [Руководство](#) по уведомлению о нарушении персональных данных в соответствии с Общим регламентом ЕС по защите данных.

Руководство уточняет требования к уведомлению о нарушениях персональных данных в учреждениях, не входящих в ЕС.

Указано, что о нарушении данных необходимо уведомлять каждый надзорный орган государства-члена ЕС, где проживают затрагиваемые субъекты данных.

О цифровом доверии

Национальное управление по защите персональных данных Перу опубликовало проект указа, который утверждает [«Рамки цифрового доверия»](#).

Под «Рамками цифрового доверия» понимается набор принципов, моделей, процессов, которые позволяют обеспечить и поддерживать доверие в цифровой среде.

Целями указа являются 1) обеспечение доверия населения при взаимодействии с цифровыми услугами, предоставляемыми государственными учреждениями; 2) укрепление цифровой безопасности.

«Рамки цифрового доверия» определяются следующими принципами:

- кибердипломатия;
- взаимодействие и сотрудничество;
- управление рисками;
- честность;

- конфиденциальность и безопасность при проектировании;
- цифровая устойчивость и восстановление;
- уважение прав человека;
- подотчетность;
- прозрачность.

Раздел 2. Зарубежные практические кейсы

О расследовании в отношении ChatGPT в Канаде

Офис Комиссара по защите частной жизни Канады [инициировал](#) расследование против в отношении компании OpenAI после получения от граждан жалоб о сборе, использовании и раскрытии личной информации сервисом ChatGPT без согласия пользователей.

Регулятор пояснил, что процесс изучения материалов находится в активной фазе, а вопросы, связанные с использованием технологии ИИ и их влияния на конфиденциальность граждан, являются в настоящее время приоритетными для госведомства.

В случае выявления нарушений со стороны OpenAI против компании могут быть применены санкции административного и технического уровня.

О соглашении Amazon с властями Индии

Министерство информации и телерадиовещания Индии и компания Amazon подписали соглашение о продвижении государственного контента.

Соглашение предусматривает сотрудничество с федеральным правительством Индии в области трансляции фильмов и телешоу из государственных студий, а также предоставляет стажировки студентам государственных киноинститутов.

Кроме того, индийское подразделение Amazon предоставит специальную функцию для увеличения популярности книг и журналов издательского подразделения министерства.

О штрафе Google по делу о защите частной жизни

Судья окружного суда США Северного округа Калифорнии обязала компанию Google выплатить штраф в размере 79 000 долларов США за невыполнение решения по групповому иску о защите персональных данных.

Решение вынесено в связи коллективным иском, в котором утверждалось, что компания незаконно отслеживает пользователей через режим «инкогнито» в Chrome.

О необходимости доказать моральный ущерб при утечке данных

Верховный суд Бразилии постановил, что сам факт нарушения персональных данных не порождает автоматически обязанности компенсировать моральный ущерб.

Указывается на необходимость доказать моральный ущерб, понесенный пострадавшей стороной, чтобы иметь возможность применить соответствующую компенсацию.

В постановлении указано, что «утечка персональных данных несмотря на то, что является нежелательным сбоем в обработке данных физического лица юридическим лицом, сама по себе не способна породить моральный ущерб, подлежащий возмещению. Поскольку моральный вред не презюмируется, необходимо, чтобы владелец данных доказал возможный ущерб, возникший в результате обнародования такой информации».

О штрафе TikTok в Великобритании

Управление комиссара по информации (ICO) Великобритании [оштрафовало](#) компанию TikTok на 12,7 млн фунтов стерлингов (~1,3 млрд рублей) за нарушение Общего положения о защите данных Великобритании (UK GDPR).

Хотя в условиях TikTok указано, что детям до 13 лет запрещено создавать учетные записи, по оценкам ICO, в 2020 году на платформе находилось более 1 миллиона британских детей до 13 лет.

ICO также заявило, что TikTok использовал персональные данные детей младше 13 лет без согласия родителей и не принял достаточных мер для удаления несовершеннолетних детей с платформы.

О жалобе на OpenAI в США

На компанию OpenAI подана [жалоба](#) в Федеральную торговую комиссию (FTC) США.

Жалоба подана некоммерческой исследовательской группой Center for AI and Digital Policy (CAIDP), которая требует проведения расследования в отношении OpenAI, а также требует приостановить коммерческое развертывание компанией больших языковых моделей, включая последнюю версию ChatGPT.

OpenAI вменяется нарушение раздела 5 закона о FTC, который запрещает нечестные и обманчивые методы ведения бизнеса.

CAIDP утверждает, что ChatGPT не соответствует стандартам агентства, согласно которым ИИ должен быть прозрачным, объяснимым, справедливым, научно обоснованным и подотчетным.

CAIDP требует от FTC, чтобы OpenAI создала способ независимой оценки продуктов GPT перед их внедрением в будущем.

Также требуется, чтобы FTC создала публичную систему отчетности об инцидентах для GPT-4, подобную той, которая используется для [отчетности](#) о потребительском мошенничестве.

Кроме того, агентству рекомендуется разработать правила для создания стандартов для продуктов генеративного ИИ.

О штрафе Samsung Securities Co. Ltd

Комиссия по защите персональных данных (PIPC) Республики Корея [наложила штраф](#) в размере 101,6 миллиона KRW (~6,3 млн рублей) на компанию Samsung Securities Co. Ltd. за нарушение Закона о защите персональных данных 2011 года (PIPA).

Регулятором было установлено, что Samsung Securities нарушила статью 29 PIPA, поскольку не реализовала меры безопасности для компенсации уязвимости системы, связанной с ошибкой настройки веб-сервера, мешающей составлению списка каталогов.

Кроме того, PIPC постановила, что Samsung Securities пренебрегла контролем доступа, не задействовав процедуры аутентификации при доступе к странице администратора, что привело к утечке персональных данных более 50.000 пользователей.

Об использовании ChatGPT и аналогов в Швейцарии

Федеральный уполномоченный по защите данных и информации (FDPIC) Швейцарии [опубликовал](#) заявление об использовании ChatGPT и аналогичных приложений с использованием искусственного интеллекта.

В частности, FDPIC подчеркнул, что обработка персональных данных с помощью таких новых технологий связана с рисками для частной жизни и информационного самоопределения.

Более конкретно, FDPIC отметил, что советует пользователям проверять цели обработки персональных данных, прежде чем вводить текст или загружать изображения, и что организации должны обеспечить соблюдение требований по защите данных при использовании приложений с ИИ.

Это включает в себя, как отметил FDPIC, обеспечение прозрачного и понятного информирования пользователей о том, какие данные обрабатываются, с какой целью и каким образом.

О штрафе McDonald's в Корее

Комиссия по защите личной информации (PIPC) Республики Корея **наложила штрафы** на общую сумму 706,66 млн. KRW (~44 млн рублей) на компанию McDonald's Korea Limited за нарушение статей Закона о защите персональных данных 2011 года.

PIPC отметила, что McDonald's не обеспечила надлежащий контроль доступа, разрешив доступ к резервным файлам, содержащим персональные данные пользователей, через протокол Server Message Block, что привело к утечке персональных данных почти 5 млн пользователей в результате взлома систем McDonald's.

Кроме того, PIPC установила, что McDonald's не удалил персональные данные более 750.000 пользователей по истечении срока хранения, а также несвоевременно уведомил об утечке персональных данных.

ИССЛЕДОВАНИЯ, ЭКСПЕРТНЫЕ МНЕНИЯ, ПОЗИЦИИ ГОСУДАРСТВЕННЫХ ОРГАНОВ, ОРГАНИЗАЦИЙ

Об отношении к нейросетям

Всероссийский центр изучения общественного мнения (ВЦИОМ) опубликовал [данные](#) социологического опроса об отношении россиян к нейросетям.

В общей сложности о нейросетях сегодня знают 63% россиян, но 51% только что-то слышали о них, а хорошо разбираются в нейросетях, по собственным оценкам, 12% наших сограждан. Впервые услышали о нейросетях в ходе опроса 37%.

Исследование показало, что в обществе преобладает нейтрально-положительное отношение к технологиям нейросетей: 40% относятся к ним нейтрально, 35% – положительно. Каждый пятый россиянин воспринимает подобные технологии отрицательно (20%).

Вероятность того, что в ближайшие 50 лет такие технологии, как нейросети, могут выйти из-под контроля человека и произойдет так называемое восстание машин, оценивается россиянами скорее невысоко: 59% не верят, что подобное случится; каждый третий – верит (30%).

О киберрисках языковых моделей

Национальный центр кибербезопасности (NCSC) Великобритании изучил вопросы кибербезопасности, связанные с ChatGPT и большими языковыми моделями (LLM).

В [пресс-релизе](#) NCSC заявил, что запуск ChatGPT подтолкнул конкурентов к разработке и внедрению собственных LLM и чат-ботов с искусственным



интеллектом, которые, будучи новыми технологиями, связаны с рисками безопасности.

В связи с этим NCSC отметила, что поскольку алгоритмы LLM обучаются на большом количестве текстовых данных, обычно взятых из открытого интернета, невозможно отфильтровать весь оскорбительный или неточный контент в момент сбора. Соответственно, сгенерированный контент может быть неточным и предвзятым.

NCSC подчеркнула, что в отношении киберугроз LLM могут помочь злоумышленникам написать незнакомые им ранее методы борьбы с вредоносным ПО и составить более убедительные фишинговые письма.

О британском руководстве для разработчиков и пользователей генеративного ИИ

Управление комиссара по информации (ICO) Великобритании выпустило [пресс-релиз](#), где указаны восемь вопросов, которые разработчики и пользователи должны задавать при использовании генеративного ИИ.

ICO подчеркнуло риски, связанные с использованием таких технологий, отметив, что организации, разрабатывающие или использующие генеративный ИИ, должны с самого начала учитывать свои обязательства по защите данных, принимая в качестве обязательной практики подход «Защита данных по проекту и по умолчанию» (privacy by design / privacy by default).

ICO отметило, что закон о защите данных (UK GDPR) применяется, когда организации обрабатывают персональные данные из общедоступных источников, и что организации, разрабатывающие или использующие генеративный ИИ, который обрабатывает персональные данные, должны иметь в виду следующие аспекты:

- Какова законная основа для обработки персональных данных?
- Является ли организация контролером, совместным контролером или

обработчиком?

- Подготовила ли организация оценку воздействия на защиту данных (DPIA) перед обработкой персональных данных?

- Как организация обеспечивает прозрачность?
- Как организация будет снижать риски безопасности?
- Как организация будет ограничивать ненужную обработку?
- Как организация будет выполнять запросы на соблюдение индивидуальных прав?

- Будет ли организация использовать генеративный ИИ для принятия исключительно автоматизированных решений?





Институт развития
интернета

iri.rf