Институт развития интернета

Еженедельный правовой дайджест

Интернет и информационные технологии

Выпуск № 141

21.04.2023

Москва 2023

Оглавление

119017, г. Москва, Кадашёвская наб., д.6/1/2, стр. 1
+7 (945) 109 00 80
info@iri.center
ири.рф

ОГРН: 1147799015231
ИНН: 7709473987
КПП: 770601001

РОССИЙСКАЯ ФЕДЕРАЦИЯ

Раздел 1. Законы и законопроекты

Об информационной поддержке НКО

Подписан Федеральный закон от 14 апреля 2023 года № 119-ФЗ «О внесении изменений в статью 31-1 Федерального закона «О некоммерческих организациях» (законопроект № 281856-8).

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.

Закон вступил в силу с 14 июля 2023 года.

О цифровизации воинского учёта

Подписан Федеральный закон от 14 апреля 2023 года № 127-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» (законопроект № 361804-7).

В числе прочего предусматривается создание Минцифры России ФГИС «Реестр воинского учёта», оператором которого будет Минобороны России.

В реестр будут включаться следующие сведения:

- ФИО, дата рождения, пол;
- паспортные данные;
- СНИЛС;

- ИНН;
- место жительства/пребывания;
- сведения об иностранном гражданстве или виде на жительство;
- код и наименование военкомата, в котором гражданин состоит на учёте;
- сведения о постановке на воинский учёт/снятии с воинского учёта;
- сведения о факте выдачи документа воинского учета;
- сведения о трудовой деятельности и об образовании;
- сведения о состоянии здоровья;
- сведения об отсрочке;
- иные определяемые Правительством Российской Федерации сведения.

Реестр будет формироваться военкоматами на основании сведений, предоставляемых в том числе органами МВД России, ФНС России, ЦИК России, судами, медицинскими и образовательными организациями.

Также предусматривается направление повесток в электронном виде через личный кабинет на Едином портале государственных услуг.

На основании реестра воинского учёта в автоматическом режиме будет формироваться общедоступный реестр повесток, информация из которого будет предоставляться посредством личного кабинета в таком реестре, личного кабинета на Едином портале государственных услуг, а также при личном обращении в многофункциональный центр.

Повестка может считаться вручённой по истечении семи дней с даты ее размещения в реестре повесток.

Закон вступил в силу с 14 апреля 2023 года.

Раздел 2. Акты и проекты актов Правительства

О государственной единой облачной платформе

Минцфиры России опубликовало проект постановления Правительства Российской Федерации «Об утверждении Положения о государственной единой облачной платформе».

Государственная единая облачная платформа ГосОблако должна будет обеспечить предоставление унифицированных облачных услуг с применением отказоустойчивой инфраструктуры с возможностью масштабирования, разделения использования инфраструктуры и перераспределения вычислительных ресурсов.

ГосОблако обеспечивает возможность предоставления потребителям следующих групп услуг:

а) предоставление вычислительных ресурсов и ресурсов хранения данных;

б) конфигурирование виртуальных машин и их сопровождение, предоставление балансировки нагрузки;

в) предоставление объектной системы хранения данных;

г) предоставление системы управления резервным копированием;

д) предоставление управляемых кластеров контейнеров;

е) предоставление программной инфраструктуры витрин данных;

ж) предоставление системного программного обеспечения;

з) предоставление каналов связи;

и) предоставление публичных IPv4-адресов;

к) обеспечение информационной безопасности;

л) предоставление комплектов средств защиты информации;

м) предоставление аппаратных комплексов, в том числе вычислительных ресурсов для создания вычислительной инфраструктуры и инфраструктуры хранения данных;

н) предоставление программно-аппаратных комплексов;

о) предоставление защищенного размещения средств защиты информации, в том числе криптографического оборудования;

п) иные группы услуг, необходимые потребителям, предоставление которых возможно обеспечить в рамках ГосОблака.

Раздел 3. Ведомственные акты и проекты ведомственных актов

О критериях запрещённой инофрмации

Минюст России зарегистрировал:

- приказ МВД России от 3 марта 2023 года № 114 «Об утверждении критериев оценки информации о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ и их прекурсоров, новых потенциально опасных психоактивных веществ, местах их приобретения, способах и местах культивирования наркосодержащих растений, необходимой для принятия Министерством внутренних дел Российской Федерации решений, являющихся основаниями для включения доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено, в единую автоматизированную информационную систему «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в

информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено»;

- приказ ФНС России от 13 марта 2023 года № ЕД-7-2/162@ «Об утверждении Критериев оценки информации, необходимой для принятия Федеральной налоговой службой решений, являющихся основаниями для включения доменных имен и (или) указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет», а также сетевых адресов в единую автоматизированную информационную систему «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено»;

- приказ Роспотребнадзора от 27 февраля 2023 года № 79 «Об утверждении критериев оценки информации, необходимой для принятия Федеральной службой по надзору в сфере защиты прав потребителей и благополучия человека решений, являющихся основаниями для включения доменных имен и (или) указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет», а также сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», в единую автоматизированную информационную систему «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено», в отношении информации о способах совершения самоубийства, а также призывов к совершению самоубийства»;

- приказ Роскомнадзора от 27 февраля 2023 года № 25 «Об утверждении

Критериев оценки материалов и (или) информации, необходимых для принятия Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций решений, являющихся основаниями для включения доменных имен и (или) указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет», а также сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», в единую автоматизированную информационную систему «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено».

Определены критерии признания запрещённым следующего контента:

- пронаркотический контент;
- нелегальные азартные игры (включая возможность денежных переводов их организаторам);
- суицидальный контент;
- детская порнография;
- ЛГБТ-пропаганда.

О банке данных экстремистских материалов

Зарегистрирован приказ Минюста России от 19 апреля 2023 года № 69 «Об утверждении порядка формирования, ведения и использования банка данных экстремистских материалов».

Банк данных экстремистских материалов будет вестись Минюстом России и должен будет содержать:

- порядковый номер записи в федеральном списке экстремистских

материалов;

- наименование, реквизиты и иные индивидуализирующие признаки экстремистского материала (в соответствии с резолютивной частью судебного акта);
- цифровую копию судебного акта о признании информационного материала экстремистским;
- реквизиты судебного акта о признании информационного материала экстремистским;
- цифровую копию правового акта Минюста России о включении сведений об экстремистском материале в федеральный список экстремистских материалов;
- информацию о типе материала;
- цифровую копию экстремистского материала;
- цифровую копию экспертного заключения (при наличии).

Сведения из банка данных будут предоставляться:

- Минюсту России и его подведомственным организациям;
- МВД России;
- Генеральной прокуратуре Российской Федерации;
- Следственному комитету Российской Федерации;
- ФСБ России;
- Роскомнадзору;
- Росфинмониторингу;
- ФТС России;
- Росгвардии;
- Верховному Суду Российской Федерации.

119017, г. Москва, Кадашёвская наб., д.6/1/2, стр. 1
+7 (945) 109 00 80
info@iri.center
ири.рф
ОГРН: 1147799015231
ИНН: 7709473987
КПП: 770601001

Раздел 4. Практические кейсы

О штрафе за неудаление «Википедией» противоправного контента

Мировой судья судебного участка № 422 Таганского района города Москвы вынес постановления о привлечении к административной ответственности по части 2 статьи 13.41 КоАП РФ за неудаление противоправного контента по требованию Роскомнадзора:

- компанию Wikimedia Foundation, Inc по делам № 05-0369/422/2023 на 800 тысяч рублей и № 05-0474/422/2023 на 1 500 000 рублей;
- компанию Twitch Interactive, Inc по делу № 05-0475/422/2023 на 4 000 000 рублей.

О штрафе за «Ростелекома» за утечку данных

Мировой судья судебного участка №7 г. Санкт-Петербурга вынес постановление по делу № 5-145/2023-7 о привлечении компании ПАО «Ростелеком» к административной ответственности за утечку персональных данных клиентов и работников.

По части 1 статьи 13.11 Кодекса Российской Федерации об административных правонарушениях компании назначен штраф в размере 60 000 рублей.

О нарушении Wildberries прав потребителей

Подольский городской суд Московской области вынес решение по делу № 2-2962/2023 по иску Сергиево-Посадского территориального отдела Управления Роспотребнадзора по Московской области к ООО «Вайлдберриз».

Суд признал противоправными действия компании в отношении неопределенного круга потребителей, выраженные в том, что при осуществлении

дистанционной продажи товаров она взимает/удерживает денежные средства с потребителей за возврат товаров ненадлежащего качества.

Суд обязал компанию осуществлять возврат товара ненадлежащего качества от потребителей за счёт продавца, а также довести содержание принятого решения до сведения потребителей через электронные и печатные средства массовой информации.

ЗАРУБЕЖНЫЕ СТРАНЫ

Раздел 1. Зарубежное нормотворчество

О запрете TikTok в Монтане

Палата представителей штата Монтана, США проголосовала за окончательное одобрение законопроекта о запрете TikTok на всей территории штата.

Если законопроект будет подписан губернатором, он вступит в силу 1 января 2024 года и потребует от магазинов мобильных приложений сделать видеоприложение недоступным для пользователей из Монтаны.

В Монтане уже запрещено использование приложения на государственных устройствах и в университетах штата.

Об ирландских руководствах по правам детей на защиту информации

Комиссия по защите данных Ирландии опубликовала четыре руководства для родителей по правам детей на защиту данных в соответствии с Общим регламентом ЕС по защите данных (GDPR).

В руководствах изложены основы прав детей на защиту данных, описаны случаи, когда может потребоваться согласие родителей на обработку данных детей,

советы о том, как родители могут защитить данные своих детей, и ограничения в осуществлении прав детей на защиту данных.

О регулировании криптоактивов в ЕС

Европейский парламент проголосовал за принятие Регламента о рынках криптоактивов (Markets in Crypto Assets, MiCA).

Будучи регламентом, MiCA будет напрямую применяться во всех государствах-членах ЕС без необходимости переноса на национальный уровень.

Криптоактив, согласно MiCA, определяется как любое цифровое представление стоимости или права, которое может быть передано и сохранено электронным способом, с использованием технологии распределенной бухгалтерской книги или аналогичной технологии.

MiCA вводит 3 подкатегории криптоактивов, а именно:

- токены с привязкой к активам (ARTs);
- токены электронных денег (EMTs);
- другие криптоактивы (общая категория для токенов, которые не подпадают под первые две, например, биткоин).

MiCA устанавливает три различных, но взаимосвязанных режима регулирования, а именно: 1) режим для эмитентов стабильных монет (ARTs и EMTs), 2) режим для эмитентов нестабильных монет (других криптоактивов) и 3) режим для организаций, предоставляющих услуги в отношении криптоактивов, которые сокращенно называются поставщиками услуг в области криптоактивов или CASPs.

Основное требование MiCA заключается в том, что эмитенты всех трех типов криптоактивов должны опубликовать информацию об эмитенте, характеристиках криптоактивов, сроках реализации проекта, рисках и других вопросах.

MiCA вводит 10 категорий услуг с криптоактивами для которых необхоодимо получение лицензии для CASP. Лицензия требуется для 1) лиц, расположенных или учрежденных в ЕС, и 2) лиц, учрежденных за пределами ЕС, таких как Великобритания и Швейцария, ориентированных на клиентов в ЕС.

Регламент направлен на утверждение Совета ЕС, после чего он будет опубликован в официальном журнале ЕС и вступит в силу через 20 дней.

MiCA будет применяться в двух частях. Первая часть, касающаяся стабильных монет, должна вступить в силу через 12 месяцев (2 квартал 2024 года), а вторая часть, касающаяся CASP, – через 18 месяцев (4 квартал 2024 года).

Европейское банковское управление и Европейское управление по рынкам ценных бумаг разработают технические стандарты и руководства, дополняющие MiCA.

О киберсолидарности в ЕС

Европейская комиссия опубликовала проект Регламента о киберсолидарности ЕС, который направлен на укрепление потенциала кибербезопасности в ЕС.

В частности, Комиссия отметила, что предлагаемый Закон устанавливает правила для лучшего обнаружения, подготовки и реагирования на значительные или масштабные инциденты кибербезопасности путем создания Европейского щита кибербезопасности (the Shield).

Щит будет представлять собой общеевропейскую инфраструктуру, состоящую из национальных и трансграничных операционных центров безопасности по всему ЕС, а также всеобъемлющего механизма чрезвычайных ситуаций в киберпространстве для повышения готовности и расширения возможностей реагирования на инциденты в ЕС.

Кроме того, предлагаемый закон предусматривает создание Механизма обзора инцидентов кибербезопасности для повышения устойчивости ЕС путем

рассмотрения и оценки значительных или крупномасштабных инцидентов кибербезопасности после того, как они произошли, и, в случае необходимости, выдачи рекомендаций по улучшению киберустойчивости ЕС.

О защите несовершеннолетних от распространения вредных материалов

В штате Арканзас, США принят Закон о защите несовершеннолетних от распространения вредных материалов.

Закон устанавливает, что коммерческие организации должны использовать разумный метод проверки возраста, прежде чем разрешить доступ к веб-сайту, который содержит значительную часть материалов, вредных для несовершеннолетних.

Разумные методы проверки возраста включают предоставление:

- оцифрованного удостоверения личности, включая цифровую копию водительских прав;
- удостоверение личности, выданное правительством;
- любой коммерчески обоснованный метод проверки возраста, который имеет второй уровень гарантии идентичности (в соответствии с уровнями гарантий Всемирного банка).

Кроме того, Закон определяет, что коммерческая организация, которая сознательно и преднамеренно публикует или распространяет в Интернете материалы, наносящие вред несовершеннолетним, с веб-сайта, содержащего значительную часть материалов, наносящих вред несовершеннолетним, несет ответственность, если она не провела разумную проверку возраста человека.

Также Закон предусматривает, что коммерческая организация, нарушившая Закон, несет ответственность перед физическим лицом за ущерб, возникший в результате доступа несовершеннолетнего к вредоносному материалу, включая судебные издержки и гонорары адвокатов по решению суда.

Раздел 2. Зарубежные практические кейсы

Об аресте за доксинг в Гонконге

Управление уполномоченного по защите персональных данных Гонконга арестовало 27-летнюю женщину по обвинению в доксинге.

По данным следствия, женщина познакомилась с жертвой через его бывшую подругу в феврале 2022 года. В июле этого года мужчина разорвал отношения, и в том же месяце на одной из социальных сетей был обнаружен пост, содержащий его персональные данные с негативными комментариями о нем.

Размещенные данные включали имя, адреса проживания и работы, номер мобильного телефона, аккаунт в социальных сетях и фотографии.

Женщина подозревается в нарушении статьи 64(3A) Постановления о персональных данных - положения, связанного с доксингом, – поскольку раскрыла личные данные без согласия.

Лицо, совершившее данное преступление, подлежит наказанию в виде штрафа в размере 100 000 гонконгских долларов (~1 млн рублей) и тюремного заключения сроком на два года.

О коллективном иске к Amazon

Суд Девятого окружного апелляционного суда США постановил, что коллективный иск, в котором утверждается, что компания незаконно отслеживала частные группы в Facebook, где водители обсуждали условия труда, должен рассматриваться в суде.

Суд постановил, что соглашение, которое подписал истец - водитель Amazon Дрикки Джексон, обязывающее его обращаться в арбитраж, а не в суд, не применимо к иску 2020 года.

Это означает, что Д. Джексон вправе представлять интересы коллективного иска от лица 800 водителей Amazon вместо того, чтобы подать иск в арбитраж.

Утверждается, что Amazon вторглась в частную жизнь водителей и занималась незаконной прослушкой, создав группу социального прослушивания для мониторинга и перехвата сообщений в частных группах Facebook с помощью автоматизированных инструментов.

Amazon утверждает, что дело должно рассматриваться в арбитраже, ссылаясь на соглашение, подписанное Джексоном, поскольку оно распространяется на «любые споры или претензии, возникающие из или связанные каким-либо образом с выполнением услуг».

Суд, в свою очередь, постановил, что использование водителями групп Facebook и предполагаемые нарушения конфиденциальности со стороны Amazon не относятся к выполнению водителями своих услуг и не затрагивают никаких положений их трудовых договоров с компанией.

Об открытии Европейского центра алгоритмической прозрачности

Европейская комиссия объявила об открытии Европейского центра алгоритмической прозрачности (ECAT).

Центр будет проводить оценку алгоритмов, используемых организациями, которые квалифицируются как очень крупные онлайн-платформы и/или очень крупные онлайн-поисковые системы в соответствии с Законом о цифровых услугах.

В состав ECAT входят представители институтов ЕС, научного сообщества, гражданского общества и промышленности.

ECAT будет обеспечивать анализ отчетов о прозрачности и самооценки рисков, представленных компаниями, и проводить инспекции их систем, когда это потребуется Комиссии.

О записи звонков британской полицией

Управление комиссара по информации (ICO) Великобритании вынесло выговор полиции Суррея и Сассекса за использование приложения, которое записывало и автоматически сохраняло более 200 000 телефонных разговоров без ведома людей.

ICO заявило, что приложение было загружено на рабочие телефоны 1015 сотрудников и собирало большое количество персональных данных, обработка которых, по мнению ICO, была несправедливой и незаконной.

Первоначально планировалось оштрафовать каждый отдел на 1 млн фунтов стерлингов.

Об отмене постановления канадского регулятора в отношении Facebook

Судья Федерального суда отклонил постановление Управления уполномоченного по вопросам конфиденциальности Канады от 2019 года о том, что компания Facebook нарушила законы о конфиденциальности.

В ходе расследования в отношении Cambridge Analytica комиссар постановил, что Facebook нарушила Закон о защите личной информации и электронных документов, поделившись данными пользователей со сторонним приложением без соответствующего согласия.

Об обращении против британского законопроекта о безопасности в Интернете

Руководители приложений для шифрованных чатов, включая WhatsApp и Signal, написали письмо правительству Великобритании, в котором утверждают, что предложенный Законопроект о безопасности в Интернете (Online Safety Bill) фактически объявит вне закона сквозное шифрование.

Отмечается, что законопроект представляет собой беспрецедентную угрозу для частной жизни, безопасности и защиты каждого гражданина Великобритании и людей, с которыми они общаются по всему миру.

О штрафе за сбор данных с использованием темных паттернов

Итальянский орган по защите данных (Garante) оштрафовал компанию, предоставляющую услуги цифрового маркетинга, на 300 000 евро за незаконную обработку персональных данных пользователей в маркетинговых целях.

Garante заявил, что онлайн-порталы компании использовали темные шаблоны, чтобы заманить пользователей дать согласие на обработку данных в маркетинговых целях и на передачу данных третьим лицам с той же целью.

Компания также не смогла доказать наличие согласия на отправку рекламных сообщений.

О соблюдении правил ведения войны в компьютерных играх

Международный комитет Красного Креста (МККК) создал специальный сайт, на котором призвал игроков в онлайн-шутеры соблюдать правила ведения войны.

В частности, МККК призывает:

- не добивать поверженных врагов;
- не стрелять по NPC-некомбатантам;
- не наносить ущерб гражданским объектам;
- применять аптечки ко всем нуждающимся, включая врагов.

Реализовать инициативу МККК предлагает в играх Arma 3 и Fortnite.

На сайте также размещены данные стримеров, которые соблюдают указанные правила.

ИССЛЕДОВАНИЯ, ЭКСПЕРТНЫЕ МНЕНИЯ, ПОЗИЦИИ ГОСУДАРСТВЕННЫХ ОРГАНОВ, ОРГАНИЗАЦИЙ

О судебной статистике

Судебный департамент при Верховном Суде Российской Федерации опубликовал данные судебной статистики за 2022 год.

Всего за отчётный период было рассмотрено 1 545 дел (в 2021 – 1118 дел) о защите авторских и смежных прав в сети «Интернет», в 1 523 делах (в 2021 – 1 095 делах) исковые требования были удовлетворены.

В сфере СМИ в 2022 году в суды было рассмотрено:

- 551 дело о признании регистрации СМИ недействительной, удовлетворены требования регулятора в 543 случаях;
- 67 дел о прекращении или приостановлении деятельности СМИ, требования удовлетворены в 65 делах, из которых предметом 2 дел было прекращение деятельности федерального СМИ, а 9 – прекращение деятельности регионального СМИ;
- 4 дела о приостановлении выпуска СМИ за нарушение законодательства Российской Федерации о выборах и референдумах, в 3 случаях требования удовлетворены полностью, в 1 – частично.

За отчётный период Мосгорсудом было рассмотрено 3 дела об ограничении доступа к аудиовизуальному сервису, во всех случаях доступ был ограничен.

Судами в 2021 годы было рассмотрено 66 257 дел (в 2021 – 87 361 дело) о признании распространяемой в сети «Интернет» информации запрещённой, из которых в 66 001 деле (в 2021 – 87 141 делах) требования были удовлетворены, из них (в 2021 – в 2 409 делах) – частично, в 256 делах (в 2021 – в 220 делах) – в удовлетворении требований было отказано.

119017, г. Москва, Кадашёвская наб., д.6/1/2, стр. 1
+7 (945) 109 00 80
info@iri.center
ири.рф

ОГРН: 1147799015231
ИНН: 7709473987
КПП: 770601001

Также за отчётный период было рассмотрено 1 099 дел (в 2021 – 1 067 дел) о признании распространяемых в сети «Интернет» материалов экстремистскими, из которых отказано в удовлетворении требований было в 2 случаях (в 2021 – 6 случаях).

За совершение преступлений в сфере компьютерной информации за отчётный период было осуждено 280 лиц (в 2021 – 225 лиц).

119017, г. Москва, Кадашёвская наб., д.6/1/2, стр. 1
+7 (945) 109 00 80
info@iri.center
ири.рф

ОГРН: 1147799015231
ИНН: 7709473987
КПП: 770601001

CHATGPT-ИССЛЕДОВАНИЯ

Материал подготовлен ChatGPT
и не является позицией АНО «ИРИ»

Тёмные паттерны

«Тёмные паттерны» – это вводящие в заблуждение методы проектирования, используемые в пользовательских интерфейсах, чтобы заставить людей совершать действия, которые они в противном случае не стали бы совершать.

Эти паттерны могут принимать различные формы, от вводящего в заблуждение текста до запутанного размещения кнопок, и они часто используются для манипулирования пользователями, чтобы заставить их отказаться от своей личной информации или совершить покупки, которые им не нужны.

Использование темных паттернов вызывает растущую озабоченность в технологической индустрии, и как потребители, так и регулирующие органы призывают к большей прозрачности и подотчетности.

Одним из распространенных примеров темного паттерна является техника «наживки и подмены» («bait and switch»). Это когда пользователя заставляют поверить, что он получает что-то одно, но затем ему предлагают нечто совершенно другое.

Например, пользователь может искать определенный товар или услугу в Интернете только для того, чтобы быть перенаправленным на страницу, предлагающую аналогичный, но более дорогой вариант. Пользователь может не осознавать, что им манипулируют, пока не станет слишком поздно.

Другим примером является техника «залезть в корзину» («sneak into basket»). Это когда веб-сайт или приложение добавляет товары в корзину покупок

пользователя без его ведома или согласия. Затем с пользователя может взиматься плата за эти товары, даже если он никогда не намеревался их приобретать.

Этот метод основан на том факте, что многие люди не проверяют свои корзины перед совершением покупки, и предполагает, что они не заметят добавленные товары.

Темные паттерны также используются для манипулирования пользователями, чтобы заставить их отказаться от своей личной информации. Например, веб-сайт может использовать метод «принудительного действия» («forced action»), требуя от пользователей предоставления личной информации для получения доступа к определенной функции или сервису.

Пользователь может не осознавать, что он отказывается от своей информации, или может чувствовать давление, вынуждающее его сделать это, чтобы продолжить использование веб-сайта или приложения.

Использование темных паттернов стало настолько серьезной проблемой, что некоторые правительства начали принимать меры.

В 2019 году штат Калифорния принял закон, который требует от компаний раскрывать информацию о том, используют ли они темные паттерны в своих пользовательских интерфейсах. Закон также дает потребителям право отказаться от использования темных паттернов и потребовать удаления их личной информации.

Европейский союз также предпринял шаги по регулированию использования темных паттернов. Общий регламент ЕС по защите данных (GDPR) требует, чтобы компании получали явное согласие пользователей, прежде чем собирать их личную информацию.

Регламент также требует, чтобы компании предоставляли пользователям четкую и краткую информацию о том, как будут использоваться их данные.

Хотя эти правила являются шагом в правильном направлении, предстоит еще многое сделать для борьбы с использованием темных паттернов. Компании должны

взять на себя ответственность за дизайн своих пользовательских интерфейсов и обеспечить, чтобы они были прозрачными и простыми для понимания.

Потребители также должны сыграть свою роль и должны проявлять бдительность при выявлении случаев использования темных паттернов и сообщать о них.

В заключение, темные паттерны вызывают растущую озабоченность в технологической индустрии и используются для манипулирования пользователями, заставляя их совершать действия, которые они в противном случае не стали бы совершать.

Эти методы обманного проектирования являются формой психологической манипуляции и могут иметь серьезные последствия как для отдельных людей, так и для общества в целом.

Хотя простого решения проблемы темных паттернов не существует, повышение прозрачности и подотчетности со стороны компаний, а также повышение осведомленности потребителей являются важнейшими шагами в борьбе с этими коварными практиками.

Комментарий АНО «ИРИ»:

ChatGPT упоминает принятый в 2019 году закон штата Калифорния, который обязывает компании раскрывать факты использования тёмных паттернов.

Наиболее близок к упомянутому Закон Калифорнии о праве на приватность (California Privacy Rights Act, CPRA) 2020 года.

Однако, этот закон вводит запрет на использование тёмных паттернов при получении согласия потребителя, а не обязанность уведомлять о них.

119017, г. Москва, Кадашёвская наб., д.6/1/2, стр. 1
+7 (945) 109 00 80
info@iri.center
ири.рф

ОГРН: 1147799015231
ИНН: 7709473987
КПП: 770601001

Кроме того, не ясно, что подразумевается под отказом потребителя от тёмных паттернов, поскольку их применение осуществляется не потребителями, а онлайн-площадками.

В 2019 был в Сенате США был представлен проект Закона о сокращении практик, вводящих в заблуждение пользователей (Deceptive Experiences To Online Users Reduction Act, DETOUR Act), который помимо запрета манипулирования с помощью пользовательского интерфейса обязывал крупные онлайн-площадки раскрывать любые эксперименты, направленные на стимулирование вовлечённости пользователей. Однако, законопроект принят не был.

119017, г. Москва, Кадашёвская наб., д.6/1/2, стр. 1
+7 (945) 109 00 80
info@iri.center
ири.рф

ОГРН: 1147799015231
ИНН: 7709473987
КПП: 770601001

Институт развития интернета

ири.рф