



приоритет2030⁺
Лидерами становятся



Защита несовершеннолетних в Интернете: сравнение права США, Великобритании и Российской Федерации : информационно-аналитическая справка / Н.С. Гераськина. — Москва, 2023. — 26 с.

Гераськина Наталья Сергеевна

Руководитель проекта Центра по обеспечению прав

молодежи в цифровом пространстве

Университета имени О.Е. Кутафина (МГЮА)

Информационно-аналитическая справка

«Защита несовершеннолетних в Интернете: сравнение права США, Великобритании и Российской Федерации»

Оглавление

1. Российская Федерация и Соединенные штаты Америки..... 1
2. Российская Федерация и Великобритания..... 17

1. Российская Федерация и Соединенные штаты Америки

По данным Института статистических исследований и экономики знаний НИУ ВШЭ почти 70% российских детей от 3 до 6 лет пользуются Интернетом¹. Этот же показатель среди детей от 7 до 10 лет составляет уже

¹ Цифровая экономика: 2022: краткий статистический сборник / Г. И. Абдрахманова, С. А. Васильковский, К. О. Вишневский и др.; Нац. исслед. ун-т «Высшая школа экономики». — М.: НИУ ВШЭ, 2022. — 124 с.

88%². Данная тенденция обуславливает инициирование изменений в действующее законодательство или принятие абсолютно новых актов, направленных на повышение уровня защиты детей и молодых людей в сети «Интернет», во многих государствах.

Так, в феврале 2022 года в Конгресс США был внесен проект Закона о безопасности детей в Интернете³ (далее – Законопроект о безопасности), возлагающий дополнительные обязательства на онлайн-платформы.

В соответствии с разделом 4 данного законопроекта защищенная платформа⁴ (далее – платформа) должна предоставлять несовершеннолетнему⁵ или родителю, действующему от имени несовершеннолетнего, легкодоступные и простые в использовании средства защиты для контроля процесса использования платформы и личных данных на платформе, включая следующие настройки (далее – средства защиты):

(А) ограничивающие возможность других лиц связаться с несовершеннолетним или найти его на платформе, в частности взрослых, не имеющих отношения к несовершеннолетнему;

(В) запретить другим лицам просматривать персональные данные несовершеннолетнего, собранные или переданные на платформе, в частности, ограничивая публичный доступ к личным данным;

(С) ограничить функции, которые увеличивают использование платформы несовершеннолетним, такие как автоматическое воспроизведение мультимедиа, вознаграждение за время, проведенное на платформе, и уведомления;

² Почти четверть заявок в друзья дети получают от взрослых пользователей. — Текст: электронный // Лаборатория Касперского. — URL: https://www.kaspersky.ru/about/press-releases/2022_pochti-chetvert-zayavok-v-druzya-deti-poluchayut-ot-vzroslyh-polzovatelej (дата обращения: 15.10.2023).

³ Законопроект о безопасности детей в Интернете (S.3663). — Текст: электронный // Официальный сайт Конгресса США. — URL: <https://www.congress.gov/bill/117th-congress/senate-bill/3663/text> (дата обращения: 15.10.2023).

⁴ Защищенная платформа в контексте законопроекта – это коммерческое программное приложение или электронный сервис, который подключается к Интернету и который используется или скорее всего будет использован лицами до 16 лет включительно.

⁵ Исключительно в контексте данного закона. В оригинале используется термин «minor» - лицо до 16 лет включительно.

(D) отказаться от алгоритмических систем рекомендаций, которые используют персональные данные несовершеннолетнего;

(E) удалить учетную запись несовершеннолетнего и запросить удаление личных данных;

(F) ограничить использование геолокации несовершеннолетнего и предоставлять уведомление об отслеживании геолокации несовершеннолетнего;

(G) ограничить время, проводимое несовершеннолетним на платформе.

Если платформа знает или имеет основания полагать, что пользователь несовершеннолетний, то указанные выше средства защиты должны быть приоритетно применимой мерой, а платформа не должна побуждать несовершеннолетнего ослаблять или отключать такие меры.

В Российской Федерации защите персональных данных посвящен Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»⁶ (далее – ФЗ «О персональных данных»), в силу ст. 3 которого персональными данными признается любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). Отдельный правовой режим для персональных данных несовершеннолетних не установлен.

Пункты (А), (В) Законопроекта о безопасности, как правило, предусматриваются настройками конфиденциальности конкретного оператора. Здесь целесообразно привести пример из политики конфиденциальности социальной сети «ВКонтакте»:

«Размещая информацию на персональной странице, в том числе свои персональные данные, Пользователь осознает и соглашается с тем, что указанная информация может быть доступна другим пользователям сети Интернет с учетом особенностей архитектуры и функционала Сайта. Пользователь самостоятельно определяет режим конфиденциальности и

⁶ Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Собрание законодательства РФ. 31.07.2006 г. № 31 (1 ч.). Ст. 3451.

условия доступа к персональным данным. Администрация Сайта принимает технические и организационные меры по обеспечению функционирования соответствующего инструментария Сайта.»

Пункты (C), (D), (G) в данный момент российским правом не урегулированы совсем.

Пункту (E) отвечает положение ст. 9 ФЗ «О персональных данных», в силу которого согласие на обработку персональных данных может быть отозвано субъектом персональных данных.

Вопросы защиты данных о геолокации (пункт (F)) регулируются общими правилами обработки персональных данных.

Таким образом, в рамках ФЗ «О персональных данных» целесообразно рассмотреть возможность создания особого правового режима для персональных данных несовершеннолетних.

Кроме того, раздел 4 Законопроекта о безопасности устанавливает, что платформа не должна рекламировать товары или услуги, продажа которых запрещена несовершеннолетним в соответствии с применимым законодательством штата или федеральным законодательством.

В свою очередь, законодательство Российской Федерации о рекламе более полно регулирует данный вопрос. Помимо объективных запретов (например, запрет рекламы алкогольной продукции обращаться к несовершеннолетним, ст. 21 Федерального закона от 13.03.2006 № 38-ФЗ «О рекламе»⁷ (далее – ФЗ «О рекламе»)), существует и т.н. субъективные запреты, направленные на защиту морально-нравственных ценностей. Они изложены в статье 6 ФЗ «О рекламе»:

В целях защиты несовершеннолетних от злоупотреблений их доверием и недостатком опыта в рекламе не допускаются:

1) дискредитация родителей и воспитателей, подрыв доверия к ним у несовершеннолетних;

⁷ Федеральный закон от 13.03.2006 № 38-ФЗ «О рекламе» // Российская газета, № 51, 15.03.2006.

2) побуждение несовершеннолетних к тому, чтобы они убедили родителей или других лиц приобрести рекламируемый товар;

3) создание у несовершеннолетних искаженного представления о доступности товара для семьи с любым уровнем достатка;

4) создание у несовершеннолетних впечатления о том, что обладание рекламируемым товаром ставит их в предпочтительное положение перед их сверстниками;

5) формирование комплекса неполноценности у несовершеннолетних, не обладающих рекламируемым товаром;

6) показ несовершеннолетних в опасных ситуациях, включая ситуации, побуждающие к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью;

7) преуменьшение уровня необходимых для использования рекламируемого товара навыков у несовершеннолетних той возрастной группы, для которой этот товар предназначен;

8) формирование у несовершеннолетних комплекса неполноценности, связанного с их внешней непривлекательностью.

Ввиду преимущества российского правового регулирования над положениями, изложенными в Законопроекте о безопасности, необходимость рецепции отсутствует.

Еще одно положение, представляющее интерес в рамках данного исследования, касается инструментов родительского контроля. Платформа должна обеспечивать легкодоступные и простые в использовании инструменты для родителей, позволяющие им надлежащим образом контролировать использование несовершеннолетним платформы.

Инструменты должны включать:

(А) возможность контролировать конфиденциальность и настройки учетной записи, включая вышеизложенные средства защиты

(В) возможность ограничивать покупки и финансовые операции несовершеннолетним;

(С) возможность отслеживать общее время, проведенное на платформе;

(D) механизм для родителей, позволяющий отказаться от использования или отключить любые родительские инструменты по умолчанию, установленные на охватываемой платформе;

(E) доступ к другой информации, касающейся использования несовершеннолетним платформы, необходимой родителям для устранения физического и(или) психологического вреда несовершеннолетнему.

О действующих мерах родительского контроля платформа обязана уведомлять несовершеннолетнего.

Похожие инструменты в Российской Федерации на законодательном уровне не предусмотрены, однако существуют в рамках точечных инициатив.

Например, Kaspersky Safe Kids. В бесплатной версии собраны инструменты, которые показывают, что ребёнок ищет в Интернете, на какие сайты заходит, какими программами пользуется и сколько времени проводит в Сети. При желании это можно регулировать, ограничивать и отключать.

Премиум-вариант позволяет следить за зарядом батареи, отслеживать активность в социальных сетях, просматривать историю запросов и составлять расписание, по которому ребёнок будет пользоваться устройством.

Для платных подписчиков доступна и геолокация с возможностью очертить безопасный периметр для прогулок. Если ребёнок попытается обойти запреты или убежит за границы указанной в программе территории, система мгновенно отправит родителю уведомление.

Распространение инструментов родительского контроля в России возможно путем предустановки соответствующего программного обеспечения на продаваемые электронные устройства. Однако данное предложение требует закрепления в Распоряжении Правительства РФ от 13.08.2022 № 2234-р «Об утверждении перечня российских программ для электронных вычислительных машин, которые должны быть предварительно

установлены на отдельные виды технически сложных товаров» (далее – Распоряжение Правительства РФ № 2234-р)⁸.

Перспектива возложения указанных обязательств на платформы, действующие на территории Российской Федерации, требует дополнительного рассмотрения и обсуждения экспертным сообществом ввиду необходимости разработки системы контроля за соблюдением данного требования.

Законопроект о безопасности также возлагает на платформы обязанности, возникающие еще до начала ее использования несовершеннолетним. Так, перед регистрацией, использованием или покупкой несовершеннолетним платформы ему в доступной форме должна предоставляться следующая информация:

(А) уведомление о политике конфиденциальности

(В) информация о том, как получить доступ к средствам защиты и родительским механизмам

(С) уведомление о том, представляет ли платформа, включая любые системы алгоритмических рекомендаций, какие-либо повышенные риски причинения вреда несовершеннолетнему.

Указанная информация представляется родителю, действующему от имени ребенка.

Если платформа использует алгоритмическую систему рекомендаций, то дополнительно должна предоставлять информацию об используемых персональных данных несовершеннолетних, о возможности влиять на алгоритмы и понижать категории выдаваемого ими контента.

При этом перед первым использованием платформы ребенок/родитель, действующий от его имени, должны подтвердить получение информации, связанной с повышенными рисками причинения вреда несовершеннолетнему.

⁸ Распоряжение Правительства РФ от 13.08.2022 № 2234-р «Об утверждении перечня российских программ для электронных вычислительных машин, которые должны быть предварительно установлены на отдельные виды технически сложных товаров» // Собрание законодательства РФ, 29.08.2022, N 35, ст. 6125.

В Российской Федерации в силу ст. 18 и ч. 7 ст. 14 ФЗ «О персональных данных» при сборе персональных данных оператор обязан предоставить субъекту персональных данных по его просьбе информацию:

- 1) подтверждение факта обработки персональных данных оператором;
- 2) правовые основания и цели обработки персональных данных;
- 3) цели и применяемые оператором способы обработки персональных данных;

- 4) наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;

- 5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

- 6) сроки обработки персональных данных, в том числе сроки их хранения;

- 7) порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;

- 8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

- 9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу и иные сведения, предусмотренные данным ФЗ.

Указанное положение отвечает пункту (А). При этом в силу ст. 9 ФЗ «О персональных данных» субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку

персональных данных должно быть конкретным, предметным, информированным, сознательным и однозначным.

Пункт (В), как правило, содержится в политике конфиденциальности, законодательно не закреплён.

В некоторой степени уведомлением в смысле пункта (С) является маркировка ресурсов, осуществляемая в соответствии с Федеральным законом от 29.12.2010 N 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»⁹ (далее – ФЗ «О защите детей от информации...»). Так, информационная продукция имеет 5 возрастных категорий: 0+; 6+; 12+; 16+ и 18+. Знак информационной продукции указывается на главной странице сетевого издания и должен соответствовать самой старшей возрастной категории информационной продукции, распространяемой в данном выпуске.

При этом рекомендации Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее – Роскомнадзор) по применению данного ФЗ устанавливают, что знак информационной продукции должен располагаться в верхней части главной страницы, по размеру должен быть не меньше 75% от заголовка второго уровня или не меньше размеров шрифта основного текста с применением полужирного начертания, или не меньше 20% от основной информационной колонки. По цвету знак информационной продукции должен соответствовать или быть контрастным цвету заголовка издания.

Регулирование пункта (В) напрямую зависит от закрепления статуса родительских механизмов контроля, перспектива которого изложена выше.

Законопроект о безопасности возлагает на платформы обязательства, связанные не только с их непосредственным функционированием, но и отчетностью. Не реже одного раза в год платформа должна публиковать публичный отчет с указанием прогнозируемых рисков причинения вреда

⁹ Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» // Российская газета, N 297, 31.12.2010.

несовершеннолетним на основе независимого стороннего аудита, проведенного путем разумной проверки платформы, и описывать меры по предотвращению и смягчению последствий, принятые для устранения таких рисков.

В такой отчет должен входить, в том числе, учет пользователей по возрасту в диапазонах 0–5 лет, 6–9 лет, 10–12 лет и 13–16 лет, среднестатистическое время, проведенное данными возрастными группами на платформе, количество обращений на незаконный и вредный контент, действия платформы по обеспечению прав несовершеннолетних и их защите от такого контента.

В Российской Федерации ст. 10.6 ФЗ «Об информации...» обязывает владельца сайта и (или) страницы сайта в сети «Интернет» ежегодно размещать отчет о результатах рассмотрения обращений, поданных на нарушение закона об информации с использованием электронной формы, а также о результатах мониторинга нарушений законодательства об информации.

Требования к отчету устанавливаются Приказом Роскомнадзора от 02.04.2021 N 47 «Об утверждении требований к форме, составу и размещению ежегодных отчетов о результатах рассмотрения обращений, поданных с использованием электронной формы для направления обращений о распространяемой с нарушением закона информации»¹⁰. Однако данные требования носят исключительно количественный характер (например, количество заблокированных страниц). Представляется целесообразным дополнить указанный приказ требованиями к качественным показателям отчетности.

Законопроект о безопасности предполагает создание Помощника министра торговли по связи и информации (далее – Помощник). Помощник

¹⁰ Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 02.04.2021 N 47 «Об утверждении требований к форме, составу и размещению ежегодных отчетов о результатах рассмотрения обращений, поданных с использованием электронной формы для направления обращений о распространяемой с нарушением закона информации» // URL: <http://publication.pravo.gov.ru/Document/View/0001202105310019> (дата обращения: 16.10.2023).

должен разработать программу, в рамках которой исследователь может подать заявку, и платформа должна предоставлять доступ к активам данных с единственной целью проведения исследований в общественных интересах, касающихся вреда безопасности и благополучию несовершеннолетних. При этом создание такого института не должно рассматриваться как способ сбора информации государственными органами.

Аналогов данного института в Российской Федерации нет. Такая инициатива может найти свое отражение в виде изменений в ФЗ «О персональных данных», Федеральный закон от 23.08.1996 N 127-ФЗ «О науке и государственной научно-технической политике»¹¹ с целью дальнейшей популяризацией изучения актуальных угроз цифровой среды путем вовлечения молодежи в рамках научного волонтерства.

Для изучения технических возможностей соблюдения требований, изложенных в Законопроекте о безопасности, Директор Национального института стандартов и технологий Соединенных штатов Америки в координации с Федеральной комиссией по связи, Федеральной торговой комиссией и Министром торговли должен провести исследование, оценивающее наиболее технологически осуществимые варианты разработки систем для проверки возраста на уровне устройства или операционной системы. Исследование должно отвечать на следующие вопросы:

(1) преимущества создания системы проверки возраста на уровне устройства или операционной системы;

(2) какую информацию, возможно, потребуется собрать для создания такого типа системы проверки возраста;

(3) точность таких систем и их воздействие или шаги по улучшению доступности, в том числе для лиц с ограниченными возможностями;

¹¹ Федеральный закон от 23.08.1996 N 127-ФЗ «О науке и государственной научно-технической политике» // Российская газета, N 167, 03.09.1996.

(4) как такая система или системы могут проверять возраст, снижая риски для конфиденциальности пользователей и безопасности данных и защищая личные данные несовершеннолетних;

(5) техническая осуществимость, включая необходимость потенциальных изменений аппаратного и программного обеспечения, в том числе для устройств, находящихся в настоящее время в продаже и принадлежащих потребителям.

Российское законодательство прямо не отвечает, с какого возраста ребенок может пользоваться социальными сетями. Этот вопрос выведен за рамки юридического регулирования – во многом по причине потенциальных сложностей с технической реализацией установления возрастных цензов.

Многие интернет-ресурсы также не спешат самостоятельно устанавливать требования к минимальному возрасту своих пользователей.

Дальше всего в этом вопросе продвинулось приложение «TikTok». В своей политике конфиденциальности разработчики установили следующие ограничения:

- TikTok предназначен только для пользователей, достигших 13 лет (14 лет в Южной Корее и Индонезии).
- Если пользователь, который пытается создать аккаунт, еще не достиг минимальных требований к возрасту, платформа ограничит ему возможность создать аккаунт с другой датой рождения.
- Корректная информация о пользователях позволяет обеспечивать пользователям опыт, соответствующий их возрасту – например, ограничивать доступ к различным функциям или показывать рекламу. Так, приложение не разрешает юным пользователям TikTok проводить прямые трансляции или пользоваться личными сообщениями до достижения определенного возраста.

Стоит отметить, что не позднее, чем через один год после даты вступления в силу Законопроекта о безопасности, Министр торговли должен

создать и созвать Совет по безопасности детей в Интернете с целью предоставления консультаций по реализации данного Закона.

Совет по безопасности детей в Интернете должен включать следующих членов:

(1) родители, эксперты-академики, медицинские работники и члены гражданского общества;

(2) представительство молодежи;

(3) представители платформ;

(4) представители Национального управления телекоммуникаций и информации, Национального института стандартов и технологий, Федеральной торговой комиссии и Министерства юстиции;

(5) Генеральный прокурор штата или его представители.

Аналогов данного института в России нет. Существуют либо общественные институты (Молодежный цифровой омбудсмен, Альянс по защите детей в цифровой среде), либо государственные органы с предметной компетенцией (например, Роскомнадзор).

В связи с этим представляется актуальным создание уполномоченного органа по цифровым правам. Преимуществами такого органа выступят коллегиальность, представительство всех заинтересованных субъектов. Также его члены будут связаны не должностными обязанностями, а фактическим отношением к данной деятельности.

При этом целесообразно установить специальный статус членов данного Совета в сравнении с общими требованиями к государственным гражданским служащим (например, возможность для молодых людей входить в Совет при отсутствии высшего образования), так как это обеспечит действительное представительство заинтересованных субъектов и реальное решение проблем цифровой среды.

Ранее, в мае 2021 года в Конгресс США также был внесен проект Закона о защите конфиденциальности детей и подростков в Интернете (далее

– Законопроект о конфиденциальности)¹², распространяющий на подростков в возрасте до 16 лет меры защиты конфиденциальности, ранее предусмотренные только для пользователей в возрасте до 13 лет.

Стоит отметить, что Законопроект о конфиденциальности распространяется только на те интернет-ресурсы и приложения, которые предназначены для несовершеннолетних¹³. Определение такого ресурса или приложения осуществляется на основании анализа его тематики, публикуемого контента, использования персонажей и (или) людей, пользующихся популярностью у данной возрастной группы, направленности рекламы и других характеристик.

В Российской Федерации отдельный правовой режим конфиденциальности несовершеннолетних на законодательном уровне не установлен. Интернет-ресурсы и приложения могут самостоятельно устанавливать дополнительные меры.

Например, в приложении «TikTok» по умолчанию аккаунты пользователей младше 16 лет установлены как приватные, что означает, что пользователь может одобрять или отклонять запросы подписчиков, и только пользователи, которых были одобрены в качестве подписчиков, могут видеть контент. Аккаунты пользователей старше 16 лет изначально устанавливаются как публичные, что означает, что любой пользователь TikTok может просматривать опубликованные видео, оставлять комментарии и участвовать в обсуждении контента.

Однако часто вопрос конфиденциальности решается самим пользователем. Например, в соответствии с политикой конфиденциальности социальной сети «ВКонтакте» пользователь самостоятельно определяет режим конфиденциальности и условия доступа к персональным данным.

¹² Законопроект о защите конфиденциальности детей и подростков в Интернете (S.1628). — Текст: электронный // Официальный сайт Конгресса США. — URL: <https://www.congress.gov/bill/117th-congress/senate-bill/1628/text> (дата обращения: 18.10.2023).

¹³ Исключительно в контексте данного закона. В оригинале используется термин «minor» - лицо до 16 лет включительно.

В рамках правового регулирования Российской Федерации возможно возложение обязанности на платформы по установке наиболее защищенного режима конфиденциальности по умолчанию при регистрации пользователя на интернет-ресурсе или в приложении с возможностью изменить режим самостоятельно (например, с 14 лет) или без таковой (младше 14 лет).

Законопроект о конфиденциальности запрещает оператору интернет-ресурса или приложения использовать, раскрывать третьим лицам или собирать личную информацию несовершеннолетнего для целевого маркетинга, если:

- несовершеннолетний является пользователем интернет-ресурса или приложения;
- оператор имеет основания полагать, что пользователь является несовершеннолетним или интернет-ресурс, приложение предназначены для несовершеннолетнего.

Указанный запрет не применяется к оператору, который получил поддающееся проверке согласие¹⁴ соответствующего несовершеннолетнего.

В Российской Федерации ФЗ «О рекламе» устанавливает ограничения касательно именно содержания рекламы (например, ст. 6 запрещает создание у несовершеннолетних впечатления о том, что обладание рекламируемым товаром ставит их в предпочтительное положение перед их сверстниками). Вопрос же о передаче персональных данных в маркетинговых целях в целом остается законодательно не урегулированным.

Снова обратимся к политике конфиденциальности приложения «TikTok». Она гласит, что система управления рекламой и рекомендациями TikTok разработана таким образом, чтобы информация о пользователе не распространялась на сторонних рекламодателей напрямую. Рекламодатели

¹⁴ В контексте данного законопроекта – любые разумные усилия (с учетом доступных технологий), включая запрос разрешения на будущий сбор, использование и раскрытие информации, обеспечивающие получение несовершеннолетним уведомления о сборе, использовании и раскрытии информации и свободное и недвусмысленное единоличное уполномочивание на осуществление таких действий.

могут выбрать только определенные группы пользователей по таким критериям, как, например, пол или возраст.

Еще одной мерой защиты Законопроект о конфиденциальности обозначил запрет на продажу подключенных к Интернету устройств, предназначенных для детей и подростков до 16 лет, если они не соответствуют определенным стандартам кибербезопасности и защиты персональных данных. Законопроект требует от производителей таких устройств отображать панель управления конфиденциальностью, которая должна содержать информацию о том, как персональные данные собираются, передаются, хранятся, используются и защищаются производителем устройства.

Упоминание панели конфиденциальности или похожих систем в Распоряжение Правительства РФ № 2234-р отсутствует. Вместе с тем, операционные системы (Android, IOS и др.) зачастую устанавливают такие панели конфиденциальности самостоятельно.

Нормативное закрепление предустановки панелей конфиденциальности (в том числе, в Распоряжении Правительства РФ № 2234-р) возможно только при создании такого технического механизма, который будет отвечать целям его внедрения, а также будет доступен всем разработчикам и дистрибьюторам.

На основании сравнительного анализа Законопроекта о безопасности и Законопроекта о конфиденциальности с российским правом можно отметить тенденцию возложения на ИТ-сектор Соединенных штатов Америки дополнительных обязательств перед государством. Вместе с тем, законодательное закрепление в российском праве ряда изложенных в законопроектах механизмов представляется стратегически важным и актуальным.

2. Российская Федерация и Великобритания

Законопроект о безопасности в Интернете (далее – Законопроект о безопасности)¹⁵ был внесен в Парламент Великобритании в мае 2021 года (как и Законопроект о конфиденциальности в Соединенных штатах Америки).

В соответствии с данным законопроектом все сервисы¹⁶ обязаны:

- проводить надлежащую и достаточную оценку риска незаконного контента в установленные сроки и в соответствии с актуальными данными о том, какой контент считается незаконными, предоставляемыми OFCOM¹⁷.
- учитывать риск незаконного контента при внесении изменений в дизайн, функции и другие элементы сервиса.
- принимать меры по созданию функциональных возможностей, позволяющих пользователям контролировать контент, с которым они сталкиваются в результатах поиска по сервису.

Дополнительные обязанности Законопроектом о безопасности возлагаются на сервисы, в отношении которых есть основания полагать, что к ним имеют доступ дети. Такие сервисы обязаны:

- управлять рисками причинения вреда детям различных возрастных групп и снижать их на основании оценки соответствующих рисков.
- снижать влияние контента, причиняющего вред детям различных возрастных групп.
- обеспечивать достаточные меры для предупреждения контента, причиняющего вред детям (например, путем использования механизмов верификации возраста), и защиты от него.

¹⁵ Законопроект о безопасности в Интернете — Текст: электронный // Официальный сайт Парламента Великобритании. — URL:<https://bills.parliament.uk/bills/3137> (дата обращения 23.10.2023)

¹⁶ В контексте данного законопроекта – Интернет-ресурс, посредством которого контент, который генерируется пользователем непосредственно на ресурсе, загружается на ресурс или распространяется пользователем, может быть доступен одному и более пользователям ресурса.

¹⁷ Британское агентство, регулирующее работу теле- и радио-компаний, а также почтовой службы.

- оценивать уровень риска функциональных возможностей сервиса по поиску информации, в результате использования которых дети могут столкнуться с контентом, причиняющим вред.

- определять, какие меры, в том числе, по повышению уровня медиаграмотности пользователей и безопасному использованию сервиса, а также другие функциональные возможности могут снизить или увеличить выявленные риски.

Оценка риска незаконного контента в соответствии с Законопроектом о безопасности означает оценку:

- базы пользователей в целом;
- категорий пользователей, которые могут столкнуться с незаконным контентом;
- каждого вида незаконного контента;
- скорости и простоты распространения незаконного контента с учетом алгоритмов сервиса и его функциональных возможностей;
- риска причинения вреда физическим лицам в результате наличия незаконного контента или использования сервиса для совершения или содействия преступлению;
- способов использования сервиса и влияние такого использования на уровень риска причинения вреда физическим лицам;
- характера и серьезности причиненного вреда в вышеупомянутых случаях;
- как дизайн и функционирование сервиса (включая управление им, использование профилактических технологий, меры по повышению медиаграмотности пользователей, а также другие системы и процессы) могут снизить или увеличить выявленные риски.

Эти же критерии используются при оценке риска причинения контентом вреда детям. Помимо этого, в качестве функциональных возможностей сервиса, повышающих вероятность риска причинения вреда детям, считается предоставление взрослым пользователям возможности

искать других пользователей сервиса (включая детей) и связываться с другими пользователями (включая детей) посредством данного сервиса.

Оценка риска причинения вреда детям осуществляется с учетом возрастных, социальных и иных характеристик, позволяющих отнести детей к определенной группе, на которую оказывается негативное влияние (при наличии цели влияния на ту или иную группу). При этом деятельность сервисов по управлению рисками, связанными с негативным влиянием контента, должна осуществляться в соответствии с актуальными данными об отнесении того или иного контента к категории «причиняющий вред» и основываться на характере контента, а не самом факте его распространения.

В случае выявления контента, причиняющего вред, но не отнесенного к такой категории, сервис обязан уведомить об этом OFCOM, указав при этом информацию о характеристиках и степени распространенности на сервисе выявленного контента. Вместе с тем, сервис несет ответственность за управление рисками негативного влияния только такого контента, который был выявлен в ходе последней проведенной оценки.

На основании оценки рисков сервис обязан принимать меры по обеспечению функционирования таким образом, чтобы предотвращать столкновение пользователей с незаконным / причиняющим вред контентом, снижать риск его публикации и распространения, а также причинения вреда физическим лицам таким контентом. Если на сервисе все же обнаружен незаконный / причиняющий вред контент, то сервис обязан свести к минимуму период времени, в течение которого опубликован такой контент, и как можно быстрее удалить его.

При этом в пользовательском соглашении сервис обязан указать следующую информацию:

- какие механизмы сервиса защищают пользователей от незаконного контента / детей от причиняющего вред контента

- какие механизмы сервиса используются для предупреждения публикации и распространения незаконного контента / контента, причиняющего вред детям, как и когда такие механизмы срабатывают

- применяемые меры в случае ограничения доступа детей ко всему сервису или к его части.

В Российской Федерации обороту и защите информации посвящен ФЗ «Об информации...». Обобщенного понятия «незаконный контент» он не содержит, норма формулируется через перечисление конкретных запретов. Например, в соответствии с ч. 1 ст. 10.4 владелец новостного агрегатора обязан:

- не допускать его использование в целях совершения уголовно наказуемых деяний, разглашения сведений, составляющих государственную или иную специально охраняемую законом тайну, распространения материалов, содержащих публичные призывы к осуществлению террористической деятельности или публично оправдывающих терроризм, других экстремистских материалов, а также материалов, пропагандирующих порнографию, насилие и жестокость, и материалов, содержащих нецензурную брань;

- соблюдать запреты и ограничения, предусмотренные законодательством Российской Федерации о референдуме и законодательством Российской Федерации о выборах;

- соблюдать требования законодательства Российской Федерации, регулирующие порядок распространения массовой информации и др.

Стоит отметить, что требования распространяются только на те новостные агрегаторы, доступ к которым в течение суток составляет более одного миллиона пользователей сети «Интернет».

В силу п. 1 ч. 1 ст. 10.5, п. 1 ч. 1 ст. 10.6 и п. 1 ч. 1 ст. 10.7 ФЗ «Об информации...» похожие требования (за исключением обусловленных видом источника информации) предъявляются и к владельцам аудиовизуальных сервисов, социальных сетей и сервисов размещения объявлений. Однако, в

отличие от новостных агрегаторов, требования к количеству пользователей, имеющих доступ к аудиовизуальному сервису или сервису размещения объявлений, значительно ниже – более ста тысяч пользователей в течение суток, а к социальным сетям – более пятисот тысяч в течение суток.

На источники информации, доступ к которым имеет количество пользователей менее установленного, упомянутые выше требования не распространяются. При этом при оценке количества пользователей учитываются только те, кто находится на территории Российской Федерации.

Аналогов процедуры «оценки рисков» и критериев для ее проведения в российском праве не предусмотрено. ФЗ «Об информации...» позволяет сервисам самостоятельно выбирать, как построить работу в целях недопущения публикации и распространения информации, нарушающей законодательство, а также ее выявления.

Таким образом, можно сделать вывод, что положения Законопроекта о безопасности требуют от сервисов большего объема предупредительной работы, чем регулирование в Российской Федерации. Внедрение общих для всех платформ критериев по предупреждению публикации и пресечению распространения незаконного контента позволит унифицировать деятельность в этой области.

Если предупредительные механизмы не сработали, Законопроект о безопасности устанавливает для сервисов обязанность по функционированию и доступности инструментов, позволяющих подавать жалобы на контент. Она возлагается:

- на все сервисы – в отношении незаконного контента;
- на сервисы, в отношении которых есть основания полагать, что к ним имеют доступ дети, – в отношении контента, причиняющего вред детям.

Любой сервис обязан обеспечить рассмотрение поступающих обращений, касающихся:

- публикуемого на сервисе контента, если у пользователей есть основания полагать, что такой контент является незаконным.

- действий сервиса по исполнению обязанностей по контролю за незаконным контентом, а также по обеспечению приватности и свободы слова.

- удаленного контента, если он был признан сервисом незаконным.
- действий сервиса по ограничению его использования пользователями (например, в случае блокировки пользователя за публикацию незаконного контента).

- использования инструментов модерации незаконного контента, если такие инструменты работают некорректно.

Сервис, в отношении которого есть основания полагать, что к нему имеют доступ дети, обязан обеспечить рассмотрение поступающих обращений, касающихся:

- публикуемого на сервисе контента, если у пользователей есть основания полагать, что такой контент причиняет вред детям.

- действий сервиса по исполнению обязанностей по контролю за причиняющим вред контентом.

- удаленного контента, если он был признан сервисом причиняющим вред детям.

- действий сервиса по ограничению его использования пользователями (например, в случае блокировки пользователя за публикацию причиняющего вред контента).

- использования инструментов модерации причиняющего вред контента, если такие инструменты работают некорректно.

Сервисы обязаны вести учет рассмотренных обращений и предпринятых в соответствии с ними мер.

В Российской Федерации в качестве механизма, позволяющего подавать жалобы на контент, в некоторой степени можно рассматривать требования ст. 10.4-10.7 ФЗ «Об информации...» по размещению на новостном агрегаторе, аудиовизуальном сервисе, социальной сети или сервисе размещения объявлений адреса электронной почты для направления

владельцу сервиса юридически значимых сообщений, а также фамилию и инициалы владельца (для физического лица) или наименование владельца (для юридического лица).

Вместе с тем, юридически значимые сообщения в их понимании российским гражданским правом включают заявления, уведомления, извещения, требования или иные юридически значимые сообщения, с которыми закон или сделка связывает гражданско-правовые последствия для другого лица. Такая трактовка обуславливает необходимость рассмотрения вопроса о прямом отражении возможности подавать обращения в ФЗ «Об информации...», например, в вышеупомянутых ст. 10.4-10.7.

Кроме того, владельцы социальных сетей дополнительно обязаны разместить электронную форму для направления обращений о распространяемой с нарушением закона информации, требования к которой устанавливаются федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, т.е. Роскомнадзором.

Правила использования социальной сети должны содержать порядок рассмотрения обращений пользователей социальной сети, обеспечивающий их рассмотрение в срок, не превышающий 30 календарных дней со дня их поступления. По результатам рассмотрения поданных обращений должен ежегодно размещаться отчет.

Таким образом, учет рассмотренных обращений и предпринятых в соответствии с ними мер на данный момент в Российской Федерации ведется только социальными сетями.

Отдельный акцент в Законопроекте о безопасности делается на регулирование поисковых сервисов. Так, все поисковые сервисы обязаны:

- соблюдать требования, предъявляемые ко всем сервисам, действующим на территории Великобритании (оценка рисков, обеспечение

механизмов подачи жалоб на контент и процессов рассмотрения таких жалоб, требования к содержанию пользовательского соглашения и т.д.).

- принимать меры по созданию функциональных возможностей, позволяющих пользователям контролировать контент, с которым они сталкиваются в результатах поиска по сервису.

Дополнительные обязанности возлагаются на поисковые сервисы, в отношении которых есть основания полагать, что к ним имеют доступ дети.

Такие сервисы обязаны:

- соблюдать требования, изложенные в Главе 2, предъявляемые ко всем сервисам, действующим на территории Великобритании, в отношении которых есть основания полагать, что к ним имеют доступ дети (оценка рисков, обеспечение механизмов подачи жалоб на контент и процессов рассмотрения таких жалоб, требования к содержанию пользовательского соглашения и т.д.).

- оценивать уровень риска функциональных возможностей поискового сервиса, в результате использования которых дети могут столкнуться с контентом, причиняющим вред.

- определять, какие меры, в том числе, по повышению уровня медиаграмотности пользователей и безопасному использованию сервиса, а также другие функциональные возможности могут снизить или увеличить выявленные риски.

Особое внимание поисковые сервисы обязаны уделять следующим категориям жалоб:

- на выдаваемый по результатам поиска контент, если пользователь считает его незаконным.

- на действия и(или) бездействие поискового сервиса (например, блокировка контента как незаконного, хотя данный контент таким не признан).

- если контент того или иного пользователя больше не появляется в результатах поиска или получает более низкий приоритет в результатах поиска по причине соблюдения поисковым сервисом законодательства.

Особое внимание поисковые сервисы, в отношении которых есть основания полагать, что к ним имеют доступ дети, обязаны уделять следующим категориям жалоб:

- на выдаваемый по результатам поиска контент, если пользователь считает, что такой контент причиняет вред детям.

- на действия и(или) бездействие поискового сервиса (например, блокировка контента как причиняющего вред детям, хотя данный контент таким не признан).

- если контент того или иного пользователя больше не появляется в результатах поиска или получает более низкий приоритет в результатах поиска по причине соблюдения поисковым сервисом законодательства.

- если пользователь не может получить доступ к контенту для определенной возрастной группы из-за некорректной работы механизма верификации возраста.

Поисковые сервисы обязаны вести учет рассмотренных обращений и принятых в соответствии с ними мер.

В Российской Федерации правовое регулирование поисковых сервисов весьма ограничено. Ключевой обязанностью, установленной ФЗ «Об информации...» и обеспечивающейся Кодексом Российской Федерации об административных правонарушениях, является принятие мер по противодействию использованию информационно-телекоммуникационных сетей и информационных ресурсов, посредством которых обеспечивается доступ к информационным ресурсам и информационно-телекоммуникационным сетям, доступ к которым ограничен на территории Российской Федерации.

В то же время, на сегодняшний день большинство поисковых сервисов и информационных ресурсов в целом уже имеют службы поддержки и

реализуют корпоративную ответственность в отношении своих пользователей в соответствии с теми техническими и иными возможностями, которыми они обладают. В связи с этим законодательное закрепление подобной обязанности представляется нецелесообразным.

Таким образом, Законопроект о безопасности достаточно подробно регламентирует деятельность платформ по предупреждению незаконного и причиняющего вред детям контента и реагированию на распространение такого контента.

Подводя итоги исследования, можно отметить тенденцию ужесточения правового регулирования платформ в Соединенных штатах Америки и Великобритании. Некоторые положения рассмотренных законопроектов имеют перспективы реализации в законодательстве Российской Федерации, но с учетом правовых, технологических и иных особенностей. Часть положений неактуальна ввиду преимущества российского права, а часть уже реализуется на практике несмотря на отсутствие корреспондирующей правовой нормы.