

|  |
| --- |
| **ОБЩЕРОССИЙСКАЯ ОБЩЕСТВЕННАЯ ОРГАНИЗАЦИЯ**  **«АССОЦИАЦИЯ ЮРИСТОВ РОССИИ»**  **МОСКОВСКОЕ ОТДЕЛЕНИЕ**  **Комиссия по правовому обеспечению Цифровой экономики** |
| 119991, г. Москва, ГСП-1, Ленинские горы, д. 1, стр. 13,  4 учебный корпус МГУ имени М.В. Ломоносова, Юридический факультет, ауд. 611 а  тел.: +7 (499) 706-00-06, доб. 148; e-mail: [digitallaw@alrf.msk.ru](mailto:digitallaw@alrf.msk.ru)  <http://www.alrf.msk.ru> |

|  |  |
| --- | --- |
| «06» марта 2020 года | г. Москва |

**ЗАКЛЮЧЕНИЕ  
ПО ТЕМЕ «ПРАВОВЫЕ СРЕДСТВА БОРЬБЫ С ПРОТИВОПРАВНЫМ КОНТЕНТОМ В СЕТИ ИНТЕРНЕТ И ИСПОЛЬЗОВАНИЕ САМОРЕГУЛИРОВАНИЯ В ДАННОЙ СФЕРЕ»**

«27» февраля 2020 года в Университете имени О.Е. Кутафина (МГЮА) состоялось заседание Комиссии по правовому обеспечению цифровой экономики Московского отделения АЮР (далее - «**Комиссия**») по теме «Правовые средства борьбы с противоправным контентом в сети интернет и использование саморегулирования в данной сфере**»**. В заседании и дискуссии приняли участие члены Комиссии, представители Государственной Думы Федерального Собрания Российской Федерации, международных и российских ассоциаций, органов государственной власти, члены Ассоциации юристов России, представители бизнеса и научного сообщества.

По результатам заседания Комиссия считает целесообразным опубликовать заключение с описанием ключевых проблем и предложений по вопросам, затронутым в докладах и рабочей дискуссии.

1. **ВВЕДЕНИЕ**

Стремительное технологическое развитие влечет за собой социальные и экономические преобразования, модернизацию способов коммуникаций. С изменением роли интернет сервисов в общественной жизни существенно повышаются риски их использования для совершения правонарушений. При этом существуют особенности распространения информации в сети интернет широкий охват аудитории, быстрота распространения, доступность сервисов, трансграничный характер их деятельности, как правило обуславливают выбор злоумышленников в пользу крупных платформ распространения информации.

Так, сервисы организаторов распространения информации в сети интернет нередко применяются для коммуникаций в ходе планирования, координации и совершения преступлений, для пропаганды идей экстремистского толка и оправдания терроризма, вовлечения в противоправную деятельность граждан.

Кроме этого, на основе таких сервисов могут реализовываться проекты социальной инженерии, распространяется недостоверная и провокационная информация, осуществляется незаконный сбор данных о пользователях.

На сайтах сервисов частных объявлений нередко размещается информация о продаже ограниченных в обороте предметов, создаются условия для совершения мошеннических действий. Так на крупнейших платформах можно встретить объявления о продаже сим-карт, дипломов, медицинских справок, больничных листов, оружия, продажа которых не допускается и т.п.

Информация, размещаемая на сайтах знакомств, зачастую используются для совершения преступлений против половой неприкосновенности, а также для обмана и посягательств на несовершеннолетних.

На многих ресурсах, в том числе сайтах операторов поисковых систем размещается реклама запрещенных в России казино, а также услуг, оказание которых не допускается без наличия лицензии или иных разрешительных документов.

В настоящее время в РФ и мировой практике многие вопросы уже имеют законодательное регулирование и даже сформировавшеюся правоприменительную практику, однако появляются все новые виды контента, содержащего заведомо недостоверную или противоправную информацию: фейкньюс[[1]](#footnote-2), дипфейк[[2]](#footnote-3), кликбейт и т.д. Нередко такой контент создается в автоматизированном порядке, с применением новых информационных технологий, в связи с чем существующие законодательные процедуры ограничения доступа к контенту либо не «улавливают» его, либо не способны эффективно реагировать на него.

Распространение недостоверного контента в ряде случаев создает угрозу нарушения прав и интересов граждан и государства, наносит значительный вред интернет индустрии, подрывает авторитет добросовестных компаний, ведет к оттоку пользователей с интернет-платформ. Важно отметить, что условия развития Интернета, оборота информации и контента постоянно меняются и развиваются. Именно поэтому необходимо обеспечить адекватные и оперативные меры реагирования на подобные явления, соблюдая баланс прав интересов граждан, бизнеса и государства.

В этой связи имеет смысл обратиться к зарубежному опыту, поскольку с аналогичными проблемами сталкиваются и иные страны и имплементированные ими механизмы могут представлять интерес для России, хотя, безусловно, их механическое копирование в российские реалии является нецелесообразным.

1. **Зарубежный опыт и практика регулирования**

**Федеративная Республика Германии**

«Сетевой закон» Германии NetzDG 2017 года[[3]](#footnote-4) регулирует деятельность социальных сетей. Он относится к коммерческим провайдерам Интернет-услуг, владельцев платформ социальных сетей, где пользователи могут публиковать контент, но не относится к платформам, где публикуется журналистский или редакторский контент, за который полностью ответственны владельцы Интернет-платформы. Соответствующие платформы должны предотвращать распространение запрещенного контента и обеспечивать взаимодействие с государственными органами в целях пресечения нарушений. При этом выполнение таких функций может быть возложено и на саморегулируемую организацию.

Согласно закону, организация может осуществлять саморегулирование, если:

- обеспечены независимость и достаточный экспертный опыт ее аналитиков;

- созданы соответствующие технические условия работы и гарантировано срочное рассмотрение обращения в течение 7-дневного периода;

- установлены процессуальные правила, регулирующие охват и структуру проведения рассмотрения контента;

- разработаны требования к аффилированным социальным сетям о порядке направления жалоб и обращений и предоставлена возможность пересмотра решений;

- создана служба рассмотрения жалоб;

- организация финансируется несколькими Интернет-провайдерами социальных сетей или организациями, что гарантирует наличие соответствующих технических мощностей.

В законодательстве Германии закрепляется принцип социальной ответственности профессиональных субъектов, осуществляющих свою деятельность в сети интернет, например, в обязательной публикации о предпринятых действиях в ответ на жалобы пользователей на немецком языке.

Отчет о рассмотрении жалоб должен публиковаться компаниями каждые 6 месяцев и содержать, в том числе:

- механизмы борьбы с незаконным контентом;

- критерии, применяемые при принятии решения о том, следует ли снимать или блокировать контент;

- количество жалоб, поданных в отчетный период, их причины и т.п.

Штрафные санкции за нарушения требований о предоставлении отчетности доходят до 5 млн. евро и устанавливаются в случаях: не подготовки отчетов, неполном или несвоевременном представлении (опубликовании) информации, не соблюдении процедуры рассмотрения жалоб, поданных соответствующими органами, или пользователями, чье место жительства или место нахождения в ФРГ.

В качестве требований к профессиональным платформам распространения информации также устанавливаются: проведение мониторинга реагирования на жалобы; применение организационных мер для повышения эффективности их рассмотрения.

**Соединенное Королевство Великобритании и Северной Ирландии**

В Великобритании действует «Белая книга о вреде, причиняемом в сети интернет (Online Harms White Paper)[[4]](#footnote-5). Документ, является частью государственной Стратегии безопасного Интернета, на его основании осуществляется контроль предоставления интернет компаниями ежегодных публичных «Отчетов прозрачности».

К отчетам предъявляются требования, согласно которым они должны отражать текущие процессы борьбы компаний с угрозами вредоносного контента на своих платформах, включая принятые меры и их эффективность. Кроме этого, крупные компании-провайдеры услуг должны раскрывать дополнительную информацию, включая механизмы проактивного реагирования на появляющиеся и существующие угрозы и др.

Кроме того, правительство Великобритании объявило, что регулятор в области медиа- и телекоммуникаций Ofcom будет самостоятельно следить и за распространением информации в интернете[[5]](#footnote-6).

Ofcom не сможет удалять конкретные сообщения из социальных сетей, но потребует от интернет-компаний, таких как Facebook и Google, публиковать заявления, устанавливающие, какой контент и поведение они считают приемлемыми на своих платформах. Задачи медиарегулятора в этой связи заключаются в контроле применения норм последовательности и прозрачности выполнения требований.

Новые правила в первую очередь будут касаться незаконного контента о терроризме и сексуальном насилии над детьми. Также Ofcom будет преследовать распространение информации, которая поощряет нанесение самоувечий или самоубийство. Как отмечается, Ofcom станет следить только за крупными интернет-компаниями. Сайты, которые не позволяют делиться пользовательским контентом, не попадут под регуляцию Ofcom.

Цель работы медиарегулятора будет заключаться в том, чтобы платформы, гарантирующие безопасность для детей, действительно придерживались своих обязательств.

В случае, если владельцы сайта не готовы модерировать контент, они должны заявить об этом пользователям.

**Япония и Сингапур**

В Японии принят специальный законодательный акт, затрагивающий Интернет -«Закон о формировании условий для безопасного пользования интернетом несовершеннолетними» от 2008 года. Им предусматривается запрет на размещение материалов, содержащих подстрекательство к совершению противоправных действий, порнографию, сцены жестокости и насилия. Интернет-ресурсы обязаны оповещать государственную полицию о пользователях, зарегистрировавшихся на сайтах, посвященных пропаганде суицида или нанесению вреда своему здоровью. Все сервисы онлайн-знакомств должны быть зарегистрированы в полиции и обязаны сообщать полиции возраст пользователей и их водительские права/кредитные карты[[6]](#footnote-7).

В Сингапуре принят специальный закон «О защите от ложных действий и манипуляций в Интернете», в рамках которого интернет-компании обязаны маркировать недостоверный контент[[7]](#footnote-8).

Правительство активно применяет данный законодательный акт, в том числе в связи с ситуацией с распространением коронавируса.

В середине февраля сингапурское правительство не менее 4 раз всего за одну неделю применило закон для «выведения на чистую воду» тех, с чьим суждением не согласилось. Государственные органы принудили социальные сети не удалять нежелательные сообщения, но повторять их вместе с правильной версией, то есть, провести показательную работу по исправлению ошибок.

**Европейский Союз**

В Резолюции Европейского Парламента от 15 июня 2017 года «Об онлайн-платформах и едином цифровом рынке» указывается необходимость борьбы онлайн-платформ с незаконным товарооборотом и контентом, а также иными правонарушениями путем применения нормативно-правовых актов наряду с эффективными мерами саморегулирования (т.е. с помощью выработки четких правил пользования их услугами, эффективных механизмов выявления многократных нарушителей или назначением специализированных отделов модерации контента и отслеживания опасных товаров) или гибридных мер».

В сентябре 2017 года Совет Европы призвал крупнейшие интернет-компании разработать новые технологии и инструменты саморегулирования для выявления и пресечения выражения ненависти и террористической пропаганды для своих платформ, что при необходимости будет подкреплено принятием специальных нормативно-правовых актов на уровне Евросоюза.

В 2018 году Европейская комиссия опубликовала Рекомендации по мерам реагирования владельцев интернет-сайтов[[8]](#footnote-9). В частности, от владельцев интернет компаний требуется удалять со своих платформ контент, связанный с терроризмом, в течение одного часа после получения уведомления от правоохранительных органов ЕС, Европола или Управления полиции ЕС. Такая срочность удаления контента объясняется тем, что террористическая пропаганда наиболее опасна в первые часы после ее публикации в сети интернет. Рекомендации применимы ко всем видам незаконного контента, включая терроризм, пропаганду агрессии и ненависти, детскую порнографию, поддельные товары и нарушения права на интеллектуальную собственность, являясь способом взаимодействия внутри отраслей экономики с помощью различных самостоятельных инициатив.

Наряду с требованиями государственных органов о борьбе с противоправным контентом участниками рынка разработан Кодекс по борьбе с дезинформацией в сети интернет[[9]](#footnote-10). Кодекс представляет собой пример саморегулирования и самоограничения интернет-платформ и рекламных ассоциаций. Таким компании как Google, Facebook, Mozilla и Twitter на основе принятого документа опубликовали подробные индивидуальные «дорожные карты», отражающие их планы по усилению мер по борьбе с дезинформацией перед выборами в Европейском Союзе. В частности, каждая из платформ разработала инструменты повышения прозрачности политической рекламы, процедуры ведения архивов, а также специальные процедуры сотрудничества с агентствами проверки публикуемых фактов. Кодекс представляет собой пример саморегулирования и самоограничения Интернет-платформ и рекламных ассоциаций.

В «Рекомендации Европейской Комиссии о мерах эффективного реагирования на нелегальный контент в сети интернет»[[10]](#footnote-11) от 01 марта 2018 года изложены следующие оперативные меры саморегулирования с целью ускоренного обнаружения и удаления незаконного контента в сети интернет, укрепления сотрудничества между организациями и правоохранительными органами, а также повышение прозрачности данной деятельности и правовых гарантий для граждан, в том числе:

- повышение четкости процедур «уведомления и реагирования». Согласно документу, организациям следует утвердить простые и прозрачные правила уведомления о незаконном контенте, включая ускоренные процедуры для надежных осведомителей.

В целях избежание ошибок лица, публикующие контент, должны немедленно информироваться о принятых решениях об удалении информации из сети интернет, а также иметь доступные механизмы оспаривания принятого решения;

- повышение эффективности сетевых инструментов и внедрение проактивных технологий. Предполагается введение и использование системы уведомления пользователей и проактивные инструменты обнаружения и удаления незаконного контента, в частности содержащего подстрекательство к терроризму, и контента, не требующего специальных знаний и экспертизы для признания незаконным, например, материалы о сексуальном насилии над детьми или контрафактные товары;

- создание механизмов дополнительного контроля и обеспечения прав, прежде всего посредством создания компетентных подразделений, отвечающих за оценку и исследование спорных ситуаций;

- взаимодействие с органами власти, через создание институтов коммуникаций и своевременного информирования уполномоченных органов при наличии доказательств тяжкого уголовного преступления или подозрения на угрозу для жизни или безопасности определенного контента организации должны незамедлительно информировать правоохранительные органы.

# Российская Федерация

Согласно данным «Mediascope»[[11]](#footnote-12), весной прошлого года месячная аудитория Рунета достигла 93 миллиона человек, а уже год спустя, по данным «GfK», в январе 2020 года[[12]](#footnote-13) она составила **94,4 миллиона активных пользователей**. Ценовая доступность интернета для россиян одна из лучших в мире — второе место после Украины. В России власти стараются развивать государственные интернет-платформы с разного рода услугами. Всё это показывает особую важность интернета в жизни граждан РФ.

Российское законодательство акцентировано на применении административных мер в сфере пресечения распространения незаконного контент. С 01 января 2012 года действует статья 15.1 Федерального закона от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее - 149-ФЗ) в целях ограничения доступа к сайтам в сети Интернет, содержащим информацию, распространение которой в Российской Федерации запрещено, создается единая автоматизированная информационная система «Единый реестр доменных имен, указателей страниц сайтов в сети Интернет и сетевых адресов, позволяющих идентифицировать сайты в сети Интернет, содержащие информацию, распространение которой в Российской Федерации запрещено». В реестр включаются:

1) доменные имена и (или) указатели страниц сайтов в сети Интернет, содержащих информацию, распространение которой в Российской Федерации запрещено;

2) сетевые адреса, позволяющие идентифицировать сайты в сети Интернет, содержащие информацию, распространение которой в Российской Федерации запрещено.

Создание, формирование и ведение реестра осуществляются Федеральной службой по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

Основаниями для включения в реестр сведений являются:

1) решения уполномоченных Правительством Российской Федерации федеральных органов исполнительной власти, принятые в соответствии с их компетенцией в порядке, установленном Правительством Российской Федерации, в отношении распространяемых посредством сети Интернет:

а) материалов с порнографическими изображениями несовершеннолетних и (или) объявлений о привлечении несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера;

б) 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;

в) информации о способах совершения самоубийства, а также призывов к совершению самоубийства;

г) информации о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), распространение которой запрещено федеральными законами;

ж) информации, направленной на склонение или иное вовлечение несовершеннолетних в совершение противоправных действий, представляющих угрозу для их жизни и (или) здоровья либо для жизни и (или) здоровья иных лиц;

2) решение суда о признании информации, распространяемой посредством сети "Интернет", информацией, распространение которой в Российской Федерации запрещено;

3) постановление судебного пристава-исполнителя об ограничении доступа к информации, распространяемой в сети "Интернет", порочащей честь, достоинство или деловую репутацию гражданина либо деловую репутацию юридического лица.

Согласно постановлению Правительства РФ от 26 октября 2012 г. № 1101, решения об признании информации запрещенной принимаются Роскомнадзором, Роспотребнадзором, МВД России, ФНС России, Росмолодежью. Кроме этого, в судебном порядке может быть признана запрещенной любая информация, распространение которой ограничивается, и (или) если в законе установлен запрет.

По информации представителей Роскомнадзора за период действия Единого реестра принято коло 60 000 судебных решений о признании информации запрещенной.[[13]](#footnote-14) При этом, помимо установленного в статье 15.1. перечня «запрещенной информации» в судах на основании обращений органов прокуратуры Российской Федерации признается запрещенной к распространению следующие виды информации:

- информация о продаже документов (дипломы, медицинские справки, и т.п.);

- информация, пропагандирующая отказ от обязательной вакцинации;

- информация о оказании услуг сексуального характера;

- порнографические материалы;

- информация о жестоком обращении с животными;

- реклама и (или) продажа алкогольной продукции, «санкционных» товаров;

- рекомендации по уходу от уплаты налогов и иных обязательств;

- сведения о продаже контрафактной продукции;

- рекомендации по злоупотреблениям при пользовании услугами жилищно-коммунального хозяйства, а также электропотреблении;

- рекомендации по отказу от службы в армии;

- информации об общественно опасном поведении и поведении представляющим угрозу жизни и здоровью граждан – «зацепинг», «руффинг»;

- сведения и сайты содержащие персональные данные граждан, обрабатываемые незаконно;

- и другие.

В целом перечень такой информации является открытым. При этом на практике развиваются две тенденции:

1. постоянное появление инициатив, связанных с расширением перечня оснований для признания информации запрещенной во внесудебном порядке и увеличении числа органов, уполномоченных принимать такие решения;
2. расширение спектра информации, признаваемой запрещенной в судебном порядке.

Кроме этого, отдельные виды информации «блокируются» на основании решений Генерального прокурора и его заместителей, а также в судебном порядке на основании определений о предварительных обеспечительных мерах.

Как следует из части 1 статьи 15.1.1. 149-ФЗ в случае обнаружения в информационно-телекоммуникационных сетях, в том числе в сети "Интернет", информации, выражающей в неприличной форме, которая оскорбляет человеческое достоинство и общественную нравственность, явное неуважение к обществу, государству, официальным государственным символам Российской Федерации, Конституции Российской Федерации или органам, осуществляющим государственную власть в Российской Федерации, Генеральный прокурор Российской Федерации или его заместители обращаются в Роскомнадзор, с требованием о принятии мер по удалению указанной информации и по ограничению доступа к информационным ресурсам, распространяющим указанную информацию, в случае ее не удаления.

В соответствии с частью 1 статьи 15.3. 149-ФЗ в случае обнаружения в информационно-телекоммуникационных сетях, в том числе в сети "Интернет", информации, содержащей призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка, недостоверной общественно значимой информации, распространяемой под видом достоверных сообщений, которая создает угрозу причинения вреда жизни и (или) здоровью граждан, имуществу, угрозу массового нарушения общественного порядка и (или) общественной безопасности либо угрозу создания помех функционированию или прекращения функционирования объектов жизнеобеспечения, транспортной или социальной инфраструктуры, кредитных организаций, объектов энергетики, промышленности или связи, информационных материалов иностранной или международной неправительственной организации, деятельность которой признана нежелательной на территории Российской Федерации в соответствии с Федеральным законом от 28 декабря 2012 года N 272-ФЗ "О мерах воздействия на лиц, причастных к нарушениям основополагающих прав и свобод человека, прав и свобод граждан Российской Федерации", сведений, позволяющих получить доступ к указанным информации или материалам, включая случай поступления уведомления о распространяемой с нарушением закона информации от федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, организаций или граждан, Генеральный прокурор Российской Федерации или его заместители обращаются Роскомнадзор, с требованием о принятии мер по ограничению доступа к информационным ресурсам, распространяющим такую информацию.

Согласно части 1 статьи 15.5. 149-ФЗ в целях ограничения доступа к информации в сети "Интернет", обрабатываемой с нарушением законодательства Российской Федерации в области персональных данных, создается автоматизированная информационная система "Реестр нарушителей прав субъектов персональных данных».

Необходимо отметить, что по данным доклада Правозащитная группа «Агора» и общественная организация «РосКомСвобода»[[14]](#footnote-15) если количество случаев ограничения доступа к интернет-ресурсам резко сократилось (с 488 609 случаев до 161 490, авторы исследования объясняют это прежде всего снижением активности преследования властями мессенджера Telegram), то число запретов информации государственными органами неуклонно растет. С 2016 года число таких запретов выросло более чем в 10 раз, с 24 000 до 272 875, при этом «попутной» блокировке подвергается более 4,74 млн интернет-ресурсов, говорится в докладе.

Таким образом, весьма широкий перечень государственных органов и оснований признания информации, запрещенной к распространению, характеризуют российскую модель регулирования отношений в сети Интернет как административную, с ярко выраженным приматом государственного вмешательства.

При этом данный подход не может эффективно функционировать в отношении контента, который генерируется с применением технических средств, например, deepfake, представляющую собой методику синтеза изображения, основанную на искусственном интеллекте. Она используется для соединения и наложения существующих изображений и видео на исходные изображения или видеоролики. Данная технология может использоваться для создания порнороликов с «участием» лица, чье изображение накладывается на исходный видеоряд; она может использоваться для создания фейковых новостей и компрометирующих материалов, а также для совершения мошеннических действий. Специалисты Агентства по передовым исследовательским проектам США (DARPA) выразили озабоченность данной технологией и заявили о возможной угрозе для национальной безопасности от ее широкомасштабного использования[[15]](#footnote-16). Для выявления такого контента необходимо использование специализированного программного обеспечения. Использование судебной процедуры с ее громоздкостью и издержками в данном случае не всегда эффективно. В связи с этим необходима выработка новых подходов к модерированию такого контента.

**Китайская народная республика, Египет, Турция, Венесуэла**

В мировой практике встречаются и более «радикальные» подходы к решению проблемы обеспечения безопасности интернет-пространства.

Китаю удалось обеспечить функционирование масштабной системы безопасности интернет-пространства, предъявляющей высокие требования к обеспечению сохранности персональной информации пользователей и позволяющей обеспечить оперативное реагирование на сетевые угрозы безопасности граждан и государства.

В соответствии с законодательством Китая операторы сети, оказывающие услуги по предоставлению доступа пользователей к сети и регистрации доменных имён для них, а также организации, оказывающие услуги по предоставлению доступа к стационарной или мобильной телефонной сети, либо оказывающие пользователям услуги, связанные с публикацией информации или обменом мгновенными сообщениями, должны требовать от пользователей предоставления реальной идентифицирующей их информации при подписании договоров с пользователями или подтверждении факта предоставления услуг [[16]](#footnote-17).

Законодательство Китая также позволяет обеспечить экстренное реагирование на локализованную деятельность организованной преступности путём принятия временных мер в отношении сетевых коммуникаций в специально обозначенных регионах. Такие меры могут выражаться, к примеру, в ограничении передачи сообщений между пользователями. Законом о кибербезопасности Китая предусмотрено, что соответствующие меры могут применяться для обеспечения защиты национальной безопасности и общественного порядка, а также для предотвращения ситуаций, представляющих серьёзную общественную опасность.

В начале года в Китае в силу вступил закон, согласно которому граждане страны обязаны публиковать в сети лишь позитивный контент.[[17]](#footnote-18) В случае публикации негативных сообщений, которые могут “угрожать национальной безопасности”, пользователей будут судить. При этом новый закон умудряется разделять абсолютно любой тип онлайн-контента на три основные группы: «поощряемый», «негативный» и «незаконный».

В Египте предусматривается возможность блокирования личных аккаунтов в социальных сетях и блогов, охватывающих аудиторию в размере от пяти тысяч человек, в случае распространения на таких интернет-страницах недостоверной информации[[18]](#footnote-19).

В Турции компании обязаны по запросу удалять нелегальный контент, который был признан таковым Управлением телекоммуникаций и связи (Telecommunications Communication Presidency). По запросу регулятора также может временно приостанавливаться работа интернет-сайтов и сервисов обмена сообщениями, как это имело место в случаях с такими ресурсами, как YouTube, Facebook и Twitter.

В Венесуэле в отношении сетевых сервисов, которые не удаляют в течение шести часов после запроса сообщения, содержащие оскорбления на национальной, расовой, религиозной, политической или иной почве, могут быть применены штрафы и блокировки.[[19]](#footnote-20)

1. **Добровольные меры, предпринимаемые интернет ресурсами по саморегулированию контента**

Следует отметить, что все крупные ресурсы уже разработали и применяют алгоритмы противодействия распространению недопустимой информации, определили процедуры ее выявления, рассмотрения обращений пользователей и реагирования на сообщения.

Компании Facebook, Microsoft, Twitter, YouTube, Instagram, Google+ и Snapchat подписали в 2016 году Европейские правила оказания услуг при поддержке Европейской Комиссии, включающие борьбу с незаконным выражением ненависти в сети интернет, заставляя партнерские платформы применять на практике четкие и эффективные процессы обработки жалоб на данные нарушения и удалять их или блокировать к ним доступ.

В июне 2017 года эти и ряд других организаций сформировали Глобальный антитеррористический Интернет-форум (Global Internet Forum to Counter Terrorism - (GIFCT)[[20]](#footnote-21), отслеживающий и удаляющий из сети интернет контент, содержащий насилие и терроризм, при помощи метода индексации изображений по типу отпечатков пальцев.

YouTube и Facebook начали публиковать регулярные отчеты транспарентности, указывая объем удаленного незаконного контента.

Facebook анонсировал планы привлечь более 30 000 сотрудников для обработки контента, а также создание специального надзорного совета для обжалования решений по контенту[[21]](#footnote-22). Facebook планирует создать независимый надзорный совет, благодаря которому пользователи смогут обжаловать решения социальной сети о размещаемом ими контенте[[22]](#footnote-23).Кроме этого, компания выступила с призывом к государственным органам законодательно закрепить принципы регулирования отношений в сети интернет. В части политического контента, а также противодействия использованию социальной платформы в противоправных целях было принято решение об ограничении использования социальной сети Facebook для продвижения проектов, связанных с криптовалютами. Администрация сети запретила любую рекламу данной и связанной с этим деятельности. Также следует отметить, что Facebook продолжает бороться с паническими сообщениями или фейковыми новостями о коронавирусе, поэтому запретил рекламу, в которой обещают вылечить или защитить от коронавируса.[[23]](#footnote-24)

Google продолжает инвестировать в автоматизированные технологии удаления контента и одновременно повышает число модераторов YouTube до 10 000 человек и более.

Борьба провайдеров интернет-услуг с дезинформацией включает установку функционала, отбирающего наиболее надежные источники новостей и данных, например, маркировка безопасности или кайтмаркинг (kitemarking)[[24]](#footnote-25), а также обращение к независимым фактчекерам и анализ уведомлений надежных пользователей, активный перехват манипулятивных или мошеннических действий (например, поддельные аккаунты и их кластеры) и более серьезный анализ наиболее популярной и часто просматриваемой информации на предмет ее достоверности.

Instagram в конце 2018 года изменил свои внутренние правила[[25]](#footnote-26), добавив меры по пресечению показов пользователям рекомендаций к просмотру контента, склоняющего к самоубийству, включая изображения, хештеги, аккаунты и подсказки набора. Также перед просмотром видео пользователь будет видеть экран предупреждения о суицидном контенте и размытое изображение нанесения человеком самоувечий, при этом данное видео все равно будет доступно для просмотра и выражения сочувствия его автору, но этот контент уже не будет индексироваться и выходить в результатах поиска, хештегов и рекомендациях.

Компания Twitter планирует ввести специальную маркировку для постов политиков и общественных деятелей, чьи публикации содержат ложную информацию[[26]](#footnote-27). Так посты, содержащие такую информацию, будут выделены ярко-оранжевым цветом. На нем также будет пометка «вреден и вводит в заблуждение». Любой пользователь Twitter сможет оценить правдоподобность информации, размещенной на платформе.

Для этого будет необходимо ответить на 3 вопроса:

* является ли контент потенциально лживым,
* сколько людей из 100 возможных ответили бы так же,
* почему содержимое поста кажется пользователю неправдоподобным.

Если пост будет признан недостоверным, он будет отмечен оранжевым цветом и количество его показов в ленте новостей будет сокращено.

Кроме того, Twitter объявил о планах маркировать медиаконтент, который платформа посчитает «синтетическим или сфабрикованным». К такому контенту относятся «дипфейки» и отредактированные снимки. Для отнесения постов с такими материалами к «синтетическим или сфабрикованным» будет выясняться, пытался ли автор таким образом обмануть своих подписчиков, заставить их поверить в несуществующее событие. После этого будет проводиться анализ того, какую общественную опасность несет такой пост. Эти правила вступят в силу с 05 марта 2020 года. Уточняется, что Twitter может также ввести систему поощрения пользователей через начисление баллов за информацию о фейковых постах, поскольку они «помогают людям понять ту информацию, которую они видят».

Новостной сайт Reddit обновил свою политику в отношении использования чужих данных, позволяющее выдавать себя за другое лицо. Новые правила запрещают не только распространение видео, созданных с помощью технологии «дипфейк», но и введение в заблуждение (выдача себя за иное лицо). Такой контент удаляется, а пользователь блокируется**[[27]](#footnote-28)**.

В качестве примера онлайн-контента, где сложились механизмы саморегулирования при его модерировании, можно привести онлайн-рекомендации и отзывы пользователей в отношении товаров и услуг, которые имеют особое значение в цифровой экономике. Основатель сети *Facebook* Марк Цукерберг утверждает, что «ничто так не влияет не людей, как рекомендации их друзей. Рекомендация, которой доверяют, влияет на людей в гораздо большей степени, чем самые искусно подготовленные сообщения, распространяемые в СМИ. Надежная рекомендация – Святой Грааль маркетинга»[[28]](#footnote-29). В основе новых бизнес-моделей экономики «совместного использования» лежат репутационные механизмы: одни пользователи дают другим пользователям рекомендации, на основе которых коммерчески значимые решения принимают иные лица. Причем такого рода решения могут порой иметь непосредственное влияние на жизнь и здоровье людей. Например, как это имеет место в случае с рекомендациями и основанными на них рейтингами водителя такси в сервисах типа *Uber*, владельца жилого помещения в сервисах типа *Airbnb* и т.п. Вот почему вопросы, связанные с достоверностью таких рекомендаций и отсутствием манипуляций с ними, приобретают важное значение не только для поддержания доверия в электронной коммерции сети «Интернет», но и для защиты жизни, здоровья и имущества потребителей.

Возможные злоупотребления, связанные с рекомендациями и отзывами на товары в Интернете, можно разделить на две большие группы:

1) наличие информации, не соответствующей действительности;

2) подготовка отзывов и рекомендаций по заказу производителей или продавцов товара, что может влечь их необъективность и тем самым – введение в заблуждение потребителей и недобросовестную конкуренцию.

Большие проблемы создают некоторые онлайн-платформы (типа *Fiverr, Kwork, Amazon Mechanical Turk*), позволяющие нанять фрилансеров для проставления «лайков», составления отзывов или распространения от своего имени заранее подготовленных отзывов и совершения иных действий под видом рядовых пользователей[[29]](#footnote-30).

Руководящие указания по отзывам и рекомендациям, оставляемым онлайн (*Online Reviews and Endorsements Guidances*), подготовленные Международной сетью по защите потребителей и контролю за соблюдением законодательства в этой области (*International Consumer Protection and Enforcement Network, ICPEN*). Данные документы адресованы трем ключевым категориям лиц, влияющих на характер и содержание отзывов и рекомендаций: администратором отзывов[[30]](#footnote-31), продавцам товаров (услуг)[[31]](#footnote-32) и «лидерам мнений»[[32]](#footnote-33).

Данные принципы нашли свое отражение в политиках ряда интернет-ресурсов (например, Amazon) и в определенной степени находят свое отражение в судебной практике европейских стран. Например, в одном из решений Верховный Суд Германии указал на наличие обязанности владельца медицинского портала осуществлять мониторинг отзывов, оставляемых посетителями. Особенно это касается оставляемых анонимно отзывов, в отношении которых поступили жалобы от врачей или из клиник относительно их недостоверности[[33]](#footnote-34). По сути такого рода требования фактически вынуждают владельцев интернет-портала внедрять специальные политики модерирования отзывов и управления поступающими жалобами, в некоторой степени схожие с теми, которые обеспечивают претензионный порядок в отношениях, связанных с защитой исключительных прав. В рекомендациях ОЭСР по защите прав потребителей в сфере электронной коммерции содержатся специальные положения, устанавливающие необходимость обеспечения интернет-ресурсами достоверности одобрительных комментариев других лиц, содержащихся в рекламе, а также недопустимость ограничений по оставлению негативных отзывов. При этом наличие любой существенной связи между блогером или иным пользователем сети «Интернет», оставившим соответствующий отзыв, которая может повлиять на объективность и восприятие отзыва, должно быть в явной форме раскрыто[[34]](#footnote-35).

Вместе с тем, несмотря на значительное государственное влияние, следует отметить и отдельные немногочисленные примеры эффективного саморегулирования имеются в России. С 01 ноября 2018 года по настоящее время действует Меморандум о защите авторских прав в интернете[[35]](#footnote-36) Его участниками являются представители 12 крупнейших компаний-производителей кино- и телепродукции, и российских интернет-площадок. В их числе «Первый канал», «ВГТРК», «СТС Медиа», «Газпром-Медиа Холдинг», «Национальная Медиа Группа», Ассоциация продюсеров кино и телевидения, Ассоциация по стимулированию оборота легального контента в сети интернет «Интернет-видео», «Яндекс», «Мэйл.Ру» («Одноклассники» и «ВКонтакте»), «Рамблер Интернет Холдинг», «Руформ» и «Кинопоиск». Меморандум заложил основы отраслевого саморегулирования в рамках в целях противодействия нелегальному распространению аудиовизуальных произведений в сети интернет. Документ ввел досудебный порядок разрешения спорных вопросов между правообладателями и поисковыми системами по поводу незаконного размещения ссылок на пиратский контент.

В декабре 2019 года отраслевым сообществом был подписан Кодекс этики при обработке данных[[36]](#footnote-37). Кодекс разработан участниками рынка данных совместно с государством и представителями общественности и представляет собой свод отраслевых стандартов профессионального и **этического** поведения, которые участники, действуя добросовестно и разумно, добровольно признают и обязуются исполнять.

Проблематика размещения противоправного контента лежит также и в уголовно правовой плоскости. Например, в УК РФ (ч. 2 ст. 205.2; п. «д» ч.3 ст. 110.1) существует ответственность для физлиц за публичные призывы к терроризму и самоубийствам. Кроме того, в последние годы неоднократно становились резонансными ситуации, в которых пользователи социальных сетей привлекались к уголовной ответственности за то, что добавляли на свои персональные страницы, ранее размещенные другими пользователями материалы, противоречащие законодательству.

По данным доклада Правозащитной группы «Агора» и общественная организация «РосКомСвобода»[[37]](#footnote-38):

* приговоры к лишению свободы за действия в интернете в течение 2019 года вынесли суды 18 субъектов Федерации (Амурской, Белгородской, Владимирской, Вологодской, Кемеровской, Курской, Магаданской, Новосибирской, Оренбургской, Ростовской, Самарской, Свердловской, Томской, Челябинской областей, Москвы, Ингушетии, Пермского и Хабаровского краях), а также в Крыму.
* Количество регионов в «зеленой» зоне пятый год подряд сокращается. В 2019 году — почти на треть по сравнению с 2018 (с 14 до 10). Таким образом, в прошедшем периоде только Чукотский автономный округ, Еврейская автономная область, Сахалинская и Рязанская области, Камчатский край, республики Хакасия, Тыва, Коми, Карачаево-Черкесия и Калмыкия оставались относительно свободными.
* С 2015 года девять субъектов федерации (Иркутская, Московская, Омская, Саратовская области, Санкт-Петербург и Москва, Алтайский, Краснодарский и Приморский края), а также Крымский полуостров ни разу не покидали «красную» зону.
* Среди госведомств абсолютным лидером по количеству наложенных запретов [оказалась](https://reestr.rublacklist.net/visual/) Федеральная налоговая служба (ФНС), которая отвечает за блокировку онлайн-казино, – на ее долю приходится 34,8% всех блокировок. На втором месте Генпрокуратура (32,4%), на третьем – суды (16%).

Примечательно то, что во многих подобных уголовных делах общественностью и правозащитниками обосновано поднимался вопрос об отсутствии умысла на совершение противоправных деяний у лиц, в отношении которых возбуждались так называемые «дела о репостах».

Вероятно, что спорных ситуаций с уголовными делами на тот момент можно было избежать, если бы законодательство предусматривало наличие превентивных мер в виде обязанности интернет-ресурсов самостоятельно создавать и поддерживать механизмы оценки контента на предмет соответствия законодательству и, в случае выявления противоречащих законодательству публикаций, своевременно удалять их в целях недопущения дальнейшего распространения. При этом данный подход не исключает возможности сообщения о фактах размещения соответствующих материалов в надзорные и правоохранительные органы для принятия последующих решений.

1. **Выводы и рекомендации**

Вопросы взаимодействия государства и субъектов цифровой среды при обороте незаконного контента, недостоверной информации требуют пересмотра сложившихся подходов, применяемых к аналоговой среде.

В России уже присутствует достаточно детальное законодательное регулирование вопросов, связанных с основаниями и порядком ограничения доступа к информации, распространяемой в сети Интернет. Данные механизмы в целом доказали свою работоспособность. Однако на практике появляются новые виды противоправного контента, выявление и оперативное удаление которого требует наличия особой технологической оснастки. Кроме того, некоторые виды противоправного контента (например, фейковые и заказные отзывы о товарах и услугах, вводящие в заблуждение потребителей или представляющие собой недобросовестную конкуренцию) не охватываются существующим законодательным регулированием.

В этой связи видится целесообразным рассмотрение возможности возложения на интернет-ресурсы общих обязанностей по выявлению и удалению такого контента, на основании правил и критериев, которые будут выработаны сообществами таких интернет-ресурсов на основании общих принципов, которые необходимо будет предусмотреть в законодательстве. Законодательное регулирование такого «саморегулирования» необходимо для обеспечения баланса интересов пользователей, государства и бизнеса, поскольку в отсутствие такого сбалансированного регулирования существует риск того, что интернет-ресурсы как коммерческие организации будут в любой спорной ситуации склоняться к удалению контента для минимизации своих финансовых и репутационных рисков, что может повлечь неоправданное и непропорциональное ограничение конституционных прав на свободу выражения мнений, поиск и распространение информации. Законодательные принципы саморегулирования в области модерирования контента в сети Интернет, помимо прочего, должны содержать положения о порядке обжалования решений интернет-ресурсов об удалении контента, требования к комиссиям и личностям лиц, вовлеченных в процесс модерирования, механизмы разрешения возможного конфликта интересов между различными интернет-ресурсами при модерирования контента и обеспечения единообразия подходов, механизмы поощрений интернет-ресурсов за участие в системе саморегулирования и общие подходы к санкциям за несоблюдение принятых правил саморегулирования.

При решении вопроса о возможном месте саморегулирования контента в общей системе регулирования контента в Российской Федерации, видится перспективным разделение всего контента на две группы:

1) контент, имеющий социальное происхождение (например, выражающая переживания или мнение лица по определенному вопросу)

2) контент, который порожден технологией и носит преимущественно "искусственный" характер (например, изображение или голос лица, сгенерированные с помощью технологий, подобных DeepFake).

Первая группа контента, являясь в ряде случаев реализацией конституционных прав на свободу слова и распространения информации, требует взвешенного и сбалансированного подхода при принятии решения о блокировке, в связи с чем должен быть судебный контроль за такого рода вопросами. Саморегулирование здесь если и возможно, то преимущественно в тех случаях, по результатам тщательного анализа сложившейся практики и вывода о том, что по каким-то причинам не срабатывают существующие механизмы. Иными словами, саморегулирование не должно подменять и ужесточать существующие законодательные механизмы ограничения доступа к информации. Вторая группа контента будет становиться все более распространенной в ближайшие годы и требует оперативного ответа преимущественно техническими средствами (принцип "проблема, порожденная технологией, должна решаться, в первую очередь, самой технологией"). Такими техническими средствами, в том числе, алгоритмами, выявляющими такой контент, обладают преимущественно участники рынка, поэтому у них больше возможностей ограничивать его распространение более оперативно и эффективно, чем у госорганов и суда. Поэтому здесь складывается благоприятная среда для обсуждения перспектив саморегулирования при ограничении доступа к такому контенту.

Федеральный закон от 01.12.2007 N 315-ФЗ «О саморегулируемых организациях» хоть и допускает возможности отраслевого саморегулирования, но вместе с тем в существующей редакции вероятно не будет иметь эффективного правоприменения для рассматриваемых целей и задач. С учетом изложенного, а также в силу трансграничности предоставляемых владельцами информационных ресурсов услуг, его применения для регулирования этой отрасли на данном этапе представляется невозможным. Как следствие, если вводить в законодательство дополнительные механизмы саморегулирования в области ограничения доступа к определенным видам контента в сети интернет (с учетом соображений, высказанных ранее), необходимо будет их дистанцировать от вышеуказанного федерального закона и предусмотреть особый правовой режим такого саморегулирования, возможно, с созданием специальной терминологии для него, не пересекающейся с упоминаемой в ФЗ «О саморегулируемых организациях».

В РФ отсутствует системный и единообразный подход к реагированию владельцев интернет-площадок на жалобы пользователей и обращения уполномоченных органов. Каждая из предоставляющих услуги платформ самостоятельно оценивает опасность контента, устанавливает формы, процедуры и сроки рассмотрения обращений пользователей, разрабатывает индивидуальные системы отчетности.

В связи с чем, как представляется, целесообразным рассмотреть правовые решения, направленные на создание общего стандарта взаимодействия площадок с интернет-пользователями, закрепления минимального набора административных и организационных мер, программно-аппаратных средств противодействия распространению информации с нарушением закона.

Так, владельцы интернет-сайтов, на которых размещается пользовательский контент могут обеспечивать:

а) размещение на сайте политики противодействия распространению информации с нарушением закона, а также электронной формы для приема обращений о распространении информации с нарушением закона;

б) публикацию на сайте в сети интернет отчетов о результатах применения административных и организационных мер, программно-аппаратных средств противодействия распространению информации с нарушением закона.

Если рассматривать возможность устанавливать перечень возможных административных и организационных мер, программно-аппаратных средств противодействия распространению информации с нарушением закона вероятно следует устанавливать актом Роскомнадзор и обновлять с учетом возникающих вызов или угроз, а также технологических возможностей компаний.

Специфическими административными и организационными мерами саморегулирования в сети интернет, например, могут стать:

1. использование владельцем информационного ресурса программного обеспечения для срочного рассмотрения обращений пользователей в течение установленного периода;
2. наличие в штате персонала, обладающего соответствующими квалификациями (разработчики фильтрационного ПО, администраторы Интернет-сервисов по фильтрации вредоносного контента с опытом работы, администраторы, квалифицированные для выполнения работы по фильтрации вредоносного контента; специалисты по работе с потребителями, ответственные за защиту несовершеннолетних);
3. установление на уровне локальных актов организации норм и правил, регулирующие проведение аналитики контента, взаимодействие подразделений, возможные санкции и порядок обжалования решений по запросу локальных организаций по защите молодежи;
4. организация работы с жалобами на незаконный или нежелательный контент (в том числе, к порядку их подачи, рассмотрения, реагирования, апелляции вынесенных решений. Например, должны быть разработаны требования к аффилированным социальным сетям о порядке направления жалоб и обращений и предоставлена возможность пересмотра решений.

5) соответствие экспертов определенным требованиям: эксперты должны обладать необходимыми знаниями, быть независимыми и компетентными;

К дополнительным мерам, которые могут реализовываться крупными компаниями могут быть отнесены следующие:

- мониторинг контента;

- принятие эффективных мер воздействия и пресечение в случае выявления нарушений закона. Владельцы ресурсов обязаны незамедлительно реагировать на жалобы и обращения, а также информировать уполномоченные органы о нарушениях или подозрительном поведении.

- построение системы подотчетности перед общественностью, публикаций отчетов о своей деятельности, в которых должны отражаться текущие меры борьбы компании с угрозами вредоносного контента на своих платформах, включая принятые меры и их эффективность;

- проведение обучения и просвещения населения в вопросах безопасного пользования сетью Интернет, выстраивание взаимодействия с пользователями.

С учетом фактически осуществляемой работы интернет-компаний по противодействию распространению контента, сложившейся зарубежной практики, целесообразно принятие законодательных решений направленных на установление единых минимальных правил (стандартов) взаимодействия площадок, предоставляющих возможности распространения пользовательского контента с пользователями и государственными органами, с целью минимизации взаимных издержек, содействия распространению информации в сети интернет, развитию информационной инфраструктуры. При этом законодательные решения должны стимулировать компании к большей открытости собственных процедур, постоянной публичной отчетности, а также совершенствованию методов борьбы с противоправным контентом.

С учетом того, что все крупные ресурсы уже разработали алгоритмы противодействия распространению недопустимой информации, определили процедуры ее выявления, рассмотрения обращений пользователей и реагирования на сообщения, реализация инициативы не повлечет для них дополнительных расходов или административных издержек, при этом обеспечит больший уровень доверия и социальной ответственности отрасли.

Таким образом, с одной стороны, удастся законодательно закрепить институт социальной ответственности владельцев информационных ресурсов, соответствующий их роли в современном мире, а с другой существенно расширить спектр возможных мер, направленных на предупреждение нарушений в сети интернет.

Кроме того, представляется целесообразным внести изменения в законодательство Российской Федерации, предусмотрев обязательное направление органами прокуратуры владельцу интернет-ресурса предостережения о недопустимости нарушения закона до выхода в суд с административным иском о блокировке такого интернет-ресурса в случае размещения на нем информации, противоречащей законодательству Российской Федерации. Введение подобного досудебного порядка, аналогичного действующему в гражданском и арбитражном исковых процессах, позволит снизить судебную нагрузку и усилить состояние прокурорского надзора в информационно-телекоммуникационной сфере. Вместе с данной мерой следуете рассмотреть вопрос о дальнейшем смягчении механизма привлечения к уголовной ответственности (через административную) за размещение информации в сети интернет, поскольку после декриминализации ч. 1 ст. 282 УК РФ появилась практика привлечения граждан за аналогичные действия к ответственности по статьям 205.2 (публичное оправдание терроризма), 319 (оскорбление представителей власти).

\*\*\*\*\*

*Координатор работы Комиссии* – Журавлев Александр Викторович, председатель Комиссии, управляющий партнер юридической компании «ЭБР».

*Куратор аналитической работы* – Едидин Борис Александрович – член Комиссии, к.ю.н., заместитель генерального директора по правовым вопросам Института развития интернета (ИРИ).

**Докладчики и эксперты, чьи материалы использованы при подготовке настоящего заключения:**

1. Дупан Анна Сергеевна - директор Института проблем правового регулирования НИУ ВШЭ

2. Липин Дмитрий Александрович, заместитель исполнительного директора-руководителя Аппарата Ассоциации юристов России.

3. Савельев Александр Иванович – заместитель председателя Комиссии, к.ю.н., доцент кафедры информационного права, старший научный сотрудник НИУ ВШЭ

4. Орехович Александра Владимировна – Член комиссии, директор по правовым инициативам Фонда развития интернет-инициатив (ФРИИ).

5. Гультяева Елена Викторовна – член Комиссии, вице-президент, руководитель правового комитета РАКИБ;

6. Лавренков Павел Алексеевич – член Комиссии, управляющий директор Юридического департамента АО «Группа «Ренессанс Страхование»;

7. Ларенс Екатерина Валериевна – член Комиссии, Старший юрист DLA Piper (Австрия).

|  |  |
| --- | --- |
| **Председатель Комиссии** | **А.В. Журавлев** |

1. [*https://www.bbc.com/russian/features-49168586*](https://www.bbc.com/russian/features-49168586) [↑](#footnote-ref-2)
2. [*https://www.rbc.ru/trends/industry/5de101619a79474a179f16db*](https://www.rbc.ru/trends/industry/5de101619a79474a179f16db) [↑](#footnote-ref-3)
3. [*https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG\_engl.pdf?\_\_blob=publicationFile&v=2*](https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf?__blob=publicationFile&v=2) [↑](#footnote-ref-4)
4. [*https://www.gov.uk/government/consultations/online-harms-white-paper*](https://www.gov.uk/government/consultations/online-harms-white-paper) [↑](#footnote-ref-5)
5. [*https://www.theguardian.com/media/2020/feb/12/ofcom-to-be-put-in-charge-of-regulating-internet-in-uk*](https://www.theguardian.com/media/2020/feb/12/ofcom-to-be-put-in-charge-of-regulating-internet-in-uk) [↑](#footnote-ref-6)
6. *Act on regulation on soliciting children by using opposite sex introducing service on internet, Act №83 2003.* [↑](#footnote-ref-7)
7. [*https://sso.agc.gov.sg/Acts-Supp/18-2019/Published/20190625?DocDate=20190625*](https://sso.agc.gov.sg/Acts-Supp/18-2019/Published/20190625?DocDate=20190625) [↑](#footnote-ref-8)
8. [*https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-measures-effectively-tackle-illegal-content-online*](https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-measures-effectively-tackle-illegal-content-online) [↑](#footnote-ref-9)
9. [*https://ec.europa.eu/commission/presscorner/detail/en/IP\_18\_3370*](https://ec.europa.eu/commission/presscorner/detail/en/IP_18_3370) [↑](#footnote-ref-10)
10. [*https://ec.europa.eu/commission/presscorner/detail/en/IP\_17\_3493*](https://ec.europa.eu/commission/presscorner/detail/en/IP_17_3493) [↑](#footnote-ref-11)
11. [*https://tass.ru/obschestvo/6344930*](https://tass.ru/obschestvo/6344930) [↑](#footnote-ref-12)
12. [*http://www.comnews.ru/content/203868/2020-01-13/2020-w03/prirost-internet-auditorii-2019-godu-obespechili-pensionery*](http://www.comnews.ru/content/203868/2020-01-13/2020-w03/prirost-internet-auditorii-2019-godu-obespechili-pensionery) [↑](#footnote-ref-13)
13. [*https://rkn.gov.ru/plan-and-reports/reports/p449/*](https://rkn.gov.ru/plan-and-reports/reports/p449/) [↑](#footnote-ref-14)
14. [*https://roskomsvoboda.org/55136/*](https://roskomsvoboda.org/55136/) [↑](#footnote-ref-15)
15. *Experts fear face swapping tech could start an international showdown. Video forensic specialists are worried Deepfakes could have national security repercussions.* [*https://theoutline.com/post/3179/deepfake-videos-are-freaking-experts-out?zd=1&zi=4odcqwza*](https://theoutline.com/post/3179/deepfake-videos-are-freaking-experts-out?zd=1&zi=4odcqwza) [↑](#footnote-ref-16)
16. *статья 24 Закона о кибербезопасности Китая (также****Закон****об интернет-безопасности КНР)* [↑](#footnote-ref-17)
17. [*https://www.chinalawtranslate.com/en/governing-the-e-cosystem-2/*](https://www.chinalawtranslate.com/en/governing-the-e-cosystem-2/) [↑](#footnote-ref-18)
18. *Закон «О регулировании прессы и средств массовой информации»* [↑](#footnote-ref-19)
19. *Law Against Hatred, for Tolerance and Peaceful Coexistence* [↑](#footnote-ref-20)
20. [*https://gifct.org/about*](https://gifct.org/about) [↑](#footnote-ref-21)
21. [*https://tass.ru/obschestvo/7784687*](https://tass.ru/obschestvo/7784687) [↑](#footnote-ref-22)
22. [*https://about.fb.com/wp-content/uploads/2020/02/Charting-A-Way-Forward\_Online-Content-Regulation-White-Paper-1.pdf*](https://about.fb.com/wp-content/uploads/2020/02/Charting-A-Way-Forward_Online-Content-Regulation-White-Paper-1.pdf) [↑](#footnote-ref-23)
23. [*https://www.businessinsider.com/facebook-corona-virus-cracks-down-ads-2020-2*](https://www.businessinsider.com/facebook-corona-virus-cracks-down-ads-2020-2) [↑](#footnote-ref-24)
24. [*https://rg.ru/2018/12/05/roskomnadzor-predlozhil-vvesti-markirovku-kontenta-dlia-malyshej.html*](https://rg.ru/2018/12/05/roskomnadzor-predlozhil-vvesti-markirovku-kontenta-dlia-malyshej.html) [↑](#footnote-ref-25)
25. [*https://www.bbc.com/russian/features-48293907*](https://www.bbc.com/russian/features-48293907) [↑](#footnote-ref-26)
26. [*https://www.kommersant.ru/doc/4261726*](https://www.kommersant.ru/doc/4261726) [↑](#footnote-ref-27)
27. [*https://www.theverge.com/2020/1/9/21058803/reddit-account-ban-impersonation-policy-deepfakes-satire-rules*](https://www.theverge.com/2020/1/9/21058803/reddit-account-ban-impersonation-policy-deepfakes-satire-rules) [↑](#footnote-ref-28)
28. *http://www.azquotes.com/quote/678720* [↑](#footnote-ref-29)
29. *Распространение подобных сервисов, предоставляемых в массовом порядке живыми людьми, повлекла возникновение феномена «Human-as-a-Service» (человек-как-услуга). Те микрозадания, с которыми пока не справляются компьютерные алгоритмы, успешно сдаются на аутсорсинг (а точнее – краудсорсинг) людям. См.: Prassl J. Humans as a Service: The Promise and Perils of Work in the Gig Economy. Oxford University Press, 2018.* [↑](#footnote-ref-30)
30. *Online Reviews and Endorsements: ICPEN Guidelines for Review Administrators, June 2016.*  [↑](#footnote-ref-31)
31. *Online Reviews and Endorsements: ICPEN Guidelines for Traders and Marketing Professionals, June 2016.* [↑](#footnote-ref-32)
32. *Online Reviews and Endorsements: ICPEN Guidelines for Digital Influencers, June 2016.* [↑](#footnote-ref-33)
33. *BGH, Urteil No. VI ZR 34/15, 1 March 2016.* [↑](#footnote-ref-34)
34. *См. § 12, 17 Consumer Protection in E-commerce: OECD Recommendation. 2016. Paris.* [↑](#footnote-ref-35)
35. [*https://rkn.gov.ru/*](https://rkn.gov.ru/) [↑](#footnote-ref-36)
36. [*https://ac.gov.ru/files/content/25949/kodeks-etiki-pdf.pdf*](https://ac.gov.ru/files/content/25949/kodeks-etiki-pdf.pdf) [↑](#footnote-ref-37)
37. [*https://roskomsvoboda.org/55136/*](https://roskomsvoboda.org/55136/) [↑](#footnote-ref-38)