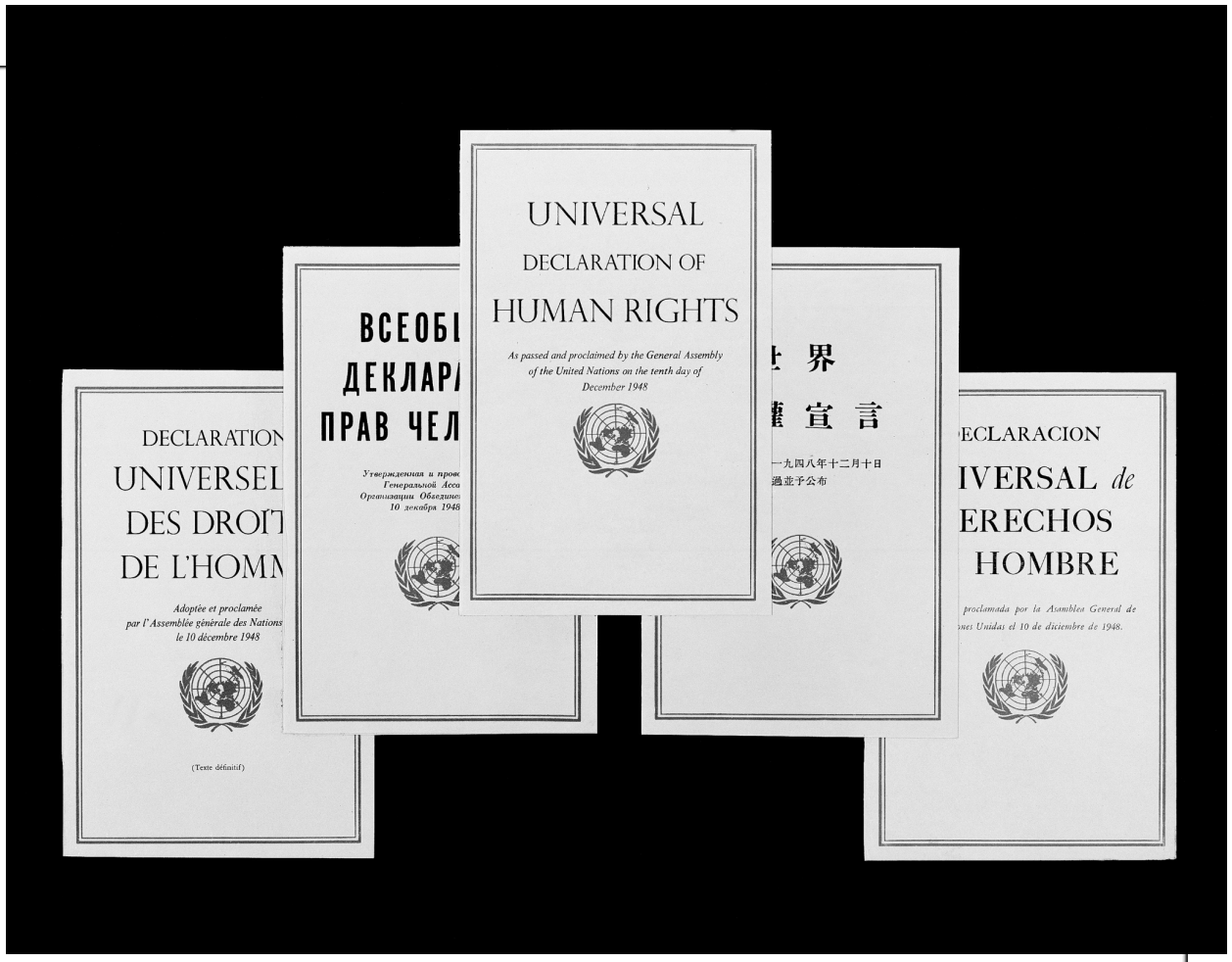
Роскомсвобода

ОВД-Инфо



Права человека и новые технологии в России

Совместное представление Верховному Комиссару ООН

ОВД-Инфо — независимый правозащитный медиапроект, направленный на мониторинг случаев политических преследований и нарушений основных прав человека в России и оказание правовой помощи их жертвам.

Роскомсвобода – первая российская общественная организация, ведущая деятельность в области защиты цифровых прав и расширения цифровых возможностей.

Фото: Reproduction of the covers of the French, Russian, English, Chinese and Spanish editions of the pamphlet: "Universal Declaration of Human Rights" published by the Department of Public Information.

В данном докладе мы освещаем проблемы отсутствия каких-либо стандартов для применения новых технологий в России и вытекающие из этого нарушения прав человека. Особенно часто такие нарушения в России можно наблюдать в использовании систем распознавания лиц, технологий онлайн-цензуры, оборудований для управления трафиком и его фильтрации и систем мониторинга социальных сетей. Эффективные механизмы восстановления нарушенных прав и компенсации вреда, предотвращения будущих нарушений, а также предварительной оценки технологий на соответствие правам человека отсутствуют. Зачастую у общества, экспертов и правозащитников и вовсе нет доступа к алгоритмам работы технологий. Все вышеперечисленное порождает множественные нарушения прав человека.

В докладе мы также анализируем хорошие практики установления стандартов и оценки технологий с позиции соблюдения прав человека в других странах, и предлагаем пути установления и работы таких стандартов и правовых процедур.

Мы рекомендуем Верховному Комиссару:

- обратить внимание на российский пример использования новых технологий в отсутствие необходимых стандартов, соблюдающих права человека;
- осудить многочисленные нарушения прав человека, допускаемые российскими властями при использовании таких технологий;
- рекомендовать странам использовать механизмы оценки и анализа потенциального влияния технологий на права человека ещё в процессе их разработки, организовывать публичные обсуждения и дискуссии с представителями тех групп населения, которых такая технология будет касаться или может затронуть в большей степени, наряду с релевантными экспертами.
- рекомендовать странам обеспечить наличие эффективных мер защиты и восстановления нарушенных использованием новых технологий прав человека, а также привлечение к ответственности лиц, совершивших эти нарушения, включая разработчиков и пользователей технологий.

Содержание:

Какие примеры лучше всего иллюстрируют взаимосвязь между техническими стандартами для новых и появляющихся цифровых технологий и правами человека?

Системы распознавания лиц

В России правоохранительные органы используют технологию распознавания лиц не только для пресечения и расследования преступлений, но и для преследования по политическим мотивам, а также для розыска в целях мобилизации.

В частности, в Москве функционирует система городского видеонаблюдения во дворах, подъездах и местах массового скопления людей[1]. Торговые центры и ночные клубы в Москве также принуждают передавать данные видеонаблюдения в центр обработки данных, доступ к которому имеют сотрудники правоохранительных органов[2]. Данные с камер городского видеонаблюдения активно использовались для установления личности участников мирного протеста в 2021 году и их дальнейшего преследования после их участия в акциях[3].

Кроме того, данные технологии активно используются в российском транспорте, включая метро[4]. В московском общественном транспорте функционирует система «Сфера» с функцией распознавания лиц, обработки и хранения полученной информации[5]. Аналогичная система действует и в Санкт-Петербурге[6] [7].

---

[1] https://video.dit.mos.ru/about/

[2] https://www.kommersant.ru/doc/5339554?from=main;
https://www.kommersant.ru/doc/5339554?from=main

[3] https://reports.ovdinfo.org/kak-vlasti-ispolzuyut-kamery-i-raspoznavanie-lic-protiv-protestuyushchih#1

[4] Постановление Правительства Российской Федерации от 8 октября 2020 года № 1641 «Об утверждении требований по обеспечению транспортной безопасности, в том числе требований к антитеррористической защищенности объектов (территорий), учитывающих уровни безопасности для различных категорий объектов инфраструктуры внеуличного транспорта (в части метрополитенов)».

[5] https://docs.cntd.ru/document/573929736

[6] https://paperpaper.ru/kak-oppozicionerov-zaderzhivayut-s-pom/

[7] https://smartevent.tbforum.ru/2017/expo/intellect-video

С 2022 года система распознавания лиц стала использоваться для превентивных задержаний в дни государственных праздников или важных общественных событий, когда, по мнению властей, более вероятна протестная активность. В большинстве случаев в московском метро задерживали тех, кто ранее привлекался к ответственности за участие в акциях протеста или за «дискредитацию» Вооруженных сил. Также иногда задерживали тех, кто не привлекался к ответственности, но участвовал в протестных акциях и был распознан с помощью системы видеонаблюдения, либо регистрировался на сайтах оппозиционных платформ, принимал участие в демократических форумах и т.д. Как правило, подобные задержания были сопряжены с доставлением в отдел МВД России и проведением профилактической беседы. Всего за 2021-2022 года ОВД-Инфо зафиксировал как минимум 595 задержаний с использованием системы распознавания лиц.

С сентября 2022 года. систему «Сфера» также стали использовать для розыска мужчин с целью их мобилизации[8], а в 2023 году. появилась информация о создании специальной базы с исчерпывающими данными о военнообязанных, которая будет сопряжена с системой распознавания лиц, в том числе на транспорте и пограничных пунктах[9].

Согласно официальным сведениям за февраль 2023 года., 8998 камер передают сигналы системе «Сфера»; эти камеры расположены не только на объектах транспорта, но и используются в передвижных комплексах[10]. При этом в начале февраля 2023 года власти сообщали, что с помощью «Сферы» задержали 7713 человек[11]. 15 февраля 2023 года в своем выступлении заместитель начальника службы безопасности Московского метрополитена М.Ю. Ромашин на конференции, посвященной транспортной безопасности, сообщил, что при необходимости сведения, которые получают с камер видеонаблюдения, накладывают на трекинг сотовой связи, данные об использовании банковских карт, проездных билетов, что позволяет выследить и задержать человека. При этом он также сказал, что «было бы

[8] https://www.bbc.com/russian/features-63346138
[9] https://zapiska.substack.com/p/6f2
[10] https://www.tbforum.ru/hubfs/Digital/SS/SS_ADAPT/%D0%A2%D0%91%D0%A4_14-02-23_%D0%93%D0%B0%D1%80%D0%B0%D0%BA%D0%BE%D0%B5%D0%B2.pdf?hsLang=ru
[11] https://rtvi.com/news/sobyanin-blagodarya-sisteme-raspoznavaniya-licz-v-moskve-zaderzhali-77-tys-chelovek-nahodyashhihsya-v-rozyske/

идеально задерживать людей еще до совершения ими преступлений или правонарушений, как только они подумают о нарушении закона»[12].

Некоторые задержанные, чья личность была установлена с использованием системы «Сфера», обжаловали свое задержание и использование в отношении них алгоритмов распознавания лиц, потребовали удалить их персональные данные из «Сферы». В настоящее время суды Москвы рассмотрели 5 таких дел, и по каждому из них отказали в удовлетворении заявленных требований[13]. На рассмотрении судов находится еще 8 дел с аналогичными исковыми требованиями. Согласно решению суда по одному из дел, задержание было связано с тем, что человек ранее был к привлечен к административной ответственности за «дискредитацию» Вооруженных сил РФ и находился в розыске по мероприятию «Митинг» в день флага России – 22 августа 2022 года.[14] По другому делу, еще находящемуся на рассмотрении суда, был получен ответ из Отдела МВД, что задержание и доставление 23 сентября 2022 года. (день «референдумов» на оккупированных Россией территориях Украины) было связано с тем, что по данным системы «Сфера» этот человек является участником массовых мероприятий. Однако, в большинстве случаев власти не признают, что использовали систему распознавания лиц «Сфера» в связи с протестной активностью, и ссылаются на закон об оперативно-розыскной деятельности и секретность информации о такой деятельности.

Технологии, используемые для онлайн-цензуры

В 2012 году в России появился первый централизованный Единый реестр блокировок, который ведёт орган надзора в сфере связи и медиа

---

[12] https://www.tbforum.ru/2023/program/transport-day2

[13] Чертановский районный суд г. Москвы. Дело № 2а-1229/2022. URL: https://mos-gorsud.ru/rs/chertanovskij/services/cases/kas/details/27922881-699f-11ed-bec0-3bcaa48bca8d?participants=созонюк; Никулинский районный суд г. Москвы. Дело № 2а-36/2023. URL: https://mos-gorsud.ru/rs/nikulinskij/services/cases/kas/details/b7288701-6c0b-11ed-97fa-a1f193b73b24?participants=аптышева; Бутырский районный суд г. Москвы. Дело № 2а-13/2023. URL: https://mos-gorsud.ru/rs/butyrskij/services/cases/kas/details/07fd9600-6a79-11ed-afe8-07e7cd38cd60?participants=аптекарь; Черемушкинский районный суд г. Москвы. Дело № 2а-248/2023. URL: https://mos-gorsud.ru/rs/cheryomushkinskij/services/cases/kas/details/da546640-97c1-11ed-b5fd-cdbece044c3e?participants=максимова; Никулинский районный суд г. Москвы. Дело № 2а-103/2023. URL: https://mos-gorsud.ru/rs/nikulinskij/services/cases/kas/details/6d969171-90e8-11ed-94c6-b74b139192e1?participants=виноградов

[14] Решение Никулинского районного суда г. Москвы от 23 января 2023 года по делу № 2а-36/2023. URL: https://mos-gorsud.ru/rs/nikulinskij/services/cases/kas/details/b7288701-6c0b-11ed-97fa-a1f193b73b24?participants=аптышева

Роскомнадзор[15]. Реестр создан на основе Федерального закона № 139-ФЗ, которым внесены поправки в закон «Об информации, информационных технологиях и о защите информации»[16] (далее - «закон об информации»), в закон «О связи»[17], и в закон «О защите детей от информации, причиняющей вред их здоровью и развитию»[18].

Основания включения сайтов и интернет-страниц в Единый реестр и общий порядок действий Роскомнадзора, провайдеров хостинга и операторов связи изначально был зафиксирован в статье 15.1 закона об информации. За последующие 10 лет список оснований и порядок блокировок расширялся и уточнялся, в законе об информации появились другие нормы, нацеленные на ограничение доступа к специфическим типам информации и онлайн-сервисам (например, к мессенджерам, сервисам электронной почты, VPN-сервисам), для некоторых из них созданы отдельные реестры блокировок (теперь их несколько, все ведутся Роскомнадзором).

В целом, ограничение доступа к сайтам или онлайн-сервисам в рамках закона об информации производится в следующем порядке: уполномоченный государственный орган или суд принимают решение об ограничении доступа к информации или онлайн-сервису, направляют решение в Роскомнадзор, Роскомнадзор вносит информации в соответствующий реестр блокировок (доменное имя сайта или указатель страницы, сетевой адрес сайта, короткое описание типа запрещённой информации, реквизиты решения, которое является основанием для блокировки, даты поступления решения в Роскомнадзор, отправки уведомления провайдеру хостинга и оператору связи). Информацию о сайтах, интернет-страницах и IP-адресах, которые надо блокировать, Роскомнадзор передаёт операторам связи России в автоматизированном режиме (выгрузка данных 2 раза в сутки). В силу закона о связи операторы связи России обязаны ограничивать доступ своих абонентов к тем сайтам и онлайн-сервисам, которые получает в выгрузке из Роскомнадзора (за неисполнение этой обязанности предусмотрен крупный административный штраф).

---

[15] Полное наименование – Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций

[16] Федеральный закон от 27 июля .2006 года № 149-ФЗ

[17] Федеральный закон от 07 июля 2003 года № 126-ФЗ

[18] Федеральный закон от 29 декабря 2010 года № 436-ФЗ

Каких-либо обязательных технологических стандартов в сфере интернет-блокировок в России не установлено. Оператором связи разрешалось блокировать целый сайт ради блокировки одной из его страниц, если у оператора связи нет технологической возможности осуществить блокировку точечно. Штрафы за неисполнение обязанности по блокировке, отсутствие стандартов и рекомендации Роскомнадзора привели к тому, что ограничение доступа к информации в России часто имеет излишний характер и затрагивает контент, который не был признан незаконным на территории России. При этом, защита права на распространение законной информации при расширительной блокировке в России затруднена и почти не приводит к положительному исходу для распространителя законного контента, так как сложившаяся судебная практика непоколебимо стоит на позиции оправданности практически любой блокировки и суды не восприимчивы к доводам о необоснованности излишних ограничений на свободу распространения информации. В этой части показательны два дела: дело директора Ассоциации интернет-издателей Владимирова Харитонова и блокировка мессенджера Telegram.

Директор Ассоциации интернет-издателей Владимиров Харитонов пытался обжаловать в российский судах ограничение доступа к своему сайту 2012 года - блокировка была нацелена на сайт с пропагандой наркотиков, произведена по IP-адресу, поэтому затронула весь сайт В.Харитонова, расположенный на том же IP-адресе. Суды признали такую блокировку законной, а Европейский суд по правам человека (далее - ЕСПЧ) признал её нарушением статьи 10 Европейской конвенции по правам человека.[19].

В 2018 году история повторилась в больших масштабах. Роскомнадзор санкционировал блокировку мессенджера Telegram по IP-адресам (одновременно по решению суда и требованию Генерального прокурора РФ). Это привело к ограничению доступа и нарушениям в работе множества иных онлайн-сервисов и сайтов, владельцы некоторых таких сервисов и сайтов пытались признать «блокировку заодно» незаконной и взыскать убытки, но российские суды им отказали (например, так поступил владелец VPN-сервиса TgVPN, дело которого сейчас находится на

[19] Владимир Харитонов против России, https://hudoc.echr.coe.int/fre?i=001-203177

рассмотрении ЕСПЧ)[20]. О снятии ограничений доступа к ресурсам мессенджера Telegram Роскомнадзор объявил 18 июня 2020 года.

DPI и ТСПУ

За время 2х-летней блокировки мессенджера Telegram в России приняли так называемый «закон о суверенном интернете»[21].

Данный закон ввёл обязательные правила маршрутизации интернет-трафика и переместил маршрутизацию трафика под контроль Роскомнадзора. Цель закона — защита российского сегмента интернета от внешних угроз. Оборудование DPI и ТСПУ — это те технологические инструменты, которые применяются для реализации указанного закона. Закон предписывает операторам связи устанавливать и применять на своих сетях специальное оборудование для фильтрации трафика (DPI) и централизованного управления трафиком (ТСПУ).

DPI — Deep Packet Inspection («глубокое исследование пакетов»). Это анализ содержимого пакетов (коротких блоков, которыми информация передаётся по интернету). Прочитать содержимое зашифрованных пакетов нельзя, но по полученным с помощью DPI метаданным можно понять, какие сайты смотрит пользователь и, в большинстве случаев, какой протокол обмена данными он использует. Изначально с помощью DPI операторы изучали интернет-трафик, чтобы выставлять приоритеты при передаче данных. Например, голосовые сообщения более требовательны к задержкам и им нужно предоставлять бóльший приоритет в общем потоке трафика. Позже появились решения для монетизации (анализа трафика для продажи информации и подмены рекламы на сайтах, не использующих HTTPS на «свою») с помощью DPI-оборудования. Но в последние пару лет мы наблюдаем использование технологии DPI в том числе для блокировки онлайн-контента.

В сентября 2019 года DPI-оборудование разных производителей тестировали в Уральском федеральном округе для целей исполнения закона в рамках пилотного проекта подконтрольного Роскомнадзору государственного предприятия ФГУП «Главный радиочастотный центр»[22].

---

[20] Подробнее о деле TgVPN: https://roskomsvoboda.org/court-case/case-tgvpn/
[21] Поправки в закон о связи и в закон об информации (Федеральный закон от 1 мая 2019 года № 90-ФЗ)
[22] https://www.rbc.ru/technology_and_media/26/09/2019/5d8b4c1c9a7947d3c58f9a48

Какая-либо документация с техническими стандартами данного оборудования не раскрывалась, тестирование проходило без участия институтов гражданского общества, механизмов и способов такого участия не предусмотрено.

В любом случае, DPI-оборудование в итоге стоит далеко не у всех операторов связи и не все, у кого оно есть, используют его для блокировки. ТСПУ же управляются централизованно Роскомнадзором, который может распространить одинаковые правила блокировок на всех.

ТСПУ — технические средства противодействия угрозам. Другими словами, это новый программно-аппаратный комплекс, позволяющий ограничивать доступ к информации, распространение которой запрещено на территории России. Роскомнадзор стал требовать от операторов связи устанавливать ТСПУ с сентября 2020 года. Делает он это в рамках закона о суверенном интернете. Теперь надзорное ведомство может централизованно управлять российским сегментом интернета, фильтруя трафик при помощи DPI.

С помощью ТСПУ можно не только блокировать, но и, например, «замедлять» те или иные сервисы и протоколы передачи данных, а также устраивать «шатдауны» на локальном уровне. Примером «замедления» с помощью ТСПУ можно назвать кейс социальной сети Twitter.

10 марта 2021 года Роскомнадзор сообщил о том, что Twitter внесли в перечень внешних угроз из-за медленного удаления материалов с запрещённой информацией, а также о своём решении замедлить скорость работы сервиса Twitter на 100% мобильных устройствах и 50% стационарных устройств. При этом однозначных оснований для замедления трафика в законе нет. В одном из нормативных актов, принятых во исполнение закона о суверенном интернете, говорится, что ограничению подлежит «угроза безопасности функционирования на территории РФ сети интернет». Среди мер по её устранению значится «изменение маршрутов сообщений электросвязи» и «изменение конфигурации средств связи». Никакой определённой технической информации о том, как именно надзорный орган осуществляет это самое замедление, в публичном доступе нет.

Эксперты высказывали лишь предположения и технологии замедления трафика, поэтому группа экспертов, в которую входил эксперт Роскомсвободы, провела исследование и 6 апреля 2021 опубликовала доклад[23]. Помимо технологического анализа в докладе отмечается, что случай с Twitter показал, что механизм онлайн-цензуры в России меняет свой характер с децентрализованного (операторы связи блокировали контент на основе информации от Роскомнадзора) на централизованный (Роскомнадзор благодаря обязательному применению оборудования ТСПУ имеет возможность в одностороннем порядке наложить желаемые ограничения). Исследователи также отметили, что, в отличие от блокировки, при которой доступ к контенту заблокирован, дросселирование (замедление трафика) направлено на снижение качества обслуживания, что делает практически невозможным для пользователей отличить навязанное/преднамеренное замедление от ряда нюансов, например, таких как высокая нагрузка на сервер или перегрузка сети.

В данном контексте важно отметить, что изначально блокировка контента была только централизованная, информацию об ограничении доступа к сайтам и основаниях можно было получить из открытых реестров Роскомнадзора. Однако замедление и блокировки по закону о суверенном интернете через ТСПУ ни в каких публичных реестрах не фиксирует и не отображается.

Ситуация с замедлением социальной сети Twitter в России наглядно демонстрирует, что общество полностью исключено из процесса формирования технических стандартов таких технологий анализа и фильтрации трафика, как DPI. На фоне этого применение таких технологий двойного назначения для онлайн-цензуры делает цензурирование более незаметным для граждан. При этом, граждане, которые использовали Twitter, попытались оспорить замедление трафика к сервису через суд в рамках общественной кампании Роскомсвободы «Битва за Twitter». Суд посчитал, что права на оспаривание замедления у пользователей Twitter нет, и отказал в принятии иска. В настоящее время отказ обжалуется в суде кассационной инстанции[24].

Роскомсвобода в сотрудничестве с Open Observatory of Network Interference (OONI) подготовила исследовательский отчёт, документирующий случаи

[23] https://censoredplanet.org/throttling
[24] Битва за Twitter, Роскомсвобода: https://runet.report/campaign/twitter/

интернет-цензуры в России за последний год (с января 2022 года по февраль 2023 года)[25]. Этот отчёт содержит технический анализ доступности интернета OONI и большой правовой анализ всех законодательных положений, принятых с начала «специальной военной операции». Эксперты OONI выявили, что заблокированные из-за военной цензуры ресурсы не все были отражены в государственном реестре блокировок.

Таким образом, применение DPI и ТСПУ для цензуры не столько обострило вопрос соблюдения прав человека при использовании таких технологий (в том числе через участие общества в разработке стандартов) в России, сколько привлекло внимание к существованию такой проблемы. Ни во времена чисто коммерческого использования данных технологий операторами связи, ни уж тем более при их использовании во исполнение закона о суверенном интернете властями, сам вопрос о необходимости учёта соблюдения прав человека (на свободу распространения информации и приватность) не поднимался, а попытки общественных институтов и отдельных субъектов бороться с нарушением прав человека из-за данных технологий, блокируются судами.

Мониторинг социальных сетей

В феврале 2023 года Роскомнадзор запустил систему автоматического поиска запрещённого контента «Окулус». Заказ на госзакупку был размещён ещё в августе 2022 года, Согласно технической документации, система в реальном времени анализирует изображения и видео, переписки в чатах и материалы каналов мессенджеров, URL-адреса и другие данные на предмет запрещенной информации и классифицировать контент по типам запрещённой информации.

Также подведомственное Роскомнадзору предприятие Главный радиочастотный центр занимается внутренними испытаниями системы поиска и обезвреживания информационных бомб «Вепрь». Исходя из технического задания данная система должна противостоять «распространению общественно значимой информации под видом достоверных сообщений, которая создает угрозу причинения вреда жизни и (или) здоровью граждан, имуществу, угрозу массового нарушения общественного порядка и (или) общественной безопасности». Также система будет работать над обнаружением авторов, распространяющих в

[25] https://ooni.org/ru/post/2023-russia-a-year-after-the-conflict/

интернете анонимные сообщения, анализировать контент по определенным темам-триггерам, а также распространение одинаковых сообщений, которые, к примеру, появляются на новостных сайтах или Telegram-каналах и подхватываются некоторыми лидерами мнений. Эксперты полагают, что обе системы «Окулус» и «Вепрь» будут использоваться Роскомнадзором совместно, чтобы заменить «ручное» выявление запрещённой на территории РФ информации. Полагаем, что данные системы могут использоваться как для принятия решений о блокировке контента, так и для наказания отдельных лиц за распространение информации в интернете. Это приведёт к снижению возможностей оспаривания и обжалования ограничений и наказаний, так как российские суды не ставят под сомнение правильность решений, принятых в автоматизированном режиме.

Таким образом, обе системы разрабатываются по заказу государственных органов, система государственных закупок РФ не предполагает анализ технологий в контексте соблюдения прав человека и участия институтов гражданского общества при разработке для выработки стандартов в данном контексте.

Какие процессы по установлению стандартов особенно важны для защиты и продвижения прав человека в контексте новых и появляющихся цифровых технологий?

Одной из проблем регулирования новых технологий является дилемма Коллингриджа: «Попытки контролировать технологии сложны… потому что на ранних стадиях, когда их можно контролировать, недостаточно известно о социальных последствиях; но к тому времени, когда эти последствия становятся очевидными, контроль становится дорогостоящим и медленным»[26]. Другой серьезной проблемой является так называемая проблема темпа: «технологии меняются экспоненциально, но социальные, экономические и правовые системы меняются постепенно»[27]. Система регулирования работает медленно и не может идти в ногу с новыми технологиями и поэтому тормозит развитие.

[26] Colingridge. D., The Social Control of Technology, Milton Keynes: the Open University Press, 1980
[27] Downes, L. (2009). The Laws of Disruption: Harnessing the New Forces That Govern Life and Business in the Digital Age. Basic Books.

Новые технологии всегда представляют риск для прав человека, поэтому очень важно оценивать технологии на ранней стадии разработки с точки зрения прав человека и воспринимать их как «взаимодействие между технологическим потенциалом и социальными ценностями»[28].

Поддержка организаций гражданского общества может резко повысить уровень осведомленности о правах человека и способствовать их защите. Проект УВКПЧ ООН «Бизнес и права человека в технологиях» представляет собой актуальный процесс, который следует развивать дальше как механизм прозрачного участия гражданского общества в защите прав человека в сфере технологий[29].

Национальные органы власти должны играть центральную роль в оценке законодательства и выявлении любых пробелов. Несмотря на то, что невозможно предсказать развитие новых технологий, уже существуют налаженные процессы, которые могут снизить риски нарушения прав человека. Одним из них является подход «human rights by design», основанный на уже хорошо известных и широко используемых методологиях «privacy by design»[30]. Разработчики должны выполнять ключевые обязательства и требования такого подхода при создании технологии.

Таким образом, значительного вреда можно легко избежать на ранних этапах. В декабре 2020 года Специальный комитет по искусственному интеллекту предложил девять принципов и приоритетов, которые помогут создать такую структуру[31]. Несмотря на то, что их основное внимание уделяется искусственному интеллекту, эти принципы можно легко использовать для всех новых технологий во всех секторах.

Существует также ряд других механизмов, которые могут помочь защитить права человека. Одним из них является должная осмотрительность при соблюдении прав человека, которая быстро становится обязательным требованием во многих юрисдикциях в связи с введением специальных правил на национальном уровне. Для каждой организации крайне важно провести оценку воздействия (human rights impact assessment), чтобы

---

[28] Palm E., THe case for ethical technology assessment. Technological Forecasting and Social Change, 73(5), 2006, p. 550

[29] https://www.ohchr.org/ru/topic/business-and-human-rights

[30] https://unsdg.un.org/2030-agenda/universal-values/human-rights-based-approach

[31] David Leslie et al., Artificial Intelligence, Human Rights, Democracy, and the Rule of Law, Council of Europe and The Alan Turing Institute, 2021

убедиться, что проектирование, разработка и развертывание технологии не нарушают права человека.

Странам следует рассмотреть возможность принятия законов или иных обязательных актов, которые бы закрепляли необходимость соблюдения прав человека при разработке новых технологий. Такие акты должны, в том числе, предусматривать, что на начальных стадиях разработки любых потенциально затрагивающих права человека технологий должна быть проведена соответствующая оценка с участием независимых экспертов. Наряду с техническими экспертами, эксперты в области прав человека должны приглашаться для оценки и анализа таких технологий и процессов их разработки. Если технология не проходит такую проверку, процесс разработки должен быть пересмотрен, и, при невозможности удовлетворить критерии оценки – остановлен.

Другое решение — создание регуляторных песочниц. Регуляторные песочницы — не совсем новая концепция. Они уже активно используются в финтехе по всему миру. Регуляторная песочница — это инструменты регулирования, позволяющие бизнесу тестировать и экспериментировать с новыми и инновационными продуктами, услугами или бизнесом под контролем регулятора в течение ограниченного периода времени[32].

Риски нарушения прав человека также можно снизить с помощью более консервативных методов, таких как сертификация и аудит. При правильном использовании, а не в качестве «галочки», эти процессы могут защитить права человека.

Перед запуском технологии следует также организовывать публичные обсуждения и дискуссии с представителями тех групп населения, которых такая технология будет касаться или может затронуть в большей степени, наряду с релевантными экспертами. Более того, если в процессе использования выяснится, что права человека затрагиваются технологией, разработчики и иные ответственные лица должны привлекаться к ответственности, а использование – приостанавливаться. Жертвы таких нарушений должны иметь возможность обратится в суд для защиты и восстановления их прав, а также получить компенсацию вреда. Если нарушение прав человека конкретного лица невозможно устранить без отказа от использования такой технологии, либо же становится очевидно,

[32] Madiega, T (2022). Artificial intelligence act and regulatory sandboxes. EPRS, PE 733.544

что права иных лиц нарушаются или могут быть нарушены, использование такой технологии должно быть прекращено, даже если ее заказчиком и/или разработчиком является государство.

Каковы общие препятствия для эффективной интеграции соображений прав человека в процессы установления технических стандартов для новых и появляющихся цифровых технологий?

Распространение новых и появляющихся технологий в мире значительно расширило инструментарий государства для репрессий и социального контроля, что привело к постепенному ухудшению уровня защиты прав человека в этой сфере за последние два десятилетия.

Если заказчиком и пользователем технологии является государство, многие ограничения прав человека, возникающие из-за использования таких технологий, как правило, оправдываются целями национальной безопасности и общественного порядка. В странах, где фактически отсутствует возможность для выражения независимого мнения и участия в общественных дискуссиях, например в России, представляется невозможным независимая экспертная оценка необходимости и пропорциональности ограничений прав человека, вызванных применением технологии.

Одним из распространенных препятствий на пути эффективной интеграции прав человека также является принятие законов и других нормативных актов, ограничивающих права человека с помощью технологий. Таким образом, государства борются не за права человека, а против правозащитников и независимых СМИ. Новые законы облегчают легализованный сбор данных граждан. Первая стратегия в России – это тотальные ограничения, попытки поставить под контроль цифровую среду с помощью законов Яровой, контроль Рунета, блокирование сайтов независимых СМИ и распространение их материалов[33].

Если заказчиком и пользователем технологии являются негосударственные компании, при отсутствии законодательно закрепленного обязательства проводить предварительную оценку соответствия технологии правам

[33] https://en.ovdinfo.org/internet-blocks-tool-political-censorship

человека, у таких компаний будет невысокая мотивация вовлекать в обсуждения представителей гражданского общества, особенно в странах, в которых законодательно не закреплена обязанность соблюдения прав человека и ответственность за их нарушения применительно к частным компаниям.

Более того, если в стране отсутствует законодательное регулирование конкретной технологии, а также общее требование о проведении предварительной оценки соответствия технологии правам человека, у лиц, пострадавших от использования технологии, будут отсутствовать эффективные способы защиты. Такая ситуация складывается в России применительно к использованию системы распознавания лиц против протестующих, поскольку использование этой технологии никак не урегулировано. В силу этого, оспорить и доказать такое применение в судах становится является чрезвычайно трудным.

Насколько доступны процессы установления стандартов для новых и появляющихся цифровых технологий для широкого круга заинтересованных сторон, в частности, для организаций гражданского общества и экспертов по правам человека? Какими показателями измеряется «доступ» в этом контексте?

В России процессы установления стандартов для технологий недоступны, поскольку в целом серьезно ограничены права человека, включая возможность выражать независимое мнение, реализовать право на свободу ассоциаций, а также участвовать в жизни государства. Существование «доступа» могло бы измеряться открытостью информации о разработке такой технологии, возможностью гражданского общества участвовать в общественных дискуссиях в связи с разработкой и использованием технологии, принимать участие в экспертной оценке соответствия технологии правам человека, а также существованием эффективных средств защиты пострадавших от использования технологий. Все эти критерии не выполняются в России.

Каковы передовая практика, механизмы и модели для эффективной интеграции соображений прав человека в процессы установления технических стандартов? Существуют ли особые проблемы при их реализации или принятии? Какие дополнительные меры следует разработать и внедрить?

Например, применение методов дистанционного зондирования земли (remote sensing) с целью фиксации объектов, свидетельствующих о совершении в Мьянме в 2017 году преступлений против человечности, показало хорошие результаты как раз из-за соблюдения стандартов прав человека в таких технологиях и использования их без «персонализации» [34]. В данном случае был применен комплексный анализ, включающий изображения со спутников и анализ почвенного слоя. Результатом стало установление факта уничтожения деревень (на их местах остались пепелища) и появления лагерей беженцев.

В судебных процессах хорошая практика использования ИИ может быть отмечена в Австралии, где существует гайд, четко очерчивающий границы такого использования для предупреждения нарушений прав человека[35]. Несмотря на то что замена судьи ИИ в каждом деле видится невозможной и чрезмерной, ИИ может активно использоваться для выполнения технической работы, а также для рассмотрения дел по административным правонарушениям.

Право человека на информацию, вытекающее из фундаментальных конвенционных прав, всесторонне нарушается в связи с дискриминационными и выборочными практиками, которые применяют социальные сети и интернет-сервисы. Хороший механизм соблюдения прав человека здесь — формирование системы правовых ограничений, аналогичных антимонопольному регулированию, которые ограничат право на необоснованную фильтрацию информации агрегаторами и соцсетями [36].

---

[34] https://reliefweb.int/report/world/what-can-go-right-positive-use-cases-science-and-technology-human-rights-investigations

[35] https://tech.humanrights.gov.au/downloads?_ga=2.33122430.1163461926.1677534476-787121396.1677534476

[36] https://dailytargum.com/article/2021/03/bedi-u-s-government-must-develop-new-methods-of-regulation-for-social-media

Каковы обязанности и ответственность организаций и заинтересованных сторон, устанавливающих стандарты в эффективном учете соображений прав человека в процессах разработки технических стандартов для новых и появляющихся цифровых технологий?

Учет права на частную жизнь

Ярким примером нарушения этого прав являются приложения ИИ для распознавания лиц. Этот тип технологий уже используется полицией в некоторых странах и рискует быть использованным авторитарными режимами для подавления политических диссидентов и меньшинств.

Исследование 2016 года показало, что половина взрослых американцев уже есть в полицейских базах данных по распознаванию лиц по всей стране. Из-за опасений по поводу конфиденциальности и неправомерного использования несколько крупных городов США ввели запрет на использование этой технологии. Калифорния, Нью-Гэмпшир и Орегон приняли законы, запрещающие использование технологии распознавания лиц с полицейскими нательными камерами. После протестов Black Lives Matter в США в 2020 году IBM, Amazon и Microsoft ограничили или приостановили продажи своих продуктов для распознавания лиц.

В Европе GDPR запрещает обработку биометрических данных с целью однозначной идентификации физического лица, данных о здоровье, данных о сексуальной жизни или сексуальной ориентации физического лица, а также обработку данных, раскрывающих расовое или этническое происхождение. Официальные лица ЕС изначально рассматривали возможность полного запрета на распознавание лиц в общественных местах, но вместо этого предоставили государствам-членам возможность ввести запрет после сильного противодействия со стороны некоторых членов. Кроме того, в апреле 2021 года Европейская комиссия предложила новые правила и действия по разработке надежного ИИ, в которых распознавание лиц считается приложением с высоким риском и разрешено только в определенных случаях.

В России, системы распознавания лиц никак не контролируются и не регулируются законодательно, у общества и правозащитников нет доступа к процессам разработки и работы таких технологий, не существует

официально закрепленного ведомства, ответственного за такие процессы, как и контролирующего законодательства. Суды и органы власти отказываются предоставлять подробности идентификации и внесения лиц в базы, как и алгоритмов выхода оттуда.

Учет права на недискриминацию

Человеческие предубеждения часто присутствуют в неавтоматизированных системах просмотра данных, и автоматизированные системы ИИ теоретически могут помочь исправить или компенсировать некоторые из этих предубеждений. Однако системы ИИ также могут быть преднамеренно или непреднамеренно предвзяты. Опасения по поводу дискриминации возникают, когда отдельные переменные в алгоритмах косвенно служат прокси для защищенной или нераскрытой информации, такой как раса, сексуальная ориентация, пол или возраст. Алгоритм может привести к тому, что пользователи будут дискриминировать группу, которая коррелирует с рассматриваемой прокси-переменной.

Применительно к контексту предупреждения преступности и предиктивной полицейской деятельности дискриминационная поддержка принятия решений ИИ может привести к серьезным нарушениям прав. Такие примеры включают использование систем искусственного интеллекта для поддержки выявления потенциальных террористов на основе контента, который они размещают в Интернете. Обучение ИИ в таких приложениях основано на текущих полицейских базах данных, которые часто отражают и усиливают существующие расовые и культурные предрассудки, существующие в сообществах. Существующие базы данных могут быть предвзятыми или неполными. В России известны случаи использования таких баз данных для политического, этнического и идеологического профилирования, что создает опасные прецеденты для дальнейшего развития таких баз и систем, а также решений, которые они принимают[37].

Обязанности и ответственность организаций, разрабатывающих и применяющих такие технологии, состоит в подробной оценке каждой стадии процесса разработки и применения данных технологий,

[37] Подробнее см. в докладе Сетевых свобод “Технологии политического профайлинга” // https://drive.google.com/file/d/1sg8wDktOErOxBR29JaXJAsXxSMBUvLFR/view?fbclid=IwAR3SHpQ8iRAKq4UsBVsKekttQ_I_LRdvlPEZ3FaNBDJ5dVGCtit41XpdK0k

прозрачном репортинге этих процессов, а также в создании механизмов остановки использования алгоритмов.