



[Перейти](#)

17.01.2022

Как власти используют камеры и распознавание лиц против протестующих

Дата публикации: 17 января 2022

English version: [How Authorities Use Cameras and Facial Recognition against Protesters](#)

ВВЕДЕНИЕ

«В воскресенье [25 апреля 2021 года] утром я проснулся от того, что ко мне в комнату в общежитии очень настойчиво кто-то стучался, — рассказывает студент Артем Пугачев. — Мой сосед открыл дверь, и тут к нам бесцеремонно вошли господа полицейские. В довольно агрессивной форме сказали мне, что пора собираться — поедем в отдел. На мои требования разъяснить, на каком основании, они не ответили. В полупринудительном порядке сопроводили меня в машину и отвезли в отдел».

В отделе полицейские оформили задержание. Двое суток Пугачев провел в полиции, а потом его признали виновным в повторном нарушении порядка проведения акции (ч.

8 ст. 20.2 КоАП) и назначили десять суток ареста. Студенту вменили участие в митинге в поддержку Алексея Навального, прошедшем в Москве 21 апреля.

После **апрельской акции** многие недоумевали: почему массовые задержания были только **в некоторых городах**? В отличие от **зимних протестов**, акция в Москве прошла без тысяч задержанных, автозаки и отделы полиции не были переполнены, насилия к протестующим полицейские не применяли. Казалось, власти смирились и решили не мешать собравшимся реализовывать свое право на свободу собраний.

Но уже спустя несколько дней стало очевидно, что это не так. Начались визиты полицейских, задержания и суды.

Задержания протестующих уже после окончания акции или, как мы их называем, «задержания постфактум» происходили и до 2021 года. В 2018-м ОВД-Инфо насчитал 219 таких случаев в 39 регионах России, в основном они носили единичный характер: в связи с одной акцией задерживали одного-двух человек, в исключительных случаях число задержанных **доходило** до десяти. Широко задержания постфактум начали применять в 2020 году во время протестов против ареста губернатора Хабаровского края Сергея Фургала. С июля по начало декабря 2020 года ОВД-Инфо **зафиксировал** там 121 задержание постфактум — почти вдвое больше, чем на самих акциях.

В 2021 году подобная практика появилась и в Москве. В день акции 31 января многих людей задерживали из-за участия в **протестах неделей ранее**. В течение недели после 21 апреля в Москве **задержали** более ста человек, а в суды поступило более 180 дел о нарушении порядка проведения публичного мероприятия (по статье 20.2 КоАП).

Всего в 2021 году мы зафиксировали по меньшей мере 454 задержания постфактум. Большинство из них — 363 — связаны с митингом в поддержку Навального 21 апреля. Остальные задержания постфактум — со всероссийскими акциями 23 и 31 января, а также с акциями 20 и 25 сентября на Пушкинской площади в Москве.

Мы полагаем, что рост количества задержаний постфактум основывается на развитии технологий мониторинга социальных сетей и распознавания лиц: авторов постов с информацией об акциях приравнивают к организаторам, а людей, выявленных по видеозаписям, объявляют участниками протестов.

Наш доклад посвящен применению систем распознавания лиц для ограничения свободы собраний. Хотя исследование фокусируется на Москве, согласно нашим данным, география этого явления выходит далеко за пределы столицы.

На основании материалов административных дел, текстов судебных постановлений и свидетельств задержанных мы показываем, как власти скрывают использование распознавания лиц в административных делах, как воспринимают этот факт суды, и какие негативные последствия влечет за собой подобная практика. Кроме того, мы объясняем, что **нужно изменить** в правовом регулировании и правоприменении для обеспечения свободы собраний.

ВНЕДРЕНИЕ СИСТЕМЫ РАСПОЗНАВАНИЯ ЛИЦ В РОССИИ

В мае 2017 года официальный сайт мэра Москвы **сообщил**, что к Единому центру хранения и обработки данных (ЕЦХД) подключили более трех с половиной тысяч камер, в том числе более 1600 из них — в подъездах жилых

домов. А уже в сентябре более трех тысяч камер городского видеонаблюдения **включили** в систему распознавания лиц. Мэрия назвала ее одной из крупнейших в мире, ответственным за ее развитие в Москве стал Департамент информационных технологий (ДИТ).

В 2018 году власти имели возможность провести масштабное тестирование новой технологии во время Чемпионата мира по футболу. Как позже **рассказывал** гендиректор корпорации «Ростех» Сергей Чемезов, к разработанной компанией NTechLab системе FindFace Security было подсоединено около 500 камер, которые позволили задержать около 180 человек в нескольких городах. Речь **шла** как о камерах городского наблюдения, так и о специально установленных камерах на стадионах и в метрополитене.

Эти технологии являются частью инструментария, который власти развивают в федеральной программе **«Безопасный город»** (к ней относится не только распознавание лиц, но и, например, городское видеонаблюдение). В большинстве регионов «Безопасный город» начали вводить в 2015–2016 годах. В сентябре 2020-го компания NtechLab **заявила**, что тестирует свои алгоритмы в Нижнем Новгороде и еще **девяти** крупных городах, правда, не назвав их.

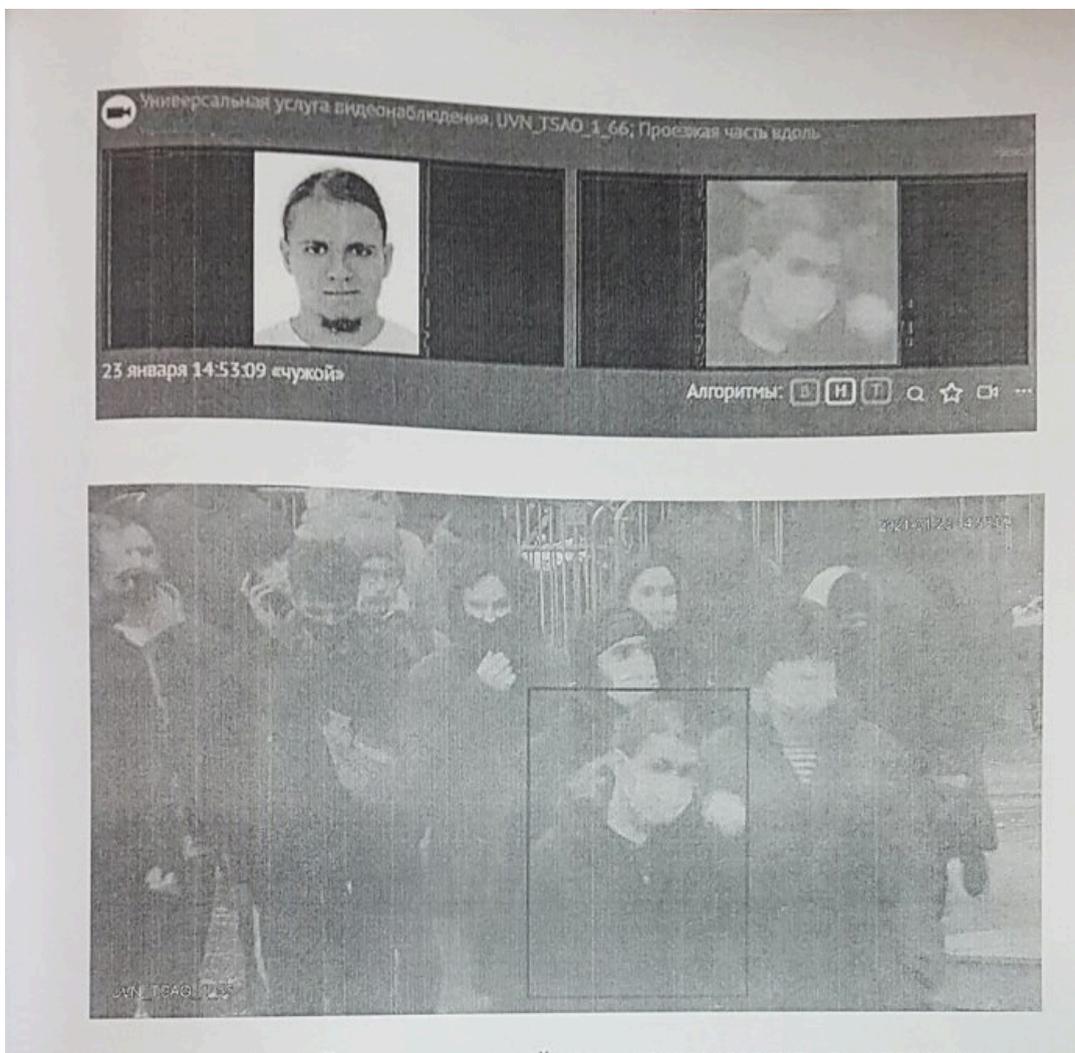
Согласно данным **NIST**, по качеству распознавания алгоритмы российских компаний NtechLab и VisionLabs (еще одна компания, чьи алгоритмы **использует** ДИТ для развития системы городского видеонаблюдения в Москве) **находятся** на втором и третьем месте в мире. Обгоняет Россию только **Китай**.

Хотя массовое ношение медицинских масок во время пандемии могло стать препятствием для распознавания лиц, разработчик биометрического распознавания Антон

Мальцев считает, что эту проблему, возможно, уже решили:

«Точность систем поначалу просела, но не критично — их сразу стали переобучать. Грубо говоря, возьмем [розничные продажи], с которыми [в сфере распознавания] работают мои знакомые. В магазине делали трекинг людей: что покупают люди, где они ходят. И у них была проблема, что все системы перестали работать, когда появились маски. За месяц-два где-то их переобучили, получили потерю точности, но и с масками у них в итоге все работало. Поэтому, если это медицинская маска, которая еще, может быть, чуть приспущена, скорее всего, работает и у нас».

И действительно, исследуя протоколы привлекаемых к ответственности постфактум, ОВД-Инфо обнаружил по крайней мере один случай в Москве, когда человека задержали на основании фотографии и видеозаписи, хотя на обоих изображениях он был в медицинской маске.



Активиста и автора телеграм-канала “Протестный МГУ” Дмитрия Иванова привлекли к ответственности по следам акции 21 апреля несмотря на то, что на видеозаписях с мероприятия он был в маске

ИСТОЧНИКИ ИЗОБРАЖЕНИЙ С АКЦИИ

Многие люди, обращавшиеся в ОВД-Инфо из-за преследований постфактум в связи с протестными акциями начала 2021 года, заявляли, что полицейские не скрывали, что нашли их с помощью фото и видеокамер.

Студенту Артему Пугачеву в отделе полиции не показывали записей с камер, но продемонстрировали рапорт сотрудника, который якобы нашел Пугачева на видео. Само видео Пугачев увидел только в суде:

«Мы приехали, дождались нашей очереди. Судья зачитала материал обвинения, спросила, есть ли у меня какие-то комментарии. Я ей рассказал свою позицию, а дальше приступили к разбору материалов дела. К этому делу был приложен диск, помощница судьи его вставила в компьютер и вывела на экран. По сути это не что иное, как запись просто с обычной городской камеры. Просто по улице идут люди, сплошным потоком. Вот, идут люди-люди-люди... И тут выхожу я и поворачиваю лицо в камеру — и в этот момент стоп-кадр».

Среди обратившихся в ОВД-Инфо из-за акции 21 апреля как минимум 164 человека отметили, что в ходе общения с полицией или во время судебного заседания их проинформировали об использовании фото- и видеоматериалов с их участием в качестве доказательств. 125 человек получили возможность ознакомиться с этими материалами. [Подробнее о методологии.](#)

Хотя чаще всего о таком сообщали жители Москвы, столицей эта практика не ограничивается: аналогичные свидетельства поступили еще как минимум из 17 городов.



Источник: ОВД-Инфо • [Скачать данные](#) • Создано с помощью [Datawrapper](#)

Некоторым правоохранителям открыто сообщали, что нашли их с помощью системы «Безопасный город». В одном случае задержанному в отделе полиции рассказали даже о том, где находилась камера, снимавшая людей, двигавшихся 21 апреля по Тверской улице к станции метро «Охотный ряд».

Помимо фотографий и записей с камер наружного наблюдения, в делах фигурировали кадры и записи оперативной съемки, а также фото и видео из интернета: телеграм-каналов, чатов, личных страниц в социальных сетях, платформы YouTube.

СВИДЕТЕЛЬСТВА ПРИМЕНЕНИЯ

Использование видеозаписей с акции само по себе не обязательно означает применение технологии распознавания лиц. В административных делах, связанных с акциями, такие материалы встречались и раньше: их использовали как доказательство массовости акции или

участия в ней конкретного человека. Известны были и случаи задержаний участников спустя несколько дней или недель после события, однако это были, как правило, публичные лица, журналисты или активные участники протестов, которых сотрудники полиции знали в лицо.

В 2021 году видеозаписи стали еще и инструментом идентификации участников. Во-первых, речь идет об определении протестующих на видеозаписях с акций с помощью распознавания лиц — именно на этом аспекте мы фокусируем внимание в настоящем докладе. Кроме того, записи с камер (например, установленных в подъездах или метро) позволяют в дальнейшем определять местонахождение этих людей, чтобы привлекать их к ответственности постфактум.

О применении технологии распознавания лиц свидетельствует, прежде всего, массовость задержаний постфактум и привлечение к ответственности непубличных фигур, а также слова сотрудников полиции.

В некоторых случаях полицейские прямо сообщали задержанным, что их выявили с помощью системы распознавания лиц. Об этом рассказывал, например, депутат Госдумы от КПРФ Сергей Обухов, которого **задержали** в московском метро после встречи с депутатами КПРФ 20 сентября. Полицейские **показали** ему на смартфоне скриншот со сравнением видеозаписи и его старой фотографии.

Хотя применение системы распознавания лиц для поиска протестующих широко освещалось в СМИ после акций января 2021 года, в официальных документах технология упоминается редко. Подобные упоминания мы нашли лишь в шести постановлениях судов первой инстанции по «митинговой» статье 20.2 КоАП в 2021 году. В четырех делах словосочетание «распознавание лиц» использует защита, еще в одном речь идет о «средствах системы отслеживания личности по фотографии» — они

перечислены в перечне доказательств, представленных полицейскими.

Вот как **описана** работа технологии распознавания лиц в одном из описываемых постановлений, со слов сотрудника полиции [сохранены орфография, пунктуация и лексика оригинала]:

«Камера подключена к системе распознавания лиц. Лицо „прикрепляется“ к определенному времени и указывает на процент схожести. Камеры были установлены в тех местах, где проходило публичное мероприятие. Материал им составлялся на основании рапорта старшего оперуполномоченного 11 отдела УУР ГУ МВД России по [адрес отдела и ФИО привлекаемого лица] и предоставленных видеоматериалов. Из видеоматериала следует, что [ФИО привлекаемого лица] в составе группы граждан, скандировавших лозунги и несущих плакаты, принимал участие в публичном массовом мероприятии».

В шестом доступном нам деле, которое можно связать с системой распознавания лиц, говорится о «биометрической идентификации лица».

Малочисленность прямых доказательств применения технологии распознавания лиц в протоколах, материалах дел и судебных постановлениях может свидетельствовать о том, что полиция и суды предпочитают официально не документировать эту информацию. Тем не менее в некоторых документах встречаются косвенные признаки использования технологии:

- изображения с указанием вероятности схожести в процентах;
- упоминание московской «Подсистемы автоматической регистрации сценариев индексирования видеoinформации»
- свидетельства полицейских о том, что участие конкретного человека в акции установил московский Департамент информационных технологий, который затем передал эту информацию в МВД.

Как объяснил ОВД-Инфо разработчик алгоритмов распознавания Юрий Мальков, поначалу систему обучают на большом массиве фотографий в открытом доступе — например, на лицах известных людей. Она учится сопоставлять два изображения и оценивать, насколько они схожи между собой. «Это не бинарное „да“ или „нет“. Система обучается так, чтобы предсказать вероятность [схожести изображений]», — поясняет Мальков.

Далее, чтобы опознать конкретного человека на видео с уличных камер, достаточно показать системе одну или несколько фотографий с его лицом. Система сравнит эти изображения с лицом неизвестного на записи с камеры и выдаст вероятность схожести в диапазоне от 0 до 100%.

В разговоре с ОВД-Инфо Юрий Мальков и другой разработчик алгоритмов распознавания Егор Бурков сошлись во мнении, что в плохо обученной системе больше ложноположительных результатов.

Адвокат и юрист проекта «Роскомсвобода» Екатерина Абашина отмечает, что нигде точно не указан необходимый процент сходства между двумя изображениями, чтобы это послужило основанием для применения к человеку каких-либо мер воздействия, например, проведения дополнительных оперативно-

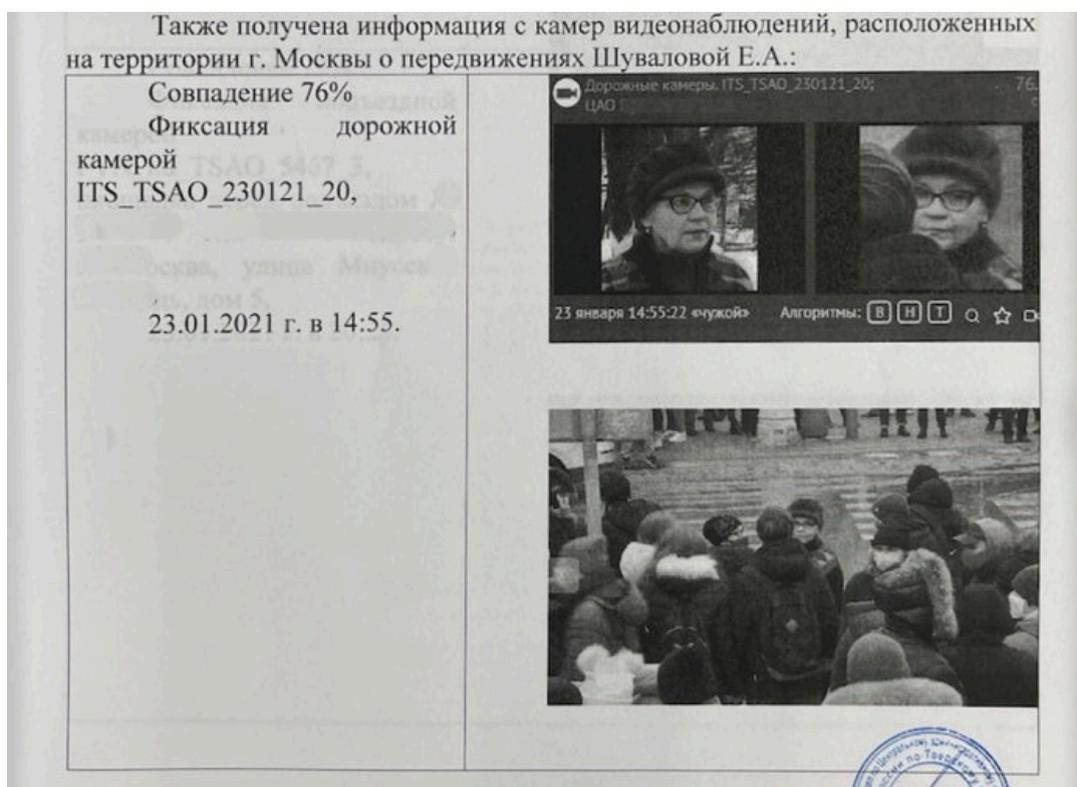
разыскных мероприятий или возбуждения дела об административном правонарушении.

В материалах административных дел после митингов изображения с видеокамер оформляются в виде фототаблиц. Типичная такая таблица выглядит как расположенные рядом скриншот видеозаписи с камеры (чаще всего городского видеонаблюдения) и фотография лица предполагаемого участника акции. Иногда в материалах оставляют только скриншот, а нужное лицо в толпе обводят ручкой.

В случаях, когда в деле есть скриншот видеозаписи, может быть, хотя и не обязательно, указан источник: в Москве это обычно Департамент информационных технологий (ДИТ) или Единый центр хранения данных (ЕЦХД). В других регионах это будет «Безопасный город». В некоторых случаях на изображении видно название камеры, по которому можно установить ее местоположение.

Иногда внизу скриншота присутствуют названия использованных алгоритмов, в редких случаях в материале бывает указана вероятность схожести изображений.

Например, в протоколе по статье о помехах движению во время публичного мероприятия (ч. 6.1 ст. 20.2 КоАП), составленном 2 марта 2021 года на автора телеграм-канала «Протестный МГУ» Дмитрия Иванова, указана вероятность схожести лица на фотографии и видеозаписи в 77,87%, а также упоминается название алгоритма. Иванова узнали, несмотря на наличие медицинской маски.



В протоколе, составленном на депутата Мосгордумы Елену Шувалову, фигурировал процент схожести лица на видеозаписи и на фотографии.

В материалах дела говорится, что факт присутствия Иванова на акции в поддержку Навального 23 января «был установлен с помощью „PARSIVE ГИС ЕЦХД“». «ПАРСИВ» — **подсистема** автоматической регистрации сценариев индексирования видеоинформации.

В 2019 году ГУ МВД России по Москве в информационно-аналитической записке о результатах оперативно-служебной деятельности московской полиции **сообщало**, что «ПАРСИВ 2.0» — это модуль, использующийся в «Безопасном городе» (ЕЦХД) для видеоаналитики, который также «активно используется сотрудниками полиции в оперативно-служебной деятельности». По словам авторов записки, модуль «ПАРСИВ 2.0» сокращает время обработки видеоархива и позволяет просматривать и идентифицировать людей с помощью камер в подъездах.

Мы нашли упоминание системы «ПАРСИВ» еще в семи судебных постановлениях, касающихся привлечения граждан к ответственности в связи с публичными

мероприятиями. «ПАРСИВ» также фигурировал в некоторых **постановлениях**, вынесенных в связи с нарушениями санитарно-эпидемиологических норм в 2020 году.

В одном из доступных ОВД-Инфо дел в отношении жителя Нижнего Новгорода на скриншоте видеозаписи также присутствовала надпись, указывающая на вероятность схожести: 78%. Подобные проценты вероятности схожести присутствуют и в некоторых других материалах дел.

ИСТОЧНИКИ ИЗОБРАЖЕНИЙ

Как минимум с **2012 года** участников акций **незаконно** фотографируют в отделах полиции. Данная практика успела укорениться и приобрела массовый характер. Так, задержанные на акции в поддержку Алексея Навального 21 апреля 2021 года в Санкт-Петербурге **сообщали ОВД-Инфо** о фотографировании в 24 из 48 отделов полиции. В некоторых случаях задержанных принуждают угрозами или силой.

Незаконное фотографирование задержанных — одно из самых распространенных нарушений, происходящих в отделах полиции.

Эксперт по безопасности и технологиям идентификации Transparency International Алексей Шляпужников **отмечает**, что такие кадры могут использоваться при распознавании:

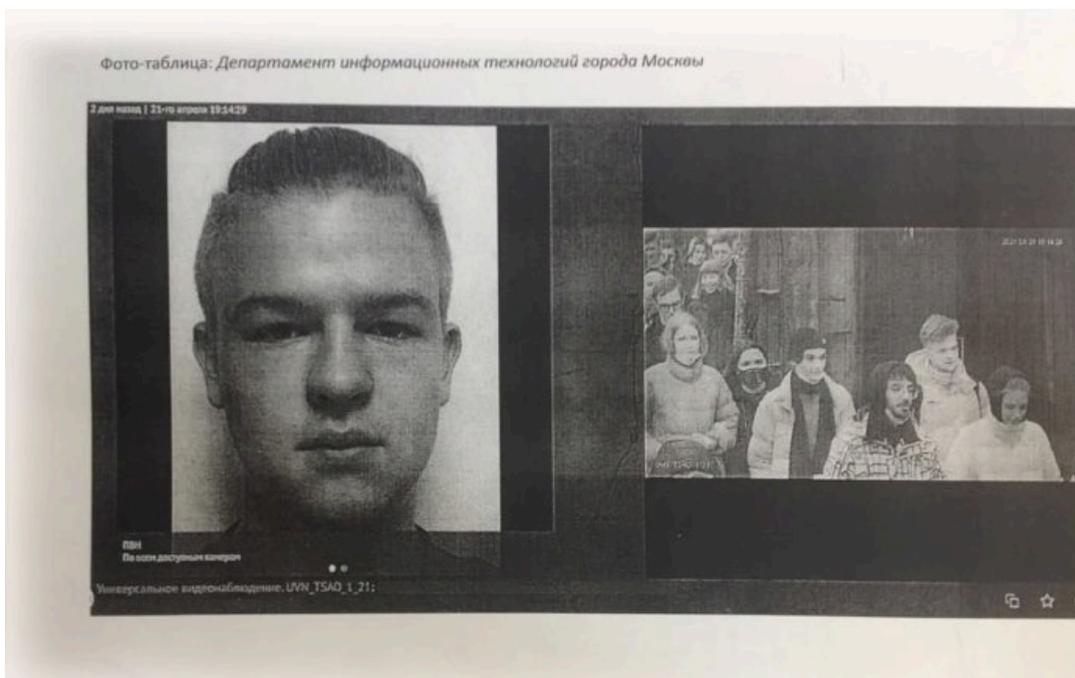
«Система включает модули „Шерлок“ — поиск по базе данных паспортов — и ПСКОВ („Поисковая система категории особой важности“), который работает в том числе с соцсетями. „Шерлок“ и ПСКОВ объединены: чем больше фотографий человека в этой системе, тем проще его найти — фотография на паспорт, на загранпаспорт, в уголовном деле, или человек просто попал в ОВД. Поэтому всех усиленно фотографируют при задержаниях. Чем больше качественных фотографий с разных ракурсов выложено в соцсети, тем проще системе распознать человека. В дела попадают выгрузки из „Шерлока“ без ссылок на соцсети, только с паспортной фотографией. Но, насколько я знаю, для опознания по видео используются все фотографии из личного дела гражданина Российской Федерации».

Тем не менее ОВД-Инфо пока не удалось обнаружить документально зафиксированные случаи использования фотографий, сделанных в отделах полиции, для распознавания лиц. Из 164 человек, обратившихся в ОВД-Инфо, только 37 (23%) были ранее задержаны за участие в других акциях и 16 (10%) из них фотографировали в отделе при предыдущих задержаниях. Невысокая доля таких кейсов свидетельствует о том, что обычно для установления личности использовались фотографии из других источников.

Егор Бурков предполагает, что основой баз поиска могут быть фотографии из паспортов:

«На очень многих людей у органов будет хотя бы одна копия какого-нибудь документа; я уверен, что сейчас основа базы — это фото из паспорта. Но если человек, к примеру, получил паспорт 15 лет назад и с тех пор больше не имел дел с государством, то у них могло не сохраниться ни одного его снимка. Сканировать соцсети слишком неудобно: даже если нужный аккаунт найдется (что уже не совсем тривиально), на выложенных фотографиях могут быть другие люди, — считает Бурков. — Поэтому когда государство лишний раз просит фотографию — например, сейчас на „Госуслугах“ при прибытии из-за границы, — это точно используется для улучшения базы».

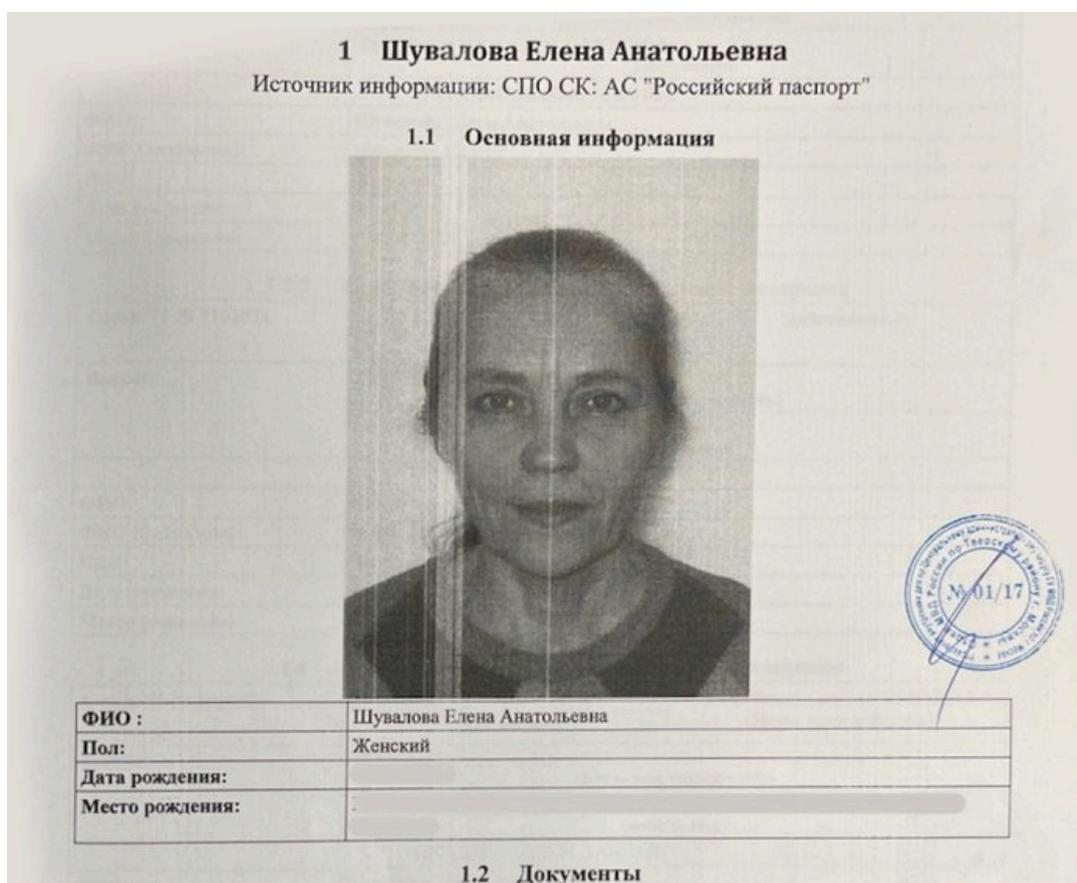
Работая с делами, в которых участников акций привлекали к ответственности постфактум, ОВД-Инфо обнаружил, что для сравнения используются фотографии из паспортов или социальных карт, в некоторых случаях — фотографии из уже недействительных паспортов. Участники протестов, обратившиеся в ОВД-Инфо после апрельской акции, рассказывали также об использовании фотографий из загранпаспортов и социальных сетей.



В протоколе, составленном на предполагаемого участника акции 21 апреля, для сравнения использовалась его фотография из социальной карты (слева).

В доступных нам материалах дел и судебных постановлениях упоминались выписки из баз данных, используемых полицейскими для хранения фотографий из паспортов:

- АС «Российский паспорт», в которой хранятся данные как раз о недействительных паспортах;
- Информационно-поисковая система «Следопыт-м»;
- Интегрированный банк данных регионального или федерального уровней (ИБД-Р и ИБД-Ф), в котором хранится паспортная информация граждан, информация о месте жительства, о случаях привлечения к ответственности в прошлом;
- Сервис обеспечения охраны общественного порядка (СООП).



Для сравнения участницы зимней акции с лицом Елены Шуваловой использовалась ее фотография из недействительного паспорта, из АС «Российский паспорт».

Эксперты считают, что для большей точности полиция может принимать во внимание и другие данные: например, отслеживая с помощью транспортных карт в метро пассажиров, побывавших на той или иной станции в определенное время, или фиксируя местоположение людей с помощью телефонных биллингов.

«Делается это для того, чтобы сравнивать не с миллионным населением всей Москвы, допустим, а с десятками тысяч, которые были в этом месте согласно биллингу телефонов. Это должно сильно увеличивать точность поиска с помощью распознавания лиц», — считает руководитель Computer Vision and Machine Learning Антон Мальцев.

ВОЗБУЖДЕНИЕ ДЕЛА

Если человек, посетивший акцию, запечатлен камерой видеонаблюдения, на него уже после акции могут завести административное дело. По словам опрошенных нами экспертов, такая вероятность возрастает, если участник акции посмотрел в камеру напрямую — в таком случае алгоритму проще распознать лицо.

Пока с задержаниями постфактум сталкивается небольшая доля митингующих. Так, даже если опираться на официальные данные (где часто занижают массовость протестов), в акции 21 апреля в Москве **участвовали** около шести тысяч человек, то есть значительно больше, чем число привлеченных впоследствии к административной ответственности.

ОВД-Инфо известно о привлечении к ответственности как через два дня, так и спустя более чем **пять месяцев** после акции.

Траектория возбуждения дела может быть разная. В одних случаях, согласно найденным нами судебным постановлениям, подразделение полиции само обращается к источникам видеозаписей (в Москве это Департамент информационных технологий или Единый центр хранения данных, в других городах — АПК «Безопасный город») с запросом; в других документах говорится, что подразделение «получило» видеоматериал.

По крайней мере в одном случае сотрудник Центра «Э», который выступал свидетелем в суде, **заявил**, что записи от 21 апреля Департамент информационных технологий прислал в ЦПЭ уже со списком потенциальных протестующих. Чья это была инициатива изначально — полицейских или ДИТ — осталось неизвестным.

Из судебных постановлений неясно, есть ли какой-то конкретный алгоритм и порядок взаимодействий между

полицией и ДИТ, ЕЦХД или системами «Безопасного города». По всей видимости, все три последние структуры могут предоставлять записи по запросу силовиков, но в Москве ДИТ выступает их главным источником.

Согласно **постановлению** Московского городского суда по жалобе на решение судьи Замоскворецкого суда, Департамент информационных технологий является «функциональным органом исполнительной власти», осуществляет «функции по разработке и реализации государственной политики в сфере информационных технологий» и выступает оператором ЕЦХД, «государственным заказчиком работ (услуг), связанных с созданием и обеспечением функционирования ЕЦХД, а также координатором деятельности по подключению информационных систем, пользователей информации об объектах видеонаблюдения и предоставлению информации в ЕЦХД».

Таким образом, в ЕЦХД хранятся все видеозаписи и изображения с видеокамер городского наблюдения в Москве, а уже ДИТ, по-видимому, применяет системы распознавания лиц и передает эти данные органам полиции. Из того же постановления:

«Сотрудники ГУ МВД России по Москве, которым предоставлен доступ к ЕЦХД, в целях реализации служебных обязанностей используют систему видеоаналитики на базе ЕЦХД для отождествления лиц, находящихся в федеральном розыске, лиц, которым по решению суда запрещено посещать массовые мероприятия, лиц, находящихся под административным надзором».

При этом, утверждает суд, ДИТ не проводит мероприятий, направленных на установление личности конкретного гражданина:

«В ЕЦХД отсутствуют персональные данные граждан (ФИО и пр.), а также биометрические персональные данные (радужная оболочка глаз, рост, вес и пр.), которые необходимы для установления личности гражданина».

Ограничивается ли как-либо круг подразделений МВД, которые могут запрашивать записи, неизвестно. В судебных постановлениях фигурируют участковые уполномоченные отделов полиции, отделы охраны общественного порядка, Центр противодействия экстремизму, Управление уголовного розыска (например, УУР ГУ МВД России по г. Москве) и Бюро специальных технических мероприятий (БСТМ). В существенной части судебных постановлений рапорты, объясняющие появление видеозаписи в материалах дела, пишут сотрудники Центра «Э». В одном из документов говорилось, что видеозапись была получена полицейскими в рамках проверки по КУСП (Книге учета сообщений о преступлениях, административных правонарушениях и происшествиях). В доступных ОВД-Инфо материалах речь также шла об исследовании видеозаписи в ходе оперативно-разыскных мероприятий.

ВЫЗОВ ИЛИ ДОСТАВЛЕНИЕ В ОТДЕЛ

После идентификации предполагаемого участника акции полиция предпринимает усилия, чтобы он прибыл в отдел, где составляется протокол об административном правонарушении, затем дело рассматривает суд. На каждом из этих этапов события могут развиваться по-разному.

Особенность привлечения к ответственности с применением распознавания лиц в том, что о намерении полиции составить протокол человек узнает совершенно неожиданно. При этом в отдел его могут доставить принудительно, а могут вызвать в добровольном порядке.

В некоторых случаях полицейские могут давить на человека как перед задержанием, так и после.

Люди, выявленные по камерам после акции 21 апреля, чаще всего сообщали о визитах полицейских по адресу прописки, хотя иногда сотрудники устанавливали и фактический актуальный адрес.

- Так, жителя Москвы пытались привлечь к ответственности из-за акции 21 апреля. Сначала полицейские **пришли** в квартиру его отца, где сам участник митинга прописан не был. Затем сотрудники полиции явились уже туда, где он жил фактически, а когда не нашли его и там, стали звонить по телефону, требуя «срочно явиться в отдел». В отделе мужчину задержали.
- По нашим данным, по крайней мере к одному участнику протестной акции пришли домой, пока он болел коронавирусом. Полицейские заставили мужчину выйти из квартиры и на лавочке около дома составили протокол за участие в акции (ч. 5 ст. 20.2 КоАП), показав материалы дела с фотографиями и скриншотами видеозаписей, где он находится в толпе протестующих.

Еще в одном случае силовики **приехали** на загородную дачу. Ко многим людям полицейские приходили домой **ранним утром** или **поздним вечером**.

Когда люди отказывались открывать дверь или явиться в отдел полиции, к ним могли применять различные меры принуждения. В некоторых случаях обратившиеся в ОВД-Инфо сообщали о применении силы или угрозах со стороны полиции.

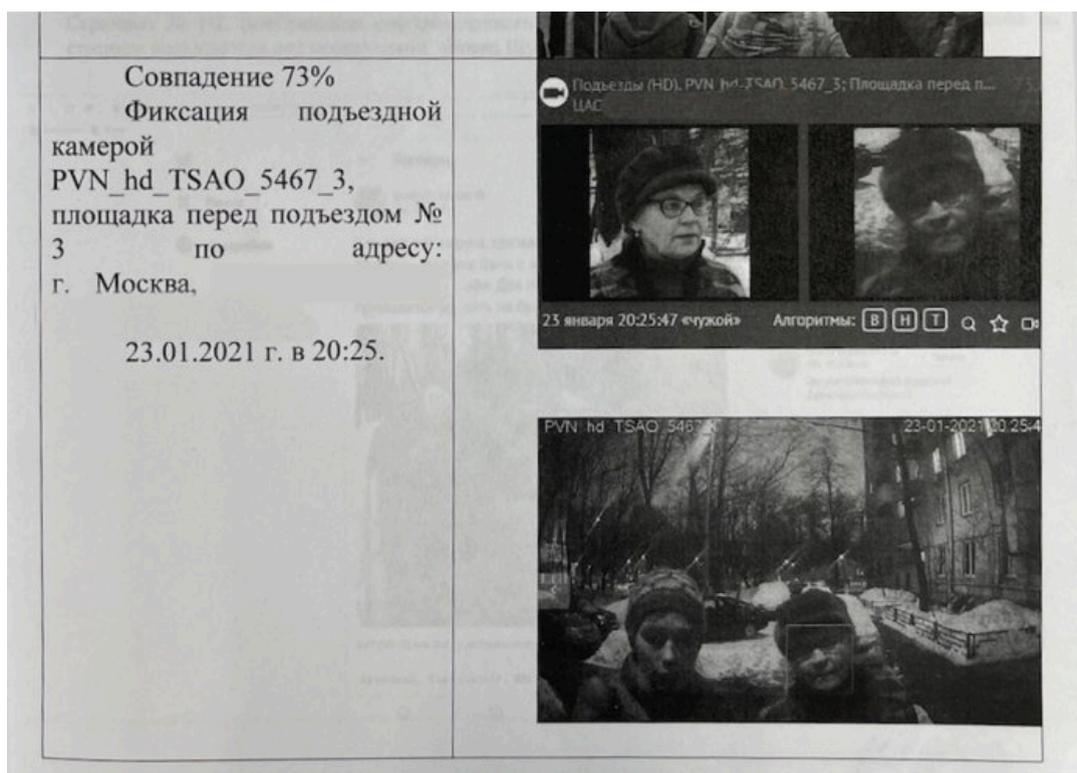
- В Нижнем Новгороде 23 апреля **задержали** местного жителя: около дома его встретили мужчины в штатском, без объяснений отняли телефон и затолкали в «газель», и там держали его лицом в пол до доставления в отдел полиции.
- Один из участников протестной акции в Москве рассказал ОВД-Инфо, что полицейские сначала долго зазывали его в отдел для составления протокола, а когда он не явился, пришли к нему домой и, по словам его жены, стали «ломиться» в квартиру. Когда мужчина приехал домой, его задержали с применением силы и увезли в полицию.
- Другого жителя Москвы полицейские, в том числе в штатском, **поджидали** в течение недели в подъезде дома, а также постоянно звонили на мобильный телефон.
- Иногда силовики специально вводили потенциальных задержанных в заблуждение. В мае жительнице Москвы, преподающей скалолазание, **позвонил** неизвестный мужчина. Он сказал, что хочет отдать ребенка в секцию, и попросил о встрече, где женщину встретили люди в гражданском и повезли в отдел полиции для составления протокола.
- Еще одним методом воздействия на протестующих стало давление на родственников. Так, москвичка рассказала ОВД-Инфо, что полицейские вызывали ее в отдел полиции на составление протокола, а когда она отказалась, приехали к ее 81-летнему отцу и там стали угрожать приехать с нарядом полиции, если она не приедет. Женщине пришлось явиться в отдел самой.

- В другом случае, по нашим данным, ради встречи с предполагаемой участницей акции силовики ввели ее в заблуждение с помощью других людей. Студентку из Москвы вызвали в отдел полиции на составление протокола, она отказалась приходить без повестки. Тогда ей позвонила декан вуза и попросила зайти. Когда студентка явилась, вместе с сотрудницей университета ее ждала полиция.

Людей, которых полиция подозревала в участии в акциях, задерживали прямо **на рабочем месте**, **снимали** с пар в институте, одного человека **забрали** прямо с урока в школе. Известны случаи задержаний в кафе, на улице, в метро, на перроне и в поезде:

- По информации ОВД-Инфо, по крайней мере одного человека сняли с поезда, потому что заподозрили в участии в акции 21 апреля. По словам задержанного, у силовиков были четыре видеозаписи, по которым они не могли с точностью определить участника акции. Мужчина вместе с адвокатом написал объяснительную, что не участвовал в акции, и его отпустили.
- Еще один человек рассказал нам, что его задержали на перроне сразу по приезде в Москву из Санкт-Петербурга. До этого полицейские несколько дней приходили к нему домой по адресу прописки, искали мужчину по месту фактического проживания. При задержании правоохранитель с телефона продемонстрировал мужчине видеозапись с митинга, на которой тот был запечатлен.
- Несколько человек **задерживали** постфактум на выходе из метро. После выборов 17–19 сентября и акций по их итогам в Москве с преследованиями столкнулись члены КПРФ. Часть из них **задержали** прямо в метро, по крайней мере одному задержанному полицейские сообщили, что нашли его по распознаванию лиц, и **показали** на телефоне сравнение скриншота видеозаписи и фотографии.
- Спустя несколько дней после акции 21 апреля в Москве к врачу-гастроэнтерологу на улице **подошел** участковый, задержал его и доставил в ОВД для составления протокола. К другой жительнице столицы полицейские несколько раз приходили домой, вызывая в отдел, а в итоге ее задержали на улице, угрожая силой затащить в машину. В Хабаровске местного жителя задержали после акции 21 апреля, когда он рано утром сел в машину, чтобы отвезти членов семьи на работу и учебу. Дорогу им перегородил полицейский автомобиль.

Задержания на перронах, в кафе и съемных квартирах могут свидетельствовать о применении в отношении преследуемых участников акций систем, отслеживающих перемещения по городу. Для поиска могут применяться записи с подъездной камеры: например, в материалах дела Дмитрия Иванова фигурировали видеозаписи с подъездной камеры дома, где живет активист.



В материалах дела, возбужденного на Елену Шувалову, присутствовал скриншот видеозаписи, полученной с подъездной камеры, где живет депутат.

- По данным ОВД-Инфо, одного из участников протестной акции, проживающего в Москве, вызвали по месту прописки на составление протокола. В отделе полицейский показал ему с приложения WhatsApp в телефоне снимок с камеры из подъезда. Хотя к делу скриншот не приобщили, происходящее сопровождалось словами: «Мы знаем, где ты живешь».
- Муниципального депутата Донского района Москвы Владимира Залищак задержали 2 февраля на станции метро «Крылатское» из-за присутствия на митинге 23 января. В рапорте **говорилось**, что «системой распознавания лиц „Фейс контроль“, установленной на валидаторе восточного вестибюля станции метро „Крылатское“, установлен гражданин [ФИО], за которым был установлен контроль как за лицом, нарушившим установленный порядок» проведения акции.

Из 164 человек, опрошенных ОВД-Инфо после акции 21 апреля, 33 были отпущены без протокола, потому что, например, возникали **технические неполадки** или показать видео в отделе было невозможно, либо когда полицейские затруднялись идентифицировать протестующих на изображениях с людьми, пришедшими в отдел.

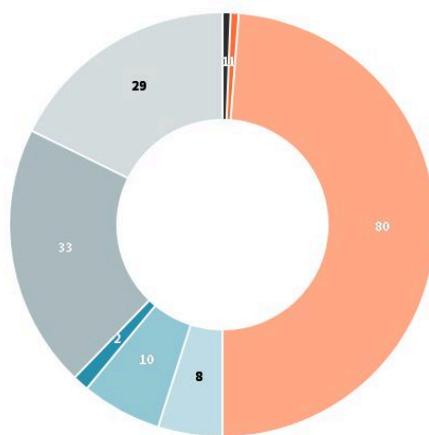
В некоторых случаях задержанным **приходилось** писать объяснительные, что на видео не они, в других адвокату **удавалось** доказать, что его подзащитный находился в это время в другом месте. Было и так, что адвокату **пришлось** привести двух свидетелей, подтвердивших, что его подзащитной не было на митинге.

Большинству из опрошенных ОВД-Инфо (99 из 164 человек) вменили нарушение порядка проведения акции — статью 20.2 КоАП. Чаще всего речь шла о сравнительно мягкой 5-й части этой статьи, по которой привлекают рядовых участников акции и которая не предполагает административного ареста. Реже вменяли части 6.1 (о помехах движению или

транспорту) и 8 (о повторном нарушении закона о митингах) — они как раз предусматривают арест в качестве наказания. Помимо 20.2 КоАП, применялись и другие статьи: мы знаем как минимум о двух случаях 20.6.1 КоАП (невыполнение правил режима повышенной готовности) и об одном случае 19.3 КоАП (неповиновение законному распоряжению сотрудника полиции).

Распределение по вменяемым статьям преследуемых за участие в акции 21 апреля на основании фото и видео

- ст. 19.3 ч.1 КоАП РФ
- ст. 20.2 КоАП РФ (часть неизвестна)
- ст. 20.2 ч.5 КоАП РФ
- ст. 20.2 ч.6.1 КоАП РФ
- ст. 20.2 ч.8 КоАП РФ
- ст. 20.6.1 ч.1 КоАП РФ
- без статьи
- нет данных



Made with Flourish • Create your own

В случае составления протокола по «арестной» статье многих задержанных не отпускали сразу, а **оставляли** в отделе до суда. Артема Пугачева, студента, которого отвезли в полицию из общежития, оставили на двое суток в отделе, а после — назначили административный арест на 10 суток.

- Через пять дней после акции 21 апреля в Москве **задержали** профессора РГГУ Александра Агаджаняна. Его оставили в отделе полиции на ночь, несмотря на то что у него астма и к нему приезжали врачи. На следующий день суд признал его виновным в участии в митинге, повлекшем нарушение движения транспорта (ч. 6.1 ст. 20.2 КоАП), и назначил ему штраф в размере 20 тысяч рублей.
- 24 сентября **задержали** участника встречи с депутатами КПРФ 20 сентября Олега Юрасова. На него составили протокол по статье о повторном нарушении правил проведения акции (ч. 8 ст. 20.2 КоАП) и оставили в отделе на 48 часов, а в суде оштрафовали на 150 тысяч рублей.

СУД: НАКАЗАНИЯ, ПРЕКРАЩЕНИЯ И ВОЗВРАТЫ

Как и людей, задержанных прямо на акциях, тех, кого задержали постфактум, скорее всего, ждет штраф, обязательные работы или административный арест. ОВД-Инфо знает по крайней мере об одном случае, когда задержание после акции привело к довольно серьезному по административным меркам наказанию: по статье о повторном нарушении закона о митингах (ч. 8 ст. 20.2 КоАП) Измайловский суд арестовал участника акции 21 апреля на 25 суток.

Бывает и так, что человека нашли по видеозаписи, но суд возвращает дело в полицию или даже прекращает его.

За период с января по 20 июля 2021 года среди доступных дел, в которых есть признаки применения распознавания лиц, нам удалось найти 6 прекращенных и 10 возвращенных в полицию для устранения недостатков ([подробнее о методологии](#)). Все постановления о прекращении производства вынес один

судья Зеленоградского районного суда Москвы в один день. Еще одно дело этот же суд вернул в полицию; пять дел вернул в полицию Перовский суд.

В качестве причин прекращения дела в постановлениях чаще всего указывали ошибки в протоколах, отсутствие состава правонарушения и истечение сроков давности. Иногда дела **прекращала** сама полиция — в связи с тем, что не находила человека на видео и фотографиях. В некоторых случаях судьи отказывались считать установление личности по видеозаписям достаточным доказательством. Подробнее об этом — в разделе **«Оформление материалов административных дел»**.

Почти всегда суды второй инстанции оставляли решения без изменений. Только в некоторых случаях они **прекращали** рассматриваемые в настоящем докладе дела: причинами и здесь становились ошибки в протоколах или сроки давности.

СИСТЕМА РАСПОЗНАВАНИЯ ЛИЦ В КОНТЕКСТЕ СВОБОДЫ СОБРАНИЙ

Сам по себе сбор данных об участниках протестов со стороны государства создает риск политически мотивированных преследований.

На эту проблему в 2020 году обратил внимание Комитет по правам человека ООН. По мнению Комитета, критически важным вопросом является «независимый и прозрачный контроль и надзор за решениями о сборе личной информации и данных по лицам, участвующим в мирных собраниях, а также за обменом ими или их хранением». Указанные Замечания распространяются и на Россию как участницу Международного пакта.

Проблемы, связанные с использованием систем уличного видеонаблюдения и системы распознавания лиц,

возникающие именно в контексте свободы собраний и выражения мнения, в 2020 году отмечала также Верховный комиссар ООН по правам человека Мишель Бачелет в своем докладе, посвященном влиянию современных технологий на права человека.

- Это, прежде всего, лишение участников собрания некоторой степени анонимности, которая является частью коллективного действия, и массовое вмешательство в частную жизнь людей, происходящее из-за неизбирательности процесса распознавания лиц — все люди, находящиеся на улице во время протеста, подвержены угрозе идентификации властями. Как следствие, ощущение постоянного наблюдения и возможность такой идентификации оказывает сдерживающий эффект на потенциальных участников собраний, которые могут ограничивать себя в выражении мнения или вообще отказаться от реализации своих прав на собрания и выражения.
- «Властям, как правило, следует воздерживаться от записи изображений участников собраний, — отмечается в документе со ссылкой на Руководящие принципы ОБСЕ. — В соответствии с требованиями соразмерности исключения следует рассматривать только в тех случаях, когда имеются конкретные указания на <...> серьезные уголовные преступления или имеются основания подозревать неминуемое и серьезное преступное поведение, такое как насилие или применение огнестрельного оружия. Существующие записи должны использоваться только для идентификации участников собрания, подозреваемых в совершении тяжких преступлений».

Данные соображения должны учитываться законодателем при установлении правового регулирования вопроса, и судами, которые разбирают конкретное дело, соотнося баланс различных прав и интересов и оценивая

негативные эффекты для фундаментального права на свободу собраний.

В январе 2021 года Консультативный Комитет при Совете Европы разработал руководящие принципы для технологий распознавания лиц при реализации Конвенции о защите частных лиц в отношении автоматической обработки персональных данных, которая ратифицирована и Россией. В них, в частности, устанавливаются минимальные требования к законодательству о системе распознавания лиц:

- подробное объяснение примеров использования и его цели;
- некоторая надежность и точность используемого алгоритма;
- срок хранения использованных фотографий;
- возможность проверки этих критериев;
- отслеживаемость процесса.

Кроме того, Комитет отмечает, что использование общедоступных изображений для идентификации лиц или создания баз данных не может быть законным только на основании их общедоступности — то есть если фотографии размещены в социальных сетях. Органы власти должны гарантировать, что такие изображения не будут использоваться без надлежащей правовой основы — например, только при подозрении в серьезных преступлениях.

Необходимость прозрачного правового регулирования использования камер уличного наблюдения **отметила** также Венецианская комиссия — экспертный орган по мониторингу законодательства и правоприменительной практики в сфере прав человека при Совете Европы. Положительным опытом, по мнению

Венецианской комиссии, является учреждение в некоторых странах специальных независимых органов, которые следят за соответствием государственного регулирования и практики международным стандартам в области защиты персональных данных.

В практике Европейского суда по правам человека пока еще нет правовых позиций по вопросу использования системы распознавания лиц в отношении участников протестных акций.

В начале 2020 года юрист Александра Россиус подала в ЕСПЧ жалобу в связи с **задержанием** в московском метро активиста Николая Глухина, который ранее провел пикет с картонной фигурой обвиняемого по «дадинской» статье (212.1 УК) Константина Котова. Доказательства против него включали в себя записи с камер видеонаблюдения в метро; сам Глухин предположил, что его идентифицировали с помощью распознавания лиц. По словам активиста, для его поиска использовалась технология распознавания лиц. 23 июня 2021 года ЕСПЧ **коммуницировал** жалобу.

Юристы Межрегиональной ассоциации правозащитных организаций «Агора» **поставили** перед ЕСПЧ вопросы о нарушении права на уважение частной и семейной жизни, ограничении свободы собраний из-за массового использования системы распознавания лиц без согласия людей. Заявители — активистка Алена Попова и политик Владимир Милов — до этого безуспешно обжаловали в российских судах использование видеонаблюдения и системы распознавания лиц во время митинга в поддержку обвиняемых по «московскому делу» в сентябре 2019 года.

Вместе с тем ЕСПЧ в различных решениях сформулировал ряд важных правил, которые можно применять и в вопросах использования распознавания лиц.

- Даже в публичном пространстве может иметь место нарушение права на частную и семейную жизнь, в том числе в случае использования камер видеонаблюдения, особенно если речь идет о сохранении и передаче видеозаписей и снимков, обработки их для идентификации конкретного человека, а также в случае использования видеозаписей для целей, выходящих за пределы обычных ожиданий.
- Использование видеонаблюдения должно быть обосновано легитимной необходимостью и пропорционально этой необходимости, а также урегулировано законодательно таким образом, чтобы было четко установлено, в каких случаях и в какой мере допустимо видеонаблюдение, на какой срок, как решение о видеонаблюдении пересматривается и обжалуется.

В жалобе приводится пример действующего на территории Евросоюза регламента, запрещающего сбор биометрических персональных данных без прямого согласия людей, что предотвращает массовое использование системы распознавания лиц.

В судебной практике стран — участниц ЕС есть решения, где использование системы распознавания лиц признавалось нарушающим право на свободу выражения мнений и собраний. Кроме того, применение средств слежения в публичном пространстве может признаваться нарушением права на частную жизнь.

Кроме общих международных проблем, в отечественных реалиях актуальны следующие правовые вопросы:

- проблема со сроками хранения записей с камер, регулирования доступа к ним и, как следствие, практическая возможность утечки данных и их произвольного использования;
- обработка биометрических данных граждан без их согласия;
- использование и оценка результатов применения системы распознавания лиц в качестве доказательств по делам об административных правонарушениях;
- отсутствие механизмов правовой защиты жертв неправового использования системы распознавания лиц.

Ниже мы подробнее рассматриваем все эти проблемы.

ХРАНЕНИЕ И ДОСТУП К ДАННЫМ С ГОРОДСКИХ КАМЕР

В Москве данные со многих камер городского наблюдения стекаются в ЕЦХД, собственником которого является городской Департамент информационных технологий (ДИТ).

Круг субъектов, которые могут обратиться к данным городского видеонаблюдения, крайне широк: «Доступ в ЕЦХД для получения информации в режиме реального времени предоставляется высшим должностным лицам субъектов Российской Федерации и уполномоченным ими лицам, федеральным органам государственной власти, органам государственной власти города Москвы, организациям в целях осуществления своих функций и полномочий согласно их компетенции». Кроме того, четко не описаны обстоятельства, при которых возможно использование ЕЦХД — а значит, все перечисленные лица и органы власти имеют право обращаться к описываемым данным практически безгранично.

ДИТ **подчеркивает**, что сотрудники правоохранительных органов имеют доступ к городской системе видеонаблюдения только со своих рабочих мест и «в целях осуществления ими своих полномочий». Доступ осуществляется по персональным учетным записям, «при выдаче которых пользователи подписывают документ о неразглашении конфиденциальной информации, а также о недопустимости передачи логина и пароля третьим лицам».

Все факты доступа к информации, содержащейся в ЕЦХД, в том числе факты демонстрации архивной информации и факты ее сохранения на внешних электронных носителях, регистрируются в журналах учета доступа к информации.

Формально срок хранения данных с камер ограничен. Как **указано** на сайте ДИТ, для камер подъездного и дворового видеонаблюдения это пять календарных дней, для камер видеонаблюдения в местах массового скопления граждан — тридцать. В регламенте доступа к ЕЦХД от 2015 года также **уточняется**, что в случае, если данные будут зарезервированы, они хранятся в базе дополнительно тридцать дней, «после чего автоматически удаляются».

- Протоколы на участников зимних акций продолжают составлять и более чем через полгода после акции. Последний известный ОВД-Инфо случай **произошел** 25 ноября.

Помимо доступа к городским камерам наблюдения, в распоряжении сотрудников полиции есть еще ряд баз данных с информацией о паспортах, месте регистрации и истории привлечения к административной ответственности конкретных людей с паспортными фото (подробнее об этом см. раздел **«Источники изображений для идентификации протестующих»**).

Этих двух блоков данных (видео с акций и фотографии человека с привязкой к личности) достаточно для массового распознавания лиц, они — ключевой инструмент для определения и поиска предполагаемых участников акций.

Проблемы с хранением данных с видеокамер наглядно иллюстрирует кейс жительницы Москвы Анны Кузнецовой, который сопровождали юристы проекта «Роскомсвобода».

Летом 2020 года Кузнецова **обнаружила услугу** в даркнете по предоставлению данных с камер городского наблюдения, которые запечатлели интересующего покупателей человека. Женщина в рамках эксперимента заказала данные по собственному изображению. После оплаты она получила отчет с результатом от 79 столичных камер с указанием адресов, где она была в течение последнего месяца. В рамках уголовного дела двое сотрудников столичной полиции **признали** вину и получили судебные штрафы 10 и 20 тысяч рублей (размер штрафов соотносим со стоимостью одного «пробива по лицу»). Само дело суд **прекратил**.

Дело Кузнецовой показывает, что хранящиеся видеоданные не имеют надежной защиты и становятся товаром на черном рынке либо появляются в общем доступе в результате утечки.

Юристы «Роскомсвободы» **потребовали** ввести мораторий на использование системы распознавания лиц, пока не будет обеспечена безопасность граждан от злоупотреблений.

ОБРАБОТКА БИОМЕТРИЧЕСКИХ ДАННЫХ

«Применение технологии распознавания лиц против протестующих является неправомерным, потому что эта технология находится в серой зоне регулирования и нет четких и конкретных правил о том, в каких случаях допустимо ее использовать, — отмечает адвокат и юрист проекта „Роскомсвобода“ Екатерина Абашина. — И это, в частности, связано с тем, что технология распознавания лиц обрабатывает биометрические данные граждан, а по закону о персональных данных это можно делать либо с согласия самого гражданина, либо в тех случаях, которые установлены федеральными законами. И нет [таких] федеральных законов, которые бы установили в качестве допустимого случая сканирование людей во время митингов с целью наложения на них административных штрафов».

Позиция судов и других органов власти, считающих законным применение распознавания лиц для поиска участников акций, основана на трех основных аргументах:

- распознавание лиц участников протестных акций не является обработкой персональных данных.
- камеры записывают информацию о территориях, а не о людях.
- система распознавания лиц используется в целях поддержания правопорядка или в иных публичных интересах;

Все эти аргументы представляются нам несостоятельными. Ниже мы объясним почему.

Распознавание лиц не является обработкой персональных данных

30 апреля на жителя Москвы Андрея Петрухина составили протокол по ч. 6.1 ст. 20.2 КоАП — его посчитали участником акции 21 апреля. В качестве доказательств полицейские использовали фототаблицу и видеозапись с камер, мужчине назначили штраф. В апелляции 18 мая Мосгорсуд **признал** применение технологии распознавания лиц в этом случае законным. По мнению суда, ДИТ на основе ЕЦХД, несмотря на использование системы распознавания лиц, оперирует только изображениями человека, сравнивая именно их; а идентификацию гражданина якобы проводит уже сотрудник полиции. По мнению суда, алгоритм распознавания лиц не работает с персональными данными:

«Алгоритм распознавания лиц, используемый в ЕЦХД, сравнивает изображение, поступающее в ЕЦХД с видеокамер, с фотографией, предоставленной правоохранительным органом. В процессе обработки соответствующих изображений происходит их сравнение на наличие / отсутствие совпадений. Департаменту [информационных технологий] не передаются персональные данные (ФИО и пр.) искомых лиц, поскольку у Департамента нет технической и юридической возможности осуществлять их сопоставление».

Утверждения судов о том, что распознавание лиц не является обработкой персональных данных, противоречит основным понятиям, содержащимся в Федеральном законе «Об обработке персональных данных». Положения о том, что фотография человека относится к биометрическим персональным данным, содержатся как в ФЗ-152 **«О персональных данных»**, так и в **разъяснениях** Роскомнадзора.

- ФЗ относит к биометрическим персональным данным сведения, которые характеризуют физиологические и биологические особенности человека и на основании которых можно установить его личность и которые используются оператором для этого.
- В разъяснениях Роскомнадзора указано, что к таким «характеристикам человека» относятся, в частности, его изображения (фотография и видеозапись), которые позволяют установить его личность и используются оператором для установления личности.
- Согласно позиции Роскомнадзора, до передачи данных фото- и видеосъемки для установления личности они не являются биометрическими персональными данными, поскольку не используются оператором (владельцем видеокамеры или лицом, организовавшим ее эксплуатацию) для подобных целей. Однако они становятся биометрическими персональными данными в том случае, если их обрабатывают с целью установления личности конкретного физического лица.

Вероятность схожести изображений, которая определяется с помощью системы распознавания лиц, приводит к установлению личности гражданина и используется органами именно в этих целях. Поэтому мы считаем, что в данном случае использование системы распознавания лиц — это работа именно с персональными данными человека без его согласия.

Совет Европы в последних поправках к **Конвенции** о защите частных лиц в отношении автоматической обработки персональных данных включил биометрию в особые категории данных, обработка которых требует особенно строгих условий. Биометрические данные при этом в статье 6 Конвенции определены как данные, однозначно идентифицирующие человека.

Согласно российскому законодательству, обработка биометрических персональных данных не допускается без письменного согласия самого человека.

Из этого правила есть исключения, в частности, оперативно-разыскная деятельность и осуществление правосудия. Тем не менее эти исключения не применимы к полномочиям полиции в делах об административных правонарушениях: правосудием занимается только суд, а не полиция, а оперативно-разыскная деятельность проводится только в случае преступления, предусмотренного Уголовным кодексом. Подробнее об этом мы рассказываем в разделе «[Оперативно-разыскные мероприятия и дела об административных правонарушениях](#)».

Камеры следят за территорией, а не за людьми

Еще один аргумент, которым оперируют власти, состоит в том, что камеры следят за территорией, а не за людьми.

- В ответе на **обращение** ОВД-Инфо о неправомерности использования распознавания лиц Уполномоченная по правам человека в Москве Татьяна Потяева, ссылаясь на Гражданский кодекс РФ, заявила, что согласие гражданина на обработку персональных данных не требуется в случаях, когда «изображение гражданина получено при съемке, которая проводится в местах, открытых для свободного посещения, или на публичных мероприятиях».
- По **мнению** Мосгорсуда, «само по себе получение изображения заявителя в период нахождения на территории, попадающей под сектор наблюдения конкретной камеры, установленной в целях контроля за окружающей обстановкой в центре Москвы, не является способом сбора персональных (биометрических данных), поскольку не использовалось непосредственно для определения личности заявителя».

Этот аргумент представляется несостоятельным, так как на видеозаписи попадают люди, лица которых в конечном счете и распознаются. То есть для целей использования системы основным объектом становится именно изображение человека, а не территории.

Распознавание лиц используется в публичных интересах

Рассматривая дело одного из предполагаемых участников акции 21 апреля в Москве, Савеловский суд **вынес обвинительное постановление**, в котором сослался на ФЗ «О полиции» и заявил, что правоохранители в рамках расследований уголовных дел и в отношении административного производства могут запрашивать у различных органов «необходимую информацию».

При этом, по мнению суда, «применение технологии распознавания лиц в городской системе видеонаблюдения

в полной мере соответствует требованиям действующего законодательства, направлено, в частности, на защиту правопорядка, обеспечение безопасности и предоставление сотрудникам ГУ МВД России по г. Москве доступа к ЕЦХД в указанных выше целях для выполнения возложенных обязанностей» и не нарушает прав человека на частную жизнь.

Московская Уполномоченная по правам человека Татьяна Потяева солидарна с судами и считает, что «применение указанной технологии и использование ее правоохранительными органами не носят произвольного характера, а имеют цель обеспечения безопасности населения Москвы и фиксации правонарушений».

И Уполномоченная, и Мосгорсуд ссылаются на п. 1 ст. 152.1 Гражданского кодекса, в соответствии с которым согласие гражданина на использование его изображения не требуется, когда оно осуществляется в государственных, общественных или иных публичных интересах или когда такое изображение не является основным объектом использования.

Между тем Гражданский кодекс применим для гражданских правоотношений, а использование изображений граждан сотрудниками правоохранительных органов ими не регулируется.

Правомерная цель поддержания правопорядка не исключает того, что вторжение в сферу прав и свобод граждан должно быть четко предписано законом. А закон не содержит норм, которые разрешали бы обработку персональных данных без согласия гражданина в контексте КоАП.

При этом отсутствие массового применения технологии распознавания лиц ко многим другим типам правонарушений (как, например, переход дороги

в неполюженном месте или безбилетный проезд) свидетельствует, что основной целью применения этой технологии является не защита общественных интересов, а преследование политических оппонентов власти.

ОФОРМЛЕНИЕ МАТЕРИАЛОВ АДМИНИСТРАТИВНЫХ ДЕЛ

Если протокол о правонарушении на человека составили постфактум, а не после задержания на акции, это зачастую означает, что его личность на месте не устанавливалась (хотя иногда паспортные данные полицейские переписывают, например, при проведении пикетов). Поэтому правоохранителям необходимо объяснить, каким образом произошло сопоставление личности между человеком, запечатленным на видеозаписи, и лицом, которое пытаются привлечь из-за участия в несогласованной акции.

Изучив доступные материалы, ОВД-Инфо приходит к выводу, что основных способов сделать это у полицейских существует два:

- 1** указание, что отождествление лиц произошло в ходе «оперативно-разыскных мероприятий»;
- 2** рапорт сотрудника полиции, в котором он заявляет, что «установил» на фотографии и видео конкретного гражданина, без дополнительных пояснений.

Ни в одном из этих случаев полиция «на бумаге» не признает, что для определения личности человека каким-либо образом использовалась технология распознавания лиц. Не исключено, что правоохранители предпочитают лишней раз не документировать применение распознавания лиц именно потому, что оно находится в «серой зоне» российского законодательства.

Оперативно-разыскные мероприятия и дела об административных правонарушениях

Использование распознавания лиц можно отнести к следующим типам **оперативно-разыскных мероприятий**: сбор образцов для сравнительного исследования, наблюдение, отождествление личности, получение компьютерной информации.

- Так, в **административном деле**, возбужденном в отношении москвички в связи с акцией 21 апреля, ссылаясь на ФЗ «Об оперативно-разыскной деятельности», полиция запрашивает провести портретное исследование ее изображения на фотографии из базы «Следопыт-М» и на видеозаписи, полученной правоохранителями из ДИТ. Материалы дела есть в распоряжении ОВД-Инфо.



фотография Петрухин А.П. полученная из информационно-поискового сервиса «Следопыт-М»



скриншот видеозаписи, сделанной 21.04.2021 в 19 часов 22 минут 30 секунды с камеры видеонаблюдения принадлежащей ДИТ Правительства г. Москвы № UVN_TSAO_1_60

Искра
Т.В. МУБАРАНОВ

По следам акции 21 апреля на студента составили протокол, в котором использовалась фотография из базы “Следопыт-М”.

Оперативно-разыскные мероприятия (ОРМ) входят в исключения, **предусмотренные** п. 2 ст. 11 ФЗ «О персональных данных»:

«Без согласия субъекта персональных данных обработка биометрических персональных данных может осуществляться <...> в случаях, предусмотренных

законодательством РФ <...> об оперативно-разыскной деятельности».

То есть в теории в ходе ОРМ полицейские могут обрабатывать персональные данные без согласия человека.

Однако согласно позиции Конституционного суда, оперативно-разыскная деятельность может осуществляться только на основании признаков преступления, предусмотренных Уголовным кодексом:

«Если в ходе проведения оперативно-разыскных мероприятий обнаруживается, что речь идет не о преступлении, а об иных видах правонарушений, то <...> дело оперативного учета подлежит прекращению».

В то же время, по мнению Конституционного суда, оперативно-разыскные действия можно проводить, когда уголовное дело еще не возбуждено, но «уже имеется определенная информация, которая должна быть проверена (подтверждена или отвергнута) в ходе оперативно-разыскных мероприятий, по результатам которых и будет решаться вопрос о возбуждении уголовного дела».

В 2020 году Конституционный суд также выразил мнение о том, что если в результате ОРМ выявлено не преступление, а административное правонарушение, само по себе это «не свидетельствует о незаконности данного оперативно-разыскного мероприятия, о недостоверности его результатов и недопустимости их использования в доказывании правонарушения согласно соответствующему процессуальному законодательству». Аналогичную позицию высказывал

и Верховный суд Чувашии. Однако оба случая касались только одного из видов ОРМ — контрольной закупки, в контексте митингов вопрос не рассматривался.

Конституционный суд не увидел проблем в практике использования материалов оперативно-разыскных мероприятий в административных делах. Однако это не значит, что в каждом конкретном случае суды общей юрисдикции не должны проверять законность и обоснованность действий исполнительных органов.

Согласно Кодексу об административных правонарушениях, не допускается использование доказательств, полученных с нарушением закона — в данном случае, закона «Об оперативно-розыскной деятельности» (орфография сохранена). А согласно этому закону основанием для ОРМ являются «ставшие известными органам, осуществляющим оперативно-разыскную деятельность, сведения о признаках подготавливаемого, совершаемого или совершенного противоправного деяния, а также о лицах, его подготавливающих, совершающих или совершивших, если нет достаточных данных для решения вопроса о возбуждении уголовного дела».

По нашему мнению, в контексте рассматриваемых митингов у полиции не было оснований для проведения ОРМ, так как изначально не было признаков совершенного преступления и признаков проверки по уголовному делу. Как следствие, полученные в ходе ОРМ сведения не являлись допустимым доказательством в рамках дел об административных правонарушениях. Законность проведения ОРМ в рамках конкретного дела должны оценивать суды, однако на практике этого не происходит.

Рапорт сотрудника без указания на ОРМ

Отдельного внимания заслуживает способ приобщения фотографий и видеозаписей с помощью рапорта

сотрудника полиции: якобы тот «установил» на изображениях конкретного гражданина.

При этом в подобных случаях нет ссылок на оперативно-разыскные мероприятия, а также нет ответов на вопрос, как именно удалось установить личность конкретного человека. В рапортах полицейских могут присутствовать указания на то, что видео и фото получены, например, из ДИТ, но не всегда указываются основания этого. Более того, во многих рапортах присутствует формулировка «человек, схожий с».

Подобные доказательства и такое их оформление в материалах дел об административных правонарушениях по-разному оцениваются судами.

В ряде исследованных ОВД-Инфо дел суды не вызывали на допрос сотрудников полиции и способ отождествления лиц просто оставался неустановленным. Таким образом, суды принимали сам рапорт полицейского без дополнительных пояснений как достаточное доказательство.

Тем не менее в некоторых случаях суды критически воспринимали подобные свидетельства.

Причиной возвращений дел в полицию становилось, например, то, что установить человека с помощью представленной правоохранителями видеозаписи невозможно. В Нагатинском районном суде Москвы эксперт, ознакомившись с делом москвича за акцию 21 апреля, **не смогла** идентифицировать его с лицом, фигурирующим в материалах. В Бабушкинском районном суде судья **заявила**, что по видеозаписи невозможно разглядеть участника акции, а поэтому факт нарушения остается недоказанным. По этой же причине Зеленоградский суд **не стал** рассматривать дело человека, которого пытались привлечь за акцию 21 апреля.

Судья Перовского районного суда Москвы в постановлении о возвращении дела **указала**, что в материалах не объясняется, каким образом установили личность привлекаемой к ответственности гражданки:

«...из рапорта оперуполномоченного 1 отделения 8 отдела УУР ГУ МВД России по г. Москве не следует, каким именно образом было установлено, что зафиксированное на видео лицо является именно [ФИО] ... а так же из рапортов УУП ОМВД России по району Ивановское г. Москвы не следует, на основании каких конкретных доказательств должностные лица пришли к выводу о том, что [ФИО]... является лицом, совершившим вменяемое ей правонарушение».

По мнению судьи, из фото- и видеоматериалов при этом следует лишь то, что «прохожие идут по тротуару»:

«Не установлено, кто именно из зафиксированных лиц является (и является ли вообще) ...[ФИО]... личность указанных лиц суду не известна, какими-либо средствами для идентификации данных лиц суд не располагает, в распоряжение суда не представлены конкретные источники установления личности изображенного на фото и видео гражданина».

Судья также указывает, что сотрудники полиции, составившие рапорт, не были очевидцами произошедшего, а значит не могут сказать, была ли обвиняемая на митинге или нет. При этом сама гражданка, которую пытались привлечь к ответственности, свое присутствие на видеозаписи отрицает, как и присутствие на мероприятии.

Из постановлений о прекращении или возвращении дел можно сделать следующий вывод: ключевой проблемой для привлечения к ответственности протестующих с помощью распознавания лиц является вопрос

установления личности на изображении и идентификация конкретного человека с этим изображением.

Без упоминания этой технологии или конкретных оперативно-разыскных мероприятий между человеком в суде и гражданином на видео или фото возникает брешь: доказать, что это одно лицо, становится невозможно.

МЕРЫ ПРАВОВОЙ ЗАЩИТЫ

Адвокат Екатерина Абашина отмечает, что по делам об административных правонарушениях практически единственным способом защиты является ходатайство об исключении из материалов дела недопустимых доказательств. Удовлетворение или игнорирование подобного ходатайства остается на усмотрение судьи.

На примере [дела](#) Анны Кузнецовой становится понятно, что подача административных исков против МВД или профильных городских ведомств пока не приводит к изменению позиции городских властей. [Аргументы властей](#) сводятся к тому, что система распознавания лиц используется в легитимных целях обеспечения общественной безопасности, а собранные данные сами по себе не содержат всех элементов для идентификации конкретного человека — Кузнецова сама предоставила злоумышленникам свою фотографию.

Особой проблемой является и то, что человек, чьи биометрические данные незаконно обрабатываются с использованием системы распознавания лиц, может и не узнать о нарушении, так как в материалах факт применения технологии скрывается. Следовательно, и обжаловать его будет затруднительно.

Специальный докладчик ООН по праву на свободу мнений и их свободное выражение Дэвид Кэй в 2019 году [отметил](#) «отсутствие судебного надзора, средств правовой защиты,

оснований для подачи исков, правоприменения и механизмов обеспечения сохранности данных [полученных в результате использования систем слежения]». В связи с высокой степенью угрозы для свободы выражения мнений и частной жизни и отсутствием прозрачного глобального и государственного регулирования, Спецдокладчик рекомендовал странам «незамедлительно ввести мораторий на экспорт, продажу, передачу, использование или обслуживание разработанных частным образом средств слежения до тех пор, пока не будет установлен режим гарантий, предусматривающий защиту прав человека».

ПРОБЛЕМЫ ПРЕСЛЕДОВАНИЯ ПОСТФАКТУМ

Раньше главный риск для участников акций заключался в возможности задержания непосредственно на мероприятии. Применение камер и системы распознавания лиц делает преследование менее предсказуемым и несет в себе дополнительные риски.

Преследование постфактум сопряжено с серьезным вторжением в частную жизнь и влиянием на другие сферы жизни, не связанные с гражданской активностью. Полицейские могут приходить как по прописке, так и по актуальному месту жительства. По крайней мере в двух известных ОВД-Инфо случаях полицейские нарушили неприкосновенность жилища: в одном, оттолкнув мать участника акции, они прошли к нему в комнату, в другом — проникли в комнату студента в общежитии.

Визиты полицейских на учебу или работу имеют маргинализирующий эффект для участника акции:

существует риск, что соученики или коллеги станут хуже к нему относиться, его могут исключить или уволить.

Публичное задержание человека в его привычной среде, в окружении коллег, соседей, одноклассников или однокурсников может привести к дискриминации даже если полиция и алгоритмы ошиблись.

При этом подобное задержание не является исключительной мерой и не соответствует требованиям КоАП — почему подозреваемого в административном правонарушении нельзя вызвать в отдел полиции в установленном законом порядке?

- Например, Леонида Гозмана **задержали** через пять дней после акции 21 апреля в отделе полиции, куда его вызвал участковый в связи с его обращением в Следственный комитет. В отделе ему показали видеозапись от 21 апреля, где видно, что он идет по Тверской улице, и составили протокол о нарушении при участии в акции (ч. 5 ст. 20.2 КоАП). В отделе его **продержали** до позднего вечера. Суд рассмотрел дело месяц спустя и **назначил** штраф.

Иногда в отношении задержанных постфактум сразу применяют арест. Эта практика противоречит позиции ЕСПЧ, который обращает внимание на необходимость отсрочки исполнения ареста в делах об административных правонарушениях до апелляции. В тех случаях, когда человека задерживают постфактум, необходимость незамедлительного исполнения ареста представляется еще менее обоснованной, чем при задержаниях на акциях.

В отличие от большинства административных статей, срок привлечения к ответственности по самой распространенной «митинговой» статье 20.2 КоАП **составляет** не три месяца, а один год. То есть в течение года после акции на ее участников могут составить протоколы и назначить им наказание. Если раньше такие

риски возникали только для задержанных на акции, то теперь с ними может столкнуться любой из участников. В результате на протяжении продолжительного времени участники собраний находятся в ожидании возможного задержания.

Если в течение полугода трижды вступило в силу решение суда по административной ответственности в связи с митингом (по статье 20.2 КоАП), то после очередной акции человеку может грозить уголовное дело по так называемой «дадинской» статье (ст. 212.1 УК). Для возбуждения дела важно не то, когда проходили акции, а то, когда вступили в силу решения судов. Привлечение к ответственности постфактум дает правоохрнительным органам возможность манипулировать этими сроками, сближая даты постановлений, даже если сами мероприятия изначально не укладывались в полгода. Это увеличивает личные риски для протестующих, а в сочетании со сложной формулировкой статьи 212.1 УК еще и запугивает их.

Артема Пугачева, которого забрали в отдел полиции прямо из комнаты в общежитии, ранее уже привлекли к ответственности за участие в акции 2 февраля. Хотя это был лишь второй для него протокол по статье 20.2 КоАП, задержание постфактум заставило его пересмотреть свое отношение к участию в акциях:

«Не хочется попасться [еще раз], можно получить 212.1 статью. Честно говоря, возможность участвовать для себя я вижу сейчас только в виде какой-то моральной или финансовой поддержки, но не лично. По крайней мере в ближайшее время, пока не „сгорят“ все эти случаи».

На практике с преследованием постфактум сталкиваются далеко не все протестующие: по-видимому, распознать удастся пока лишь отдельных лиц. Кроме того, в судах бывает сложно доказать, что человек действительно участвовал в акции, если он не был сразу же задержан. Тем

не менее само наличие угрозы преследования и перечисленных негативных эффектов имеет высокий потенциал деморализации гражданского общества и становится рычагом для дальнейшего ограничения свободы собраний.

ЗАКЛЮЧЕНИЕ

2021 год ознаменовался массовыми задержаниями участников акций постфактум. В Москве такие задержания начались в январе и к осени стали уже обыденной практикой.

Например, массовым задержаниям в метро и на улице подверглись участники встречи с депутатами КПРФ на Пушкинской площади 20 сентября. Спустя четыре дня после мероприятия МВД Москвы **выпустило** заявление, в котором проинформировало, что в связи со встречей задержано более 30 человек и «комплекс мероприятий, направленный на установление личностей участников, продолжается».

Преследование постфактум сопряжено с дополнительными негативными эффектами: продленным ощущением угрозы, риском, что полицейские будут посещать родственников или неожиданно придут на работу, учебу, домой.

Увеличение масштабов таких задержаний становится возможным с введением уличной съемки в сочетании с технологией распознавания лиц.

Несмотря на явную угрозу частной жизни граждан, в последние годы системы распознавания лиц активно внедряются в ежедневное пользование. В банковской сфере уже **предлагают** идентификацию с их помощью, а в офисы некоторых компаний **можно войти** по биометрическим данным. Кроме того, с 15 октября

на всех станциях московского метрополитена **уже можно** оплачивать проезд с помощью системы распознавания лиц FacePay. Запуская FacePay, мэр города Сергей Собянин **заявил**:

«Мы думали, что никто не будет записываться. Кому охота себя фотографировать, заводить в систему свои данные, привязывать банковский счет — это же с ума сойти. Пятнадцать тысяч за несколько недель **записались**. С 15 сентября мы удвоим количество станций, а с 15 октября сделаем по всем станциям метрополитена Москвы».

С июля 2020 года в Москве действует «экспериментальный правовой режим», позволяющий компаниям, занимающимся разработками в сфере искусственного интеллекта и включенным в специально созданный для этого реестр, получать доступ к обезличенным персональным данным. Этот режим был введен в рамках **«Национальной стратегии искусственного интеллекта на период до 2030 года»**. На основе искусственного интеллекта работают и системы распознавания лиц. Как **объясняется** на портале стратегии, этот режим действует для того, чтобы «устранить правовые барьеры» и ускорить развитие и внедрение технологий в Москве. В тексте уточняется, что в дальнейшем подобные «песочницы» для развития технологий могут появиться и в других регионах.

Развивают и внедряют системы распознавания лиц и подразделения правоохранительных органов. Так, в 2020 году издание «Коммерсантъ» **писало**, что МВД к концу 2022 года потратит 245 млн рублей на разработку базы данных ИБД-Ф 2.0 для автоматизации работы полицейских. В ИБД-Ф планируется включить подсистему «Опознание. Биометрическая идентификация», позволяющую искать людей по изображениям через биометрический процессор по распознаванию лиц.

С распространением систем распознавания лиц в повседневной жизни увеличивается и количество источников, откуда правоохранительные органы могут получать изображения для сравнений с предполагаемыми участниками акций, и возможность правовых нарушений — например, в случае утечки данных.

В контексте уличных акций распознавание лиц фигурирует не только в столице. Наше исследование показывает, что география технологии расширяется. Явные указания на ее применение нам удалось обнаружить в судебных постановлениях, вынесенных в отношении демонстрантов в Нижнем Новгороде и Сочи. По нашим данным, после акции 21 апреля как минимум в 17 городах люди сталкивались с преследованием постфактум и использованием фото- и видеодоказательств — такое сочетание с большой вероятностью может указывать на использование распознавания лиц.

Анализ масштабов этого явления затрудняет то, что органы власти, по-видимому, предпочитают не документировать случаи применения технологии. В материалах дел об административных правонарушениях и в судебных постановлениях мы часто находим лишь косвенные подтверждения без прямого указания. Это становится препятствием и для судебного обжалования.

По нашему мнению, нежелание властей афишировать на бумаге применение распознавания лиц связано, в первую очередь, с тем, что эта технология, несмотря на стремительное развитие, остается в «серой зоне» правового регулирования.

Эту проблему в декабре 2021 года **выделяют** и авторы доклада президентского Совета по правам человека, посвященного цифровому пространству:

«Параллельная „цифровая“ власть в России и в мире пока фактически никак не регламентирована. В нашей стране

она не укладывается в рамки и без того плохо работающего на практике и почти неисполняемого федерального закона № 152-ФЗ „О персональных данных“. Эта власть сейчас проявляет себя как ей угодно, существуя в „серой зоне“ или правовом вакууме».

Несмотря на редкие **позитивные примеры** применения записей с уличных видеокамер для защиты права на свободу собраний, отсутствие четкого регулирования в одних случаях и нарушение уже существующих правил в других превращают технологию распознавания лиц в новый инструмент масштабных политических преследований.

ПРЕДЛОЖЕНИЯ ПО УЛУЧШЕНИЯМ

Для решения специфических проблем, связанных с привлечением к административной ответственности участников протестов, выявленных с использованием системы распознавания лиц, мы предлагаем следующее:

- Прекратить практику задержаний участников публичных мероприятий по прошествии продолжительного времени после самой акции. Если правоохранные органы сочтут, что в действиях участников протестов имелись признаки административного правонарушения, такого человека можно вызвать в отдел полиции в установленном законом порядке, не применяя задержания.
- В соответствии с позицией ЕСПЧ, исключить возможность исполнения административного ареста в отношении участников протестных акций, задержанных постфактум, до вступления в силу решения суда, то есть до окончания апелляционного обжалования.
- Сократить срок привлечения к административной ответственности по статье 20.2 КоАП (нарушение порядка организации или участия в публичном мероприятии) до трех месяцев, как это предусмотрено для большого количества других составов административных правонарушений.
- Прекратить противоречащую позициям Конституционного суда практику проведения оперативно-разыскных мероприятий по делам об административных правонарушениях. Здесь могло бы быть полезным постановление Пленума Верховного суда, в котором нижестоящим судам было бы предписано руководствоваться позицией Конституционного суда и исключать из дел об административных правонарушениях доказательства, полученные в рамках оперативно-разыскных мероприятий.

- Исключать из материалов дела те видео и фото, к которым не прилагается обоснование того, как на указанных материалах был установлен конкретный человек. Также рекомендовать судам выносить частные определения в отношении должностных лиц, составивших материалы дела с использованием недопустимых доказательств.
- В настоящее время уже имеется довольно обширная и противоречивая судебная практика, связанная с тем, как полиция обосновывает идентификацию личности по видео. Есть судебные постановления, в которых дается оценка использованию системы распознавания лиц в административных делах. Улучшить и унифицировать ситуацию мог бы обзор практики от Верховного суда, в котором суд обозначил бы стандарты доказывания и обратил бы внимание на несоразмерность подобного вмешательства в права и свободы граждан в контексте административных правонарушений.
- Полиции следует публично отчитаться о тех случаях, в которых при расследовании дел об административных правонарушениях проводились ОРМ, а также о мерах, предпринятых для предотвращения данной практики.
- В соответствии с **разъяснениями** Роскомнадзора, полиции следует своевременно удалять персональные данные, в том числе биометрические, используемые системой распознавания лиц, когда искомые цели будут достигнуты или потеряют актуальность. Полиция должна противодействовать созданию не предусмотренных законом баз данных с биометрическими данными людей, привлекаемых к административной ответственности, как в контексте свободы собраний, так и в других сферах.

- ЕЦХД следует в обобщенном виде периодически публиковать данные из журналов учета доступа к информации, в частности о количестве запросов на доступ к данным с указанием ведомств и их подразделений, которые такие данные запрашивали. Публикация такой информации сделает более прозрачной ситуацию с доступом к данным видеонаблюдения, а также улучшит видимость масштабов использования системы наблюдения и распознавания лиц.
- Свой негативный эффект оказывает неполная и несвоевременная публикация материалов дел на сайтах судов, что противоречит требованиям федерального законодательства. Судам следует своевременно публиковать предусмотренные акты, а также воздержаться от удаления данных, если это не предусмотрено законом.

Что касается общих предложений, мы предлагаем следующее:

- Ввести мораторий на использование системы распознавания лиц до урегулирования правоприменения в соответствии с международными стандартами, исключающими произвольное использование технологии в целях ограничения свободы собраний и выражения.

Существуют разные варианты подобного урегулирования. Например, за использованием технологии можно установить обязательный судебный контроль, как это предусмотрено для других случаев грубого вторжения в частную жизнь граждан, например, в случае обысков. Также важно ввести в практику механизм уведомления субъекта персональных данных о применении в отношении него распознавания лиц, чтобы человек имел возможность обжаловать подобное вмешательство. Судебному контролю должны подвергаться как доступ

к базам данных с видео- и фотоизображениями, которые используются при распознавании лиц, так и основания, на которых этот доступ предоставляется.

Особенно важно, у каких органов и в каких случаях есть доступ к использованию системы распознавания лиц. Подобные списки должны быть закрытыми и не предполагать расширительного толкования.

Не менее важен контроль над базами данных, с которыми сверяют видео уличного наблюдения. Должен быть правовой механизм исключения персональных данных человека из указанных баз.

Как в случае хранения видеозаписей с камер уличного наблюдения, так и в случае хранения данных в базах для сравнения с изображениями на видео должен быть установлен срок хранения данных.

Важно на нормативном уровне закрепить недопустимость использования распознавания лиц в административных делах, связанных с реализацией свободы собраний (например, статьи 20.2 и 20.2.2 КоАП). Негативный сдерживающий эффект от подобного вторжения в свободу собраний несоизмерим с возможной оптимизацией расследования административных правонарушений, которые не имеют такой общественной опасности, как преступления.

Частичной проработкой нормативного регулирования могло бы заняться Министерство цифрового развития, связи и массовых коммуникаций как федеральный орган исполнительной власти, который с лета 2021 года осуществляет регулирование в сфере идентификации физических лиц на основе биометрических персональных данных.

- Проводить периодический аудит использования персональных данных гражданами органами власти с привлечением независимых экспертов, исходя из соображений безопасности хранения данных и принимая во внимание фактические цели их обработки. Основные выводы аудита обнародовать.
- В целях повышения прозрачности использования системы распознавания лиц и безопасности собранных данных, представляется полезным создание общественного или экспертного совета при ответственном за технологию ведомстве на федеральном, региональном и муниципальном уровнях. В настоящее время существует **Консультативный совет** при Роскомнадзоре. Данный совет может создавать совещательные и экспертные органы, а Роскомнадзор может привлекать к подобной работе ученых и экспертов в сфере прав человека, в том числе из профильных НКО, занимающихся вопросами свободы собраний.
- Положительной практикой представляется периодическая публикация отчетов ответственных за использование технологии распознавания лиц ведомств о том, как используется технология и на каких данных она обучается.
- Мы также обращаем внимание на важность парламентского контроля и контроля со стороны Счетной палаты над расходами бюджетных средств на развитие и использование подобных технологий.

- Кроме того, частным компаниям, занимающимся разработкой и продажей систем распознавания лиц, в целях противодействия нарушению прав человека, не следует продавать технологии государствам, которые не предоставили достаточных оснований о нормативном урегулировании вопроса, а также о соответствии практики международным стандартам в сфере защиты прав и свобод человека в случае использования таких систем.

РЕЗЮМЕ

В 2021 году постфактум после акций протеста задержали не менее 454 человек в 17 городах. Большинство таких случаев — 363 — были связаны с митингом в поддержку Алексея Навального 21 апреля. Еще 91 задержание произошло в связи со всероссийскими акциями 23 и 31 января, а также акциями 20 и 25 сентября на Пушкинской площади в Москве.

Задержания постфактум применялись и ранее: по данным ОВД-Инфо, в 2018-м известно о 219 таких задержаниях в 38 регионах; в 2020-м во время протестов в Хабаровском крае зафиксировано 121 задержание между акциями. Однако в 2021 году подобные задержания стали особенно массовыми и концентрированными. Мы объясняем это тем, что для выявления участников акций полиция начала использовать машинное распознавание лиц, запечатленных на фото и видео.

Среди обратившихся в ОВД-Инфо в связи давлением постфактум после акции 21 апреля как минимум 164 человека отметили, что в ходе общения с полицией в суде они узнали об использовании в качестве доказательств фото- и видеоматериалов.

Из судебных постановлений нам известно, что к поиску предполагаемых участников по камерам подключались

различные подразделения полиции: отделы охраны общественного порядка, участковые, Центр «Э», уголовный розыск, Бюро специальных технических мероприятий (БСТМ).

Для выявления протестующих используются записи с камер наружного наблюдения (в Москве они хранятся в базе ЕЦХД, которой оперирует Департамент информационных технологий, в других городах они собираются системами «Безопасный город»), оперативная съемка сотрудников правоохранительных органов, фото и видео из интернета: телеграм-каналов, чатов, личных страниц в социальных сетях, YouTube.

Известны случаи, когда камеры — например, установленные в подъезде или в метро — использовались также для определения местонахождения человека для привлечения его к административной ответственности.

Для идентификации полиция задействует базы данных с фотографиями из документов (паспортов, загранпаспортов, социальных карт) и из соцсетей. Доказательств того, что используются снимки, сделанные в отделах полиции при предыдущих задержаниях, мы не обнаружили.

Хотя сотрудники полиции нередко сообщают задержанным, что их «нашли по камерам», в официальных документах — материалах дел и судебных постановлениях — применение технологии распознавания лиц скрывается.

Признаками использования распознавания лиц является наличие в материалах дел фотографий человека из документа, доступом к которому может обладать МВД, и ее сравнение со скриншотом из видео с акции; указание процента схожести изображений или упоминание модуля «ПАРСИВ». При этом география этой технологии выходит за пределы Москвы: явные указания на ее применение нам

удалось обнаружить в судебных постановлениях, вынесенных в отношении демонстрантов в Нижнем Новгороде и Сочи.

Преследование за участие в акции, отложенное во времени, сопряжено с дополнительными сложностями и большими негативными последствиями по сравнению с задержанием во время акции. В том числе, с серьезным вторжением в частную жизнь и влиянием на другие сферы жизни человека.

Практика задержаний постфактум имеет явную карательную направленность и оказывает запугивающий и маргинализирующий эффект на потенциальных участников собраний. С учетом того, что срок привлечения к административной ответственности по наиболее распространенной «митинговой» статье 20.2 КоАП увеличен до года, участники акций на протяжении продолжительного времени находятся в ожидании возможного задержания. Уже известны случаи, когда на человека составляли протокол спустя более шести месяцев после акции. Наконец, привлечение к ответственности постфактум дает правоохранительным органам возможность манипулировать сроками рассмотрения дел в судах, создавая основу для использования обвинений в «повторном» и «неоднократном» нарушении (ч. 8 ст. 20.2 КоАП и 212.1 УК), которые чреватые суровыми санкциями.

Привлечение участников акций к ответственности с применением технологии распознавания лиц предполагает обработку биометрических данных без согласия их обладателей. В материалах дел идентификация демонстрантов часто оформляется как проведение оперативно-разыскных мероприятий, не предусмотренных для административных правонарушений. Само применение технологии при этом находится в «серой зоне» — случаи, когда

правоохранители могут ее применять, не нарушая закона «О персональных данных», нигде не прописаны.

Вероятно, законность использования распознавания лиц для административного преследования протестующих не очевидна и сотрудникам правоохранительных органов: именно этим может объясняться то, что применение технологии скрывают в официальных документах. Отсутствие в документах упоминания технологии затрудняет обжалование ее использования и не дает увидеть истинный масштаб ее применения.

В отдельных случаях суды одобряют использование распознавания лиц в делах демонстрантов под предлогом защиты общественных интересов. Между тем отсутствие массового применения этой технологии ко многим другим типам правонарушений (таким как переход дороги в неположенном месте или безбилетный проезд) свидетельствует, что основной целью является не защита общественных интересов, а преследование политических оппонентов власти.

Ряд вопросов, связанных с созданием и функционированием инфраструктуры, необходимой для использования системы распознавания лиц для ограничения протестов (уличная фото- и видеосъемка, хранение полученных данных, формирование баз фотоснимков с идентификацией личности), доступом сотрудников полиции к базам данных, защитой персональных данных недостаточно урегулированы. В сочетании с непрозрачностью применения и отсутствием публичного контроля возможно превращение этой технологии в инструмент политически мотивированного преследования.

Пока с задержаниями постфактум сталкивается небольшая доля участников акций. Даже если опираться на официальные данные, в акции 21 апреля в Москве участвовали около шести тысяч человек — значительно

больше, чем впоследствии привлекли к административной ответственности. Тем не менее риски преследования постфактум распространяются на всех участников, что не может не оказывать сдерживающий эффект, препятствуя реализации права на свободу собраний.

Давление на общество оказывает также лишение участников собрания некоторой степени анонимности, которая является частью коллективного действия, и массовое вмешательство в частную жизнь людей, происходящее из-за неизбирательности процесса распознавания лиц.

С критикой применения системы распознавания лиц выступают и международные органы защиты прав человека. В частности, они указывают на то, что ее использование может приводить к чрезмерному вмешательству полиции в жизнь граждан.

В международном праве отмечается важность детального и предсказуемого нормативного регулирования применения таких технологий, важность уважения права на частную жизнь в публичном пространстве, а также необходимость согласия на обработку персональных данных.

С учетом того, что системы распознавания лиц активно развиваются, а их применение захватывает все больше сфер жизни, особенно важно исключить такое их использование, которое приводит к ущемлению прав человека. Важно также разработать необходимое правовое регулирование, отвечающее международным стандартам. Более детальные рекомендации представлены в разделе [«Предложения по улучшениям»](#).

ПРИЛОЖЕНИЕ

Основания для прекращения или возвращения дел после задержания постфактум

В качестве примера мы публикуем 16 дел по статье 20.2 КоАП, связанных с задержанием постфактум, которые московские суды первой инстанции прекратили или вернули в полицию для устранения недостатков в протоколах.

Задержание постфактум порождает дополнительные основания для прекращения дел. Мы полагаем, что аргументы, которые привели к благоприятному развитию событий, могут быть полезны тем, кого постфактум привлекают к ответственности за участие в акциях, и защитникам, которым, вероятно, все чаще придется сталкиваться с такими делами.

Предлагаемые нами доводы можно сгруппировать в три блока: идентификация участника акции по видео или фотографии, свидетельские показания и процессуальные нарушения. Ниже в таблице можно найти примеры таких аргументов в реальных делах.

1 Свидетельские показания и показания:

- a. свидетели правонарушения не опрашивались.
- b. есть показания свидетеля защиты (что не участвовал в митинге).
- c. полиция не опрашивала привлекаемого.
- d. авторы рапорта не присутствовали при правонарушении.

2 Процессуальные нарушения:

- a. не участвовал в составлении протокола.
- b. нет подтверждения об уведомлении в составлении протокола.

3 Идентификация ответчика как участника акции и видео как доказательство:

- a. на месте совершения правонарушения личность не устанавливали.
- b. на месте совершения правонарушения не задерживали.
- c. не представлены конкретные источники установления личности граждан на видео.
- d. сам суд не имеет средств для идентификации.
- e. полиция не показала суду, какой человек на видео является ответчиком.
- f. не установлено, когда и по какому адресу произведена видеозапись.
- g. из видео не следует, что проходил митинг (прохожие идут по тротуару).
- h. не доказано, что человек на видео и в суде — один и тот же.

Hide fields Filter Grouped by 1 field Sort		
Ссылка на сайте...	Суд	Решение
РЕШЕНИЕ		
Вынесено постановлен 6		
1	https://mos-gorsud.ru/rs/zelenogradskij/services/cases/admin/detail/s/6a358e40-d7d6-11eb-8178-dfb4ef517ebd	Зеленоградский районн... Вынесено постано...
2	https://mos-gorsud.ru/rs/zelenogradskij/services/cases/admin/detail/s/f95f67e0-db09-11eb-90c1-a95323b15270	Зеленоградский районн... Вынесено постано...
3	https://mos-gorsud.ru/rs/zelenogradskij/services/cases/admin/detail/s/2fc30270-db09-11eb-90c1-a95323b15270	Зеленоградский районн... Вынесено постано...
16 records		
Airtable Download CSV View larger version		
Открыть таблицу / Open table		

Ещё почитать

31.05.2025 Саратовская область

На несовершеннолетних жительниц Пугачева завели уголовное дело из-за сушки вещей над Вечным огнем



«Ничего маме не говори про „газель“, чтобы она не волновалась». В Екатеринбурге силовики избили студента, пытаюсь добраться до его мобильного
Угрозы «увезти в лес» за отказ дать пароль от мобильного, выкручивание рук и побои. Так прошло задержание активиста в Екатеринбурге.



Меня избили полицейские

К сожалению, насилие со стороны полицейских — это не редкость. С ним может столкнуться любой

задержанный — предугадать такое нельзя. Мы подскажем вам шаги, которые помогут привлечь...



Требуем запретить «карусельные» аресты

В октябре 2025 года суд в Петербурге отправил под административный арест участников группы «Стоптайм»: вокалистку Диану Логинову (Наоко), барабанщика Владислава Леонтьева и гитариста...



«Московское дело»

420 новостей и текстов по теме