В ТВЕРСКОЙ РАЙОННЫЙ СУД ГОРОДА МОСКВЫ
129090, г. Москва, ул. Каланчёвская, д. 43А

АДМИНИСТРАТИВНЫЙ ИСТЕЦ: **К.А.**

АДМИНИСТРАТИВНЫЙ ОТВЕТЧИК 1: **Главное управление Министерства внутренних дел Российской Федерации по городу Москве (ГУ МВД России по г. Москве)**
127994, г. Москва, ул. Петровка, д. 38

АДМИНИСТРАТИВНЫЙ ОТВЕТЧИК 2: **Департамент информационных технологий г. Москвы**
Юр. адрес: 107078, г. Москва, ул. Новая Басманная, д. 10с1
Фактический адрес: 105064, г. Москва, Яковоапостольский пер., д. 12с1

АДМИНИСТРАТИВНОЕ ИСКОВОЕ ЗАЯВЛЕНИЕ

об обжаловании действий органов власти по применению городской системы видеонаблюдения и технологии распознавания лиц

1. ОБСТОЯТЕЛЬСТВА: использование технологии распознавания лиц в системе видеонаблюдения «Городская система наблюдения» в городе Москве

1.1. Впервые мэрия Москвы сообщила[1] о запуске системы массового распознавания лиц осенью 2017 года. На тот момент сообщалось, что к ней подключили более 3000 видеокамер, изображение с которых автоматически анализируется в режиме реального времени. При помощи нейросетей лица попавших в камеру прохожих сравнивают с фото из баз данных.
1.2. По информации, размещённой на официальном сайте Мэра Москвы “в 2019 году в столице будет развернута общегородская система распознавания лиц для розыска преступников. В мэрии пояснили, что с этой целью уже обновлены 40% из 162 тыс. городских видеокамер”.
1.3. Департамент информационных технологий отмечал, что в тестовом режиме система распознавания лиц применялась во время Чемпионата мира по футболу в Москве в 2018 году. Начальник Отдела городского видеонаблюдения Дмитрий Головин сообщил, “что во время чемпионата мира по футболу мы подключили 4,5 тыс. камер на объектах мундиаля и развернули 3 пилотные зоны: на входных КПП стадиона «Лужники», «Спартак» и площадки Фестивалей болельщиков на Воробьёвых горах – там установили

[1] Новость на Официальном сайте Мэра Москвы от 28.09.2017 “В Москве заработала одна из крупнейших в мире систем видеонаблюдения с функцией распознавания лиц”. URL: https://www.mos.ru/news/item/30105073/.

видеокамеры с модулем распознавания лиц ГИС ЕЦХД….В результате удалось задержать 98 человек, которые числились в базах правоохранительных органов".

1.4. Постановлением Правительства Москвы от 9 сентября 2019 г. №1161-ПП «О мерах, направленных на реализацию Государственной программы города Москвы «Умный город», в 2019 году на реализацию мероприятий по созданию и обеспечению функционирования в городе Москве системы видеоаналитики на основании технологии по распознаванию лиц в рамках реализации Департаментом информационных технологий города Москвы нового мероприятия Государственной программы города Москвы «Умный город» за счёт бюджетных ассигнований из бюджета города Москвы акционерному обществу «Электронная Москва» предоставлена субсидия в размере 4 926 700,0 тыс. рублей (п. 1 постановления).

1.5. Согласно информации из открытых источников[2], 20 июня 2019 года на Единой электронной торговой площадке http://roseltorg.ru была размещена информация о проведении открытого конкурса в электронной форме на оказание услуг по методологическому и аналитическому обеспечению городской системы видеонаблюдения на базе государственной информационной системы «Единый центр хранения и обработки данных» стоимостью 261 217 566 рублей. По результатам указанного конкурса между Департаментом информационных технологий города Москвы и АО «Ситроникс» (ИНН 7735116621) был заключён контракт на сумму 259 911 478 рублей 29 копеек.

1.6. В рамках контракта Исполнитель также обязан оказать услуги по анализу нормативно-правовых и организационных условий предоставления услуг «Городской системы видеонаблюдения» и предоставить правовое заключение по результатом этого анализа.

В ходе составления обзора нормативных правовых актов Российской Федерации и города Москвы, а также проектов нормативно-правовых актов, регулирующих использование фото/видеоизображения гражданина при функционировании систем видеонаблюдения, включая ГСВ, Исполнитель отражает следующие проблемы правового регулирования (включая, но не ограничиваясь):

- проблему необходимости/отсутствия необходимости получения согласия гражданина на использование его изображения при осуществлении видеонаблюдения;
- проблему необходимости/отсутствия необходимости удаления изображения гражданина из ГСВ по требованию гражданина;
- потенциальные случаи неправомерного использования изображения гражданина при осуществлении видеонаблюдения в ГСВ;
- возможную ответственность оператора ГСВ и пользователей ГСВ за неправомерное использование изображений гражданина;
- необходимость/отсутствие необходимости информирования гражданина об осуществлении видеонаблюдения и получении изображения гражданина при осуществлении видеонаблюдения;
- возможность реализации информации, содержащей изображение гражданина из ГСВ, на возмездной основе;

---

[2] Информация о государственной закупке №0173200001419000838. URL: http://zakupki.gov.ru/epz/order/notice/ok504/view/common-info.html?regNumber=0173200001419000838.

- защиту конституционных и иных охраняемых законом прав граждан, связанных с использованием их изображений, при функционировании ГСВ;
- правовые проблемы, связанные с возможностью использования изображения гражданина при реализации функции ГСВ по идентификации гражданина с использованием его изображения (в том числе на основе его сопоставления с базами данных), и иные правовые проблемы, связанные с использованием изображения гражданина в ГСВ.

1.10. Технология распознавания лиц представляет собой метод оценки двух и/или более изображений гражданина в целях его идентификации (установления личности). При применении технологии распознавания лиц производится фотография лица гражданина и извлечение из неё биометрических данных (уникальных параметров и черт лица); впоследствии полученные биометрические данные сравниваются с биометрическими данным, полученными в результате обработки изображений из баз данных пользователя технологии (в настоящем деле полиции).

Работа технологии распознавания лиц состоит из следующих этапов:

1) составление или использование уже существующей базы данных с фотографиями;
2) сбор изображений (фотографий) граждан для сравнения с имеющимися фотографиями (например, с помощью камер видеонаблюдения);
3) обнаружение лица гражданина;
4) извлечение биометрических данных (уникальных параметров и черт лица) из собранных изображений;
5) сопоставление биометрических данных, извлечённых из изображений гражданина;
6) выдача результата сопоставления биометрических данных из разных источников.

Работа технологии распознавания лиц обусловлена применением камер видеонаблюдения. При этом обработка изображений и биометрических данных фактически осуществляется только в рамках программного обеспечения по распознаванию лиц. Камеры видеонаблюдения лишь производят запись происходящего, а технология распознавания лиц уже используется для обнаружения на видеозаписи лиц граждан, извлечения из полученных изображений биометрических данных, сопоставления с имеющимися у государственного органа данными и оценки соответствия между ними.

2. ОБСТОЯТЕЛЬСТВА ДЕЛА АДМИНИСТРАТИВНОГО ИСТЦА

2.1. К.А. (далее – Административный истец) гражданка РФ, не судима, подозреваемой или обвиняемой по какому-либо уголовному делу не является, лицом, привлекаемым к ответственности за какое-либо административное правонарушение, также не является.

2.2. 21 июня 2020 г. Административный истец получила рассылку с информацией о том, что через мессенджер «Telegram» можно получить услугу «пробива по лицу». Перейдя по ссылке из объявления Административный истец выяснила, что пользователь указанного мессенджера с никнеймом (псевдонимом) «Вимм-Билль-Данн» предлагает неограниченному кругу лиц купить данные, полученные из московской системы видеонаблюдения и распознавания лиц.

2.3. В целях проверки фактической защищённости собственных биометрических данных и иных данных о своей частной жизни в городской системе видеонаблюдения и распознавания лиц Административный истец купила услугу «Пробив человека через московскую систему распознавания лиц, установленную на камерах в городе Москва» (приложение 5, протокол осмотра нотариуса).

19 июля 2020 года Административный истец отправила свои фотографии пользователю мессенджера «Telegram» с никнеймом (псевдонимом) «Вимм-Билль-Данн».

За услугу «пробива по лицу» пользователь «Вимм-Билль-Данн» запросил 16 500 (шестнадцать) тысяч рублей, которые были перечислены посреднику, выполняющему роль Гаранта сделки, на биткойн-кошелёк.

2.4. В результате, 21 июля 2020 года пользователь «Вимм-Билль-Данн» выслал Административному истцу файл с результатами поиска изображения лица истца в системе распознавания лиц **за период 20 июня 16:34:22 по 21 июля 16:34:35** (то есть 1 месяц, предшествующий дате высылки отчёта).

В частности, файл состоит из 27 страниц и содержит следующие данные:

- исходная фотография Административного истца, предоставленная для проведения поиска;
- результаты поиска по камерам города Москвы за указанный месячный период в виде списка;
- адреса нахождения камер, которые распознали Административного истца в указанный месячный период;
- точные даты и время фиксации изображения Административного истца каждой камерой.

2.5. Информация, содержащаяся в файле с результатами «пробива лица» Административного истца, является достоверной – Административный истец действительно посещала указанные в файле адреса в указанное время.
2.6. Описанное в настоящем разделе свидетельствует о том, что к видеоданным, содержащимся в Едином центре хранения и обработки данных (далее – ЕЦХД), а также к технологии распознавания лиц, имеют доступ неустановленные лица, которые за плату предоставляют эти данные любому, кто готов заплатить назначенную цену.

Также, из отчёта усматривается, что записи с камер города Москвы хранятся в ЕЦХД не менее месяца.

3. ПРАВОВОЕ ОБОСНОВАНИЕ

3.1 Федеральные законы

3.1.1. Дефиниции

Персональные данные – любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных) (абз. 1 ст. 3 Федерального закона от 27 июля 2006 г. №152-ФЗ «О персональных данных» (далее – закон персональных данных).

В соответствии с ч. 1 ст. 11 закона о персональных данных, к **биометрическим персональным данным** относятся сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых **можно установить его личность** и которые используются оператором для установления личности субъекта персональных данных.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели

обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными (абз. 2 ст. 3 закона о персональных данных).

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных (абз. 3 ст. 3 закона о персональных данных).

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники (абз. 4 ст. 3 закона о персональных данных).

3.1.2. Исходя из определения, установленного законом о персональных данных, к биометрическим персональным данным относятся физиологические данные (дактилоскопические данные, радужная оболочка глаз, анализы ДНК, рост, вес и другие), а также иные физиологические или биологические характеристики человека, в том числе изображение человека (фотография и видеозапись), которые позволяют установить его личность и используются оператором для установления личности субъекта.

3.1.3. Обработка биометрических персональных данных может осуществляться только при наличии **согласия в письменной форме субъекта персональных данных**, за исключением случаев, предусмотренных ч. 2 ст. 11 закона о персональных данных, предусматривающей исключения, связанные с реализацией международных договоров Российской Федерации о реадмиссии, в связи с осуществлением правосудия и исполнением судебных актов, а также в случаях, предусмотренных законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-розыскной деятельности, о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию.

3.1.4. Вместе с тем, законодательством Российской Федерации, к которому отсылает часть 2 ст. 11 закона о персональных данным в целях определения допустимых случаев обработки биометрических данных без письменного согласия субъекта персональных данных, такие случаи не установлены.

Таким образом, законодательство РФ не предусматривает ясных, однозначных и прогнозируемых оснований и правил обработки биометрических данных операторами-государственными органами в отсутствие согласия субъекта персональных данных. Следовательно, применение технологии распознавания лиц в городе Москве по умолчанию и в режиме реального времени является незаконным.

3.2. Подзаконные акты города Москвы

3.2.1. Постановлением Правительства Москвы от 9 августа 2011 г. №349-ПП «Об утверждении Государственной программы города Москвы «Умный город» была утверждена указанная государственная программа, а контроль за выполнением постановления возложен на руководителя Департамента информационных технологий города Москвы Лысенко Э.А.

3.2.2. Постановлением Правительства Москвы от 7 февраля 2012 г. №24-ПП «Об утверждении положения о государственной информационной система «Единый центр хранения обработки данных», утверждено соответствующее Положение о ГИС ЕЦХД, а Департамент информационных технологий г. Москвы (далее – ДИТ Москвы) утверждён в качестве государственного заказчика работ (услуг), связанных с создание и обеспечением функционирования ГИС ЕЦХД, а также её оператором и координатором деятельности по подключению к указанной ГИС внешних информационных систем, пользователей информации об объектах видеонаблюдения и предоставлению информации в ГИС ЕЦХД (далее - ЕЦХД) (п. 2.1. постановления).

3.2.3. **ЕЦХД** представляет собой государственную информационную систему города Москвы, содержащую совокупность информации об объектах, за которыми ведётся видеонаблюдение в городе Москве (далее - объекты видеонаблюдения), а именно: видеоизображение объекта видеонаблюдения, сведения о его местонахождении, дате и времени осуществления видеонаблюдения, совокупность сведений о поставщиках и пользователях информации об объектах видеонаблюдения, истории движения данной информации (далее - информация), а также содержащую программные и технические средства, обеспечивающие взаимодействие между оператором ЕЦХД, поставщиками информации, пользователями информации в электронной форме (п. 2 Положения о ГИС ЕЦХД, утв. постановлением Правительства Москвы от 7 февраля 2012 г. №24-ПП).

3.2.4. Согласно пункту 4 Положения о ГИС ЕЦХД (утв. постановлением Правительства Москвы от 7 февраля 2012 г. №24-ПП), основными функциями ЕЦХД являются:

- сбор, обработка, хранение информации, предоставление доступа к информации;
- обеспечение информационного взаимодействия между оператором ЕЦХД, поставщиками и пользователями информации в ЕЦХД.

3.2.5. В соответствии с пунктом 5 Положения о ГИС ЕЦХД, **поставщиками информации** в ЕЦХД являются органы исполнительной власти города Москвы и подведомственные им организации, обладающие информацией об объектах видеонаблюдения, а также иные лица, с которыми в соответствии с настоящим Положением заключены соглашения или государственные контракты.

В соответствии с пунктом 7 Положения о ГИС ЕЦХД, **пользователями информации**, хранимой и обрабатываемой в ЕЦХД, являются органы и организации, информация которым предоставляется в соответствии с требованиями законодательства Российской Федерации и города Москвы, а также иные лица, получившие доступ к информации в порядке, установленном настоящим Положением.

3.2.6. Распоряжением ДИТ Москвы от 31 июля 2015 г. №64-16-241/15 утверждены регламенты доступа к информации, содержащейся в ГИС ЕЦХД, передачи информации в ГИС ЕЦХД из других информационных систем. В сущности, три регламента, утверждённые указанным распоряжением ДИТ Москвы, образуют общие правила создания, функционирования и использования ГИС ЕЦХД и содержащейся в ней информации.

3.2.7. **При этом какие-либо основания, принципы, правила и порядок использования технологии распознавания лиц в городе Москве не были сформулированы**, в частности не определены:

- доспустимые случаи и цели применения указанной технологии;

- порядок использования указанной технологии уполномоченными органами власти (длительность применения технологии, срок хранения полученных биометрических данных, способы обработки и проч.);

- механизмы защиты прав и интересов субъектов персональных данных при применении указанной технологии.

- критерии соответствия в процентах, позволяющих установить информацию о том, что гражданин на двух изображениях в поисковой выдаче является одним и тем же лицом.

4. Нормы международного права

4.1. Конвенция о защите прав человека и основных свобод от 4 ноября 1950 года

4.1.1. Согласно статье 8 Конвенции о защите прав человека и основных свобод от 4 ноября 1950 года (далее – Конвенция), каждый имеет право на уважение его личной и семейной жизни, его жилища и его корреспонденции (п. 1). Не допускается вмешательство со стороны публичных властей в осуществление этого права, за исключением случая, когда такое вмешательство предусмотрено законом и необходимо в демократическом обществе в интересах национальной безопасности и общественного порядка, экономического благосостояния страны, в целях предотвращения беспорядков или преступлений, для охраны здоровья или нравственности или защиты прав и свобод других (п. 2).

4.1.2. В пункте 5 Постановления Пленума Верховного Суда Российской Федерации от 27 июня 2013 г. №21 «О применении судами общей юрисдикции Конвенции о защите прав человека и основных свобод от 4 ноября 1950 года и Протоколов к ней» (далее – Постановление Пленума ВС РФ от 27.06.2013 г. №21) разъясняется, что под ограничением прав и свобод человека (вмешательством в права и свободы человека) понимаются любые решения, действия (бездействие) органов государственной власти, органов местного самоуправления, должностных лиц, государственных и муниципальных служащих, а также иных лиц, вследствие принятия или осуществления (неосуществления) которых в отношении лица, заявляющего о предполагаемом нарушении его прав и свобод, созданы препятствия для реализации его прав и свобод.

4.1.3. При этом в силу части 3 статьи 55 Конституции Российской Федерации, положений Конвенции и Протоколов к ней любое ограничение прав и свобод человека должно быть **основано на федеральном законе**; **преследовать социально значимую, законную цель** (например, обеспечение общественной безопасности, защиту морали, нравственности, прав и законных интересов других лиц); **являться необходимым в демократическом обществе** (**пропорциональным** преследуемой социально значимой, законной цели).

Несоблюдение одного из этих критериев ограничения представляет собой нарушение прав и свобод человека, которые подлежат судебной защите в установленном законом порядке.

4.1.4. В пункте 8 Постановления Пленума ВС РФ от 27.06.2013 г. №21 разъясняется, что судам при рассмотрении дел всегда следует обосновывать необходимость ограничения прав и свобод человека исходя из установленных фактических обстоятельств. Обратить внимание судов на то, что ограничение прав и свобод человека допускается лишь в том случае, если имеются **относимые и достаточные основания для такого ограничения, а также если соблюдается баланс между законными интересами лица, права и свободы которого ограничиваются, и законными интересами иных лиц, государства, общества**.

4.1.5. Таким образом, учитывая то, что федеральными законами Российской Федерации не закреплены основания для применения технологии распознавания лиц (т.е. сбора и обработки властями, государственными органами биометрических данных граждан и данных об их частной жизни), действия Административных ответчиков по применению технологии распознавания лиц на территории города Москвы в «Городской системе видеонаблюдения», построенной на базе ЕЦХД, образуют нарушение статьи 8 Конвенции о защите прав человека и основных свобод от 4 ноября 1950 года.

5. Нормы мягкого права. Рекомендации/резолюции ООН

Статьёй 9 Международного пакта о гражданских и политических правах (Нью-Йорк, 16 декабря 1966 г.), ратифицированного Указом Президиума ВС СССР от 18 сентября 1973 г. N 4812-VIII, гарантируется, что каждый человек имеет право на свободу и личную неприкосновенность. Никто не может быть подвергнут произвольному аресту или содержанию под стражей. Никто не должен быть лишён свободы иначе, как на таких основаниях и в соответствии с такой процедурой, которые установлены законом. Вместе с тем, использование технологии распознавания лиц значительно повышает риск ошибочного ареста гражданина.

Кроме того, ст. 17 Конвенции установлено, что никто не может подвергаться произвольному или незаконному вмешательству в личную и семейную жизнь человек. Каждый человек имеет право на защиту закона от такого вмешательства. Нетаргетированная слежка в отношении граждан ведет к нарушению иных прав человека, предусмотренных статьями 12, 18-19, 21-22 Конвенции, и препятствует свободной реализации права на свободу самовыражения, свободу слова и мирный протест.

Согласно резолюции ООН по результатам доклада специального докладчика ООН по вопросам самовыражения «Право на неприкосновенность частной жизни в цифровой век» №A/HRC/39/29, массовая слежка не допускается международным правом прав человека, поскольку при таких мерах невозможно проводить анализ каждого конкретного случая на предмет необходимости и соразмерности применяемых мер. В соответствии с рекомендациями специального докладчика ООН по вопросам самовыражения Дэвида Кея, изложенным в п. 66 резолюции ООН A/HRC/41/35 «Слежение и права человека», государствам следует 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[3].

6. Практика ЕСПЧ

6.1. Европейский суд по правам человека (далее - ЕСПЧ) уже рассматривал ряд дел о сборе и обработке публичными властями и государственными органами биометрических данных граждан: дело «Антович и Миркович против Черногории» [Antović and Mirković v. Montenegro] (жалоба №70838/13); дело «Перри против Соединённого Королевства» [Perry v. United Kingdom] (жалоба №63737/00); дело «S. и Марпер против Соединённого Королевства» [S. and Marper v. United Kingdom] (жалобы №№ 30562/04 и 30566/04). Полагаем, что правовые позиции ЕСПЧ, изложенные в окончательных постановлениях по

[3] Доклад специального докладчика ООН по вопросам самовыражения Дэвида Кея A/HRC/41/35 «Слежение и права человека». URL: https://undocs.org/ru/A/HRC/41/35.

указанным делам, подлежат учёту при рассмотрении настоящего дела, поскольку их обстоятельства являются аналогичными друг другу.

6.2. В пункте 2 Постановления Пленума Верховного Суда Российской Федерации от 27 июня 2013 г. №21 «О применении судами общей юрисдикции Конвенции о защите прав человека и основных свобод от 4 ноября 1950 года и Протоколов к ней» (далее – Постановление Пленума ВС РФ от 27.06.2013 г. №21) разъясняется, что правовые позиции Европейского Суда по правам человека (далее – ЕСПЧ), которые содержатся в окончательных постановлениях ЕСПЧ, принятых в отношении Российской Федерации, являются обязательными для судов.

6.3. В том же пункте данного постановления также содержатся следующие разъяснения в отношении учёта и применения позиций ЕСПЧ, изложенных в окончательных постановлениях в отношении других государств-участников Конвенции: с целью эффективной защиты прав и свобод человека судами учитываются правовые позиции Европейского Суда, изложенные в ставших окончательными постановлениях, которые приняты в отношении других государств-участников Конвенции. При этом правовая позиция учитывается судом, если обстоятельства рассматриваемого им дела являются аналогичными обстоятельствам, ставшим предметом анализа и выводов Европейского Суда.

6.4. Постановление ЕСПЧ от 28 ноября 2017 г. Дело «Антович и Миркович против Черногории» [Antović and Mirković v. Montenegro] (жалоба №70838/13).

Дело касалось вмешательства в право на частную жизнь по жалобе двух профессоров факультета математики Университета Черногории в связи с установкой системы видеонаблюдения в учебных помещениях. Заявители утверждали, что у них не было контроля над информацией, которая собиралась через систему видеонаблюдения, а также что слежка была незаконной. Национальные суды отказали заявителям в компенсации, придя к выводу о том, что право на тайну личной жизни не было затронуто в деле, так как аудитории, в которых преподавали заявители, являлись общественными местами.

ЕСПЧ напротив установил нарушение статьи 8 Конвенции, установив, что использование видеонаблюдение противоречило закону. При этом ЕСПЧ отметил, что в соответствии с ранее сформулированной Судом позицией, к частной жизни может относится в том числе профессиональная деятельность человека. Таким образом, статья 8 Конвенции подлежала применению. По существу дела суд установил, что использование камер видеонаблюдения привело к нарушению прав заявителей на тайну частной жизни, а доказательства подтвердили, что видеонаблюдение нарушило положения национального законодательства.

Обстоятельства приведённого дела аналогичны тем, на которые ссылается Административный истец в части возможности нарушения ст. 8 Конвенции (права на частную жизнь) при осуществлении сбора персональных данных путём видеосъёмки в публичных местах. Административный истец также утверждает, что хотя видеозапись с применением технологии распознавания лиц применялась в публичном месте, это нарушило право истца на частную жизнь в форме незаконной обработки биометрических данных.

6.5. Постановление ЕСПЧ от 17 июля 2003 г. Дело «Перри против Соединённого Королевства» [Perry v. United Kingdom] (жалоба №63737/00).

Обстоятельствами данного дела были следующие: заявитель, подозреваемый в совершении ряда грабежей, не явился на несколько предъявлений для опознания в полиции. Старший офицер полиции дал тогда разрешение снять его на видео скрытно в целях идентификации. Полиция организовала доставку заявителя в полицейский участок для проведения опознания. Заявитель снова отказался участвовать в опознании, но в то время, пока он ждал в месте, отведенном для посетителей, его сняли на видеопленку по системе внутреннего кабельного телевидения, положение камер которого было отрегулировано так, чтобы получить его четкое изображение. Был смонтирован видеоматериал, на котором имелось изображение 11 добровольцев и заявителя. Видеоматериал был показан ряду свидетелей, двое из которых опознали Перри как лицо, совершившее некоторые грабежи. При разбирательстве уголовного дела заявителя в суде судья отклонил ходатайство об исключении видеоматериала в качестве доказательства, хотя и признал, что полицейские, организуя такую видеосъемку, действовали не полностью в соответствии с требованиями полицейского Кодекса практики. Заявитель был осужден, и его апелляционная жалоба на обвинительный приговор была отклонена.

ЕСПЧ пришёл к выводу о том, что допущено нарушение положений Статьи 8 Конвенции (принято единогласно). Суд отметил, что уловка, к которой прибегли полицейские, вышла за рамки обычного или ожидаемого использования камер наблюдения для обеспечения безопасности, и видеосъемка заявителя и ее монтирование с другим видеоматериалом в целях дальнейшего использования может быть поэтому расценено как обработка или сбор личных сведений о заявителе. Кроме того, видеозапись не была получена добровольно или в обстоятельствах, когда заявитель мог разумно ожидать, что видеозапись будет сделана и использована в целях его опознания. Посему акт вмешательства государства в реализацию права человека на уважение его частной жизни имел место. В праве Соединенного Королевства имеется достаточная база для подобного вмешательства, но суды установили, что полиция не соблюла лишь порядок, установленный в полицейском Кодексе практики. В свете такого подхода можно только заключить, что действие, предпринятое полицейскими, как оно было осуществлено в настоящем деле, не соответствовало требованиям внутреннего права страны.

Обстоятельства приведённого дела аналогичны тем, на которые ссылается Административный истец в части скрытого характера применения камер видеонаблюдения с функцией распознавания лиц. Также как и в деле, рассмотренном ЕСПЧ, Административный истец не мог разумно ожидать, что видеозапись и использование технологии распознавания лиц будет сделана и использована властями в целях, которые истцу заранее неизвестны при том, что истец к тому же не является подозреваемой/обвиняемой по уголовному делу.

6.6. Постановление ЕСПЧ от 4 декабря 2008 г. Дело «S. и Марпер против Соединённого Королевства» [S. and Marper v. United Kingdom] (жалобы №№ 30562/04 и 30566/04).

Данное дело касалось неограниченного хранения образцов отпечатков пальцев, биоматериалов и образцов ДНК заявителей в базе данных после прекращения производства уголовного дела в отношении них. Власти заявляли, что, несмотря на прекращение уголовного преследования, данные заявителей хранились в целях идентификации будущих преступников.

ЕСПЧ установил, что имело место нарушение статьи 8 Конвенции, придя к выводу, что бессрочное хранение указанных биометрических данных является несоразмерным вмешательством в частную жизнь заявителей и не может быть признано необходимым в демократическом обществе.

Суд полагает, в частности, что использование современных научных технологий в системе уголовного правосудия нельзя применять любой ценой, без тщательной оценки баланса между потенциальными выгодами от широкого использования таких технологий и важнейших интересов, связанных с правом на частную жизнь. Любое государство, являющееся первопроходцем в развитии новых технологий, несёт также особую ответственность за нахождение справедливого баланса. В этом отношении неограниченные полномочия властей по хранению таких материалов (биометрических данных) в Англии и Уэльсе особенно удивительны с учетом того, что они допускает хранение данных независимо от характера или тяжести преступления, а также возраста подозреваемого. Кроме того, для хранения не был установлен предел времени и имелись лишь ограниченные возможности для того, чтобы оправданные лица могли требовать удаления этих данных из общенациональной базы или их уничтожения. Отсутствовали также положения о независимой проверке оснований для хранения в соответствии с установленными критериями. Особую озабоченность Суда вызывал риск стигматизации, поскольку с лицами, которые не были признаны виновными в каком-либо преступлении и имели право на презумпцию невиновности, обращались таким же образом, как с осужденными. Хранение могло являться особенно вредоносным в отношении несовершеннолетних, таких в случае с первым заявителем, с учётом их особой ситуации и важности их развития и интеграции в общество.

Суд заключил, что массовое и неизбирательное применение полномочий по хранению образцов отпечатков пальцев, биоматериалов и образцов ДНК людей в статусе подозреваемых, но не осуждённых, как это было в деле, не отвечает требованию о соблюдении справедливого баланса между конкурирующими публичными и частными интересами. Таким образом, государство-ответчик вышло за пределы приемлемых пределов усмотрения. Соответственно, хранение персональных данных представляло собой несоразмерное вмешательство в право заявителей на уважение личной жизни и не могло считаться необходимым в демократическом обществе.

Обстоятельства приведённого дела аналогичны тем, на которые ссылается Административный истец в части массового и неизбирательного характера применения технологии распознавания лиц властями столицы, а также отсутствия чётких и сбалансированных с точки зрения публичных и частных интересов правил обработки биометрических данных граждан в государственных информационных системах г. Москвы. С учётом позиции ЕСПЧ, изложенной в указанном деле, действия Административных ответчиков по применению технологии распознавания лиц на территории города Москвы в «Городской системе видеонаблюдения», построенной на базе ЕЦХД, нельзя назвать соразмерными, разумными и необходимыми в демократическом обществе.

Таким образом, действия Административных ответчиков по применению технологии распознавания лиц на территории города Москвы в «Городской системе видеонаблюдения», построенной на базе ГИС ЕЦХД, не основаны на законе, нарушают установленные правила обработки биометрических данных и нарушают права Административного истца на частную жизнь, гарантированные ст.ст. 23, 24 Конституции РФ и ст. 8 Конвенции о защите прав человека и основных свобод от 4 ноября 1950 года.

На основании вышеизложенного, руководствуясь ст. 4, ст. 19, ч. 4 ст. 24, ст. 124 КАС РФ,

ПРОШУ СУД:

1. Признать незаконным действия Административных ответчиков по применению технологии распознавания лиц на территории города Москвы в «Городской системе видеонаблюдения», построенной на базе ГИС ЕЦХД.
2. Обязать Административных ответчиков воздержаться от применения технологии распознавания лиц на территории города Москвы в «Городской системе видеонаблюдения», построенной на базе ГИС ЕЦХД.
3. Обязать Административных ответчиков удалить биометрические персональные данные и данные о частной жизни Административного Истца из базы данных изображений гражданина, применяемых в «Городской системе видеонаблюдения», построенной на базе ГИС ЕЦХД, и представить доказательства такого удаления.
4. Обязать Административного ответчика ГУ МВД России по г. Москве в лице МВД России принять подзаконный акт о порядке использования технологии распознавания лиц и данных из ГИС ЕЦХД.
5. Взыскать в пользу Административного истца компенсацию морального вреда 100 000 (сто тысяч) рублей.

Приложения:

1. Квитанция об оплате государственной пошлины;
2. Копия нотариального протокола осмотра переписки в мессенджере «Telegram» и отчёта «пробива лица» от 23 июля 2020 года;
3. Новость на Официальном сайте Мэра Москвы от 28.09.2017 г. “В Москве заработала одна из крупнейших в мире систем видеонаблюдения с функцией распознавания лиц”. URL: https://www.mos.ru/news/item/30105073/;
4. Информация о государственной закупке №0173200001419000838. URL: http://zakupki.gov.ru/epz/order/notice/ok504/view/common-info.html?regNumber=0173200001419000838;
5. Доклад специального докладчика ООН по вопросам самовыражения Дэвида Кея A/HRC/41/35 «Слежение и права человека». URL: https://undocs.org/ru/A/HRC/41/35;
6. Копии административного искового заявления для сторон (2 экз.)

«15» сентября 2020 г.