Вестник Томского государственного университета. 2019. № 449. С. 201–212. DOI: 10.17223/15617793/449/25

УДК 004.048; 34.343

О.И. Андреева, В.В. Иванов, А.Ю. Нестеров, Т.В. Трубникова

ТЕХНОЛОГИИ РАСПОЗНАВАНИЯ ЛИЦ В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ: ПРОБЛЕМА ОСНОВАНИЙ ПРАВОВОГО РЕГУЛИРОВАНИЯ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Обобщены современные практики внедрения в общественную жизнь и практическую деятельность технологий видеонаблюдения и распознавания лиц. Проведен анализ нормативно-правового регулирования данной деятельности в различных государствах. Показан фундаментальный характер возникающих этико-правовых проблем. Определено, каким требованиям должно отвечать нормативное регулирование применения технологий, основанных на деятельности искусственного интеллекта вообще и систем распознавания лиц в частности.

Ключевые слова: цифровизация в уголовном процессе; правовое регулирование использования искусственного интеллекта; этика искусственного интеллекта; технологии распознавания лиц; третья природа; права человека.

Современное общество находится на этапе глобального перехода к новому технологическому укладу, связанному с «цифровой революцией», значение которой определяется не только изменениями в технологиях, но и, в неменьшей (если не в большей) степени, коренной перестройкой состояния общественных институтов, включая формы и модели организации общества, механизмы государственного управления, а также общественные системы ценностей и идеологии. Все формы взаимодействия субъектов социума прямо определяются материально выраженными технологиями взаимодействия, так что фундаментальная проблема не только правоведения, но и гуманитарного знания в целом заключается в теоретической экспликации роли техники в социальных процессах, выявлении совокупности этико-аксиологических проблем, создаваемых научно-техническим прогрессом, отыскании форм опережающего или по крайней мере не запаздывающего правового реагирования.

Цифровые технологии создают «третью природу», новую форму действительности, существенно отличающуюся не только от искусственной природы «века прогресса», но и от техносреды «атомного века». В имеющемся на настоящий момент разнообразии экономических, социологических и исторических способов обоснования научно-технического прогресса, определения его влияния на социальные процессы следует руководствоваться, на наш взгляд, концепциями, в которых техника – в виде однажды изобретенных и далее объективно существующих инструментов (технологий) достижения целей человека – понимается как основа всякой материальной культуры [1]. Общая логика развертывания научно-технического прогресса связана с преобразованием окружающей человека среды, изначально – естественной природы. Пока технические возможности человечества ограничивались созданием артефактов в области физического мира, гуманитарная деятельность и право могли опираться на этические кодексы традиционных религий и устоявшиеся, складывавшиеся столетиями мировоззренческие принципы тех или иных национальных культур. Однако с развитием кибернетики функции технических объектов не исчерпываются исполнением целей человека в физическом мире, но все более и более затрагивают нефизические сферы: мышления, эмоций, принятия решений и т.п. В первой трети XXI в. возникают технологии, радикально меняющие доступ человека к физической и социальной реальности, к самому себе. Это технологии «искусственного интеллекта» в самом общем смысле этого термина, подразумевающие наличие в человеческом окружении таких технических объектов, которые обладают сопоставимым с человеком или превосходящим его доступом к объективной реальности, причем этот «доступ» может осуществляться как рецептивно, так и проективно: технический объект превращается в технический субъект, функционирующий не только в режиме (пассивного) познания, но и режиме (активного) воздействия на действительность.

В результате возникает ряд этических и правовых проблем как фундаментального, так и сугубо прикладного характера. В первом случае следует говорить об этике искусственного интеллекта, понимая под проблемой ряд задач осмысления фундаментальной трансформации трихотомии свой / другой / чужой, оценки социально-гуманитарных последствий масштабного внедрения «интеллектуальных» технологий, обеспечения национальной безопасности в новых технологических условиях. Во втором случае следует анализировать возможные и необходимые формы реакции правовых систем на технологические вызовы, накапливать и обобщать опыт правового регулирования возникающих явлений, изучать и фиксировать приемлемые формы трансформации права в новых условиях [2].

Один из наиболее ярких примеров этико-правовых проблем прикладного характера – активное использование интеллектуальных систем видеонаблюдения, имеющих функцию распознавания лиц, а также анализа поведения наблюдаемого лица. Интеллектуальные системы видеонаблюдения активно внедряются не только в деятельность органов внутренних дел и государственного управления, но и в деятельность коммерческих организаций (транспортных организаций, банков, супермаркетов, кафе), поскольку результаты обработки визуальной информации с применением нейронных сетей могут не только использоваться для предотвращения, раскрытия и расследования преступлений, но и обеспечивать безопасность, облегчать доступ к финансовым продуктам и повышать продажи.

На данный момент лидером по массовости и эффективности использования камер видеонаблюдения и поиска людей с их помощью, а также в области распознавания лиц с помощью специального оборудования можно назвать Китай. По официальным данным, в 2017 г. в стране были установлены 176 млн камер, еще около 450 млн планируется установить до 2020 г. (для сравнения, в США их около 50 млн). Неизвестно, сколько китайских камер оборудованы системой распознавания лиц, но, по задумке властей, к 2020 г. искусственный интеллект сможет за три секунды узнать в лицо каждого из почти 1,4 млрд жителей страны. Система распознает идущего по улице человека и может отправить необходимый сигнал правоохранителям: человек имеет неоплаченные штрафы / уклоняется от уплаты алиментов / находится в розыске [3]. С помощью этой технологии китайское правительство сможет собирать гигантский объем информации о своих гражданах. Объединив эти данные с базами полиции, банков и онлайн-сервисов, власти планируют с 2020 г. ввести по всей стране так называемый рейтинг общественной надежности. Каждому жителю будет присваиваться определенное количество баллов, исходя из его поведения. На основе этих баллов ему будут открывать (или закрывать) доступ к таким привилегиям, как туристические визы, социальные пособия или выгодные ставки по кредитам.

Распознавание лиц нередко используется в социально значимых целях. Так, компания Marinus Analytics использует искусственный интеллект в сервисе Amazon Rekognition для разработки инструментов, таких как Traffic Jam, которые позволяют правозащитным агентствам выявлять жертв работорговли и определять их местоположение. Эксперты экономят ценное время за счет анализа изображений при автоматическом поиске среди миллионов записей в течение нескольких секунд. Ранее этот процесс требовал индивидуального анализа с привлечением специалистов [4]. Другой пример – финансовая компания Aella Credit, расположенная в Западной Африке и предлагающая банковские услуги через мобильное приложение лицам, не имеющим доступа к основным финансовым услугам на новых рынках. Благодаря функциям обнаружения и сравнения лиц компания Aella Credit осуществляет проверку личности без вмешательства человека. Такой простой сценарий использования технологии распознавания лиц позволяет получить доступ к финансовым услугам лицам, которые иначе не смогли бы его получить.

«Умные» системы видеонаблюдения используются в правоохранительной деятельности. Так, еще по состоянию на 2013 г. в Великобритании число установленных видеокамер приближалось к четырем миллионам, Часть из них способны отслеживать, нет ли на теле проходящего человека каких-либо подозрительных предметов, а также распознавать лица людей, находящихся в розыске [5].

В нашей стране сегодня также применяются системы распознавания лиц. Эта практика находится в стадии становления, и первопроходцем здесь является столица. Так, в Московском метрополитене в 2019 г. начали тестировать систему биометрической идентификации. На данный момент камеры видеонаблюдения с новой функциональностью установлены на всех турникетах двух станций метро, а именно на станциях «Октябрьское Поле» и «Сухаревская». Сейчас распознавание лиц осуществляется для обеспечения безопасности, а в будущем оно может быть использовано и для оплаты проезда. Система на основе искусственных нейросетей, которую внедряет авиакомпания S7, позволяет идентифицировать пассажира, просканировав его лицо. Сейчас она работает в московском аэропорту Домодедово в тестовом режиме. «Умные» камеры позволяют попасть, не доставая документов, в бизнес-зал в зоне вылета рейсов по России [6]. Подобные практики внедряются и в банках, предлагающих гражданам оставить свои биометрические данные, для удобства обслуживания и повышения безопасности банковских вкладов.

Аппаратно-программные комплексы технических средств «Безопасный город» функционируют в городах в целях мониторинга и предупреждения различных угроз общественной безопасности, правопорядку и безопасной среде обитания. Одним из направлений реализации данного комплекса является предупреждение и выявление правонарушений посредством системы наружного видеонаблюдения, из которой видеоинформация поступает в дежурные части органов внутренних дел [7]. Первые 1 500 камер с технологией распознавания лиц протестировали в Москве в 2017 г., а в 2018 г. в столице к системе подключили уже более 7 000 камер. До конца 2019 г. власти Москвы планируют объявить конкурс на создание новой системы распознавания лиц, которая должна охватить более 200 тысяч камер города [8]. Изначально сотрудники московской полиции скептически относились к технологии, однако успешные результаты эксперимента их переубедили. Согласно отчетам МВД за два года (2018–2019) – 1 000 умных камер, расположенных у подъездов жилых домов, помогли задержать 90 разыскиваемых людей. Также система распознавания лиц, внедренная на станциях метрополитена, позволила проводить по 5–10 задержаний ежемесячно [9]. Камеры самостоятельно сопоставляют лица из видеопотока с базой данных людей, находящихся в розыске, и в случае совпадений сообщают находящемуся рядом сотруднику полиции.

Отмечается тенденция внедрения данной системы и в других городах России. Так, на улицах Екатеринбурга в ближайшее время начнут устанавливать камеры, оснащенные системой распознавания лиц. Такое заявление сделал в эфире радиостанции «Серебряный дождь» директор «НПО Автоматики» Андрей Мисюра. По его словам, первые камеры появятся в микрорайоне «Академический». Искусственный интеллект должен будет анализировать поведение жителей района. «Сотрудничество подразумевает организацию интеллектуального пространства, включающего в себя системы управления потоками личного, служебного и общественного транспорта, интеллектуальное парковочное пространство и системы планирования маршрутной дорожной сети» [10]. В тестовом режиме работает и система цифрового распознавания лиц на

железнодорожном вокзале Самары, о чем сообщает правительство Самарской области. Но, кроме этого, систему распознавания лиц планируют внедрить на станциях метрополитена, на центральном автовокзале и на набережной реки Волги. Впервые систему по распознаванию лиц использовали на чемпионате мира по футболу – 2018. Благодаря системе во время чемпионата удалось выявить 27 человек, в том числе пять иностранцев, ранее совершавших противоправные действия, а в 2019 г. распознать и задержать двух правонарушителей [11].

Более того, нейросети, осуществляющие распознавание лиц, способны и более «активно» участвовать в обнаружении и раскрытии преступлений, реагируя на выявляемое ими «подозрительное» поведение или обнаруживая «подозрительное» видеоизображение. Так, в Китае мужчина задушил свою подругу, после чего взял ее смартфон и запустил банковское приложение Money Station, чтобы снять с ее счета 4 200 долларов, из-за которых и произошла ссора. Данное приложение использовало для доступа к финансовым операциям функцию распознавания лиц, поэтому мужчина продемонстрировал на камеру лицо убитой девушки. Однако искусственный интеллект, обрабатывающий биометрическую информацию, распознав неподвижное лицо женщины, не только не предоставил злоумышленнику доступ к банковскому счету жертвы, но и «забил тревогу», дав персоналу банка сигнал, чтобы они самостоятельно посмотрели на ее лицо. Сотрудники банка заметили, что на ней есть синяки и странный след на шее, похожий на тот, что остается от удушья, нашли место нахождения женщины по геолокации и вызвали полицию. В результате полиция задержала убийцу в тот момент, когда он пытался сжечь тело жертвы [12].

Использование технологии распознавания лиц может существенно облегчить человеческую деятельность. Эта функция используется во многих смартфонах в качестве средства идентификации владельца. Ряд крупных компаний используют системы распознавания лиц вместо обычных пропусков в своих системах безопасности. Так, в компании СИБУР технология распознавания лиц используется для идентификации работников и посетителей в системе управления доступом в офис, а также для оплаты питания в корпоративной столовой. Использование технологии позволило упростить режим получения доступа на территорию гостями – они могут воспользоваться для пропуска на территорию киоском самостоятельной регистрации [13]. Предполагается, что используемая в аэропорту Домодедово система, включающая модуль распознавания лиц, может сделать существенно более удобным пребывание пассажиров на территории аэропорта, например, вместо объявлений с фамилиями опаздывающих пассажиров будут приходить индивидуальные напоминания по SMS о том, что пассажиру пора пройти контроль безопасности или пройти на посадку [6].

Зачастую технологии распознавания лиц начинают применяться в бизнесе для увеличения продаж, сокращения расходов, создания более персонализированного сервиса, и не всегда это происходит с согласия субъектов, изображения которых анализируются нейронными сетями. Например, в ряде магазинов, торговых центров и даже в кафе и ресторанах технология распознавания лиц используется для того, чтобы обнаружить людей, ранее внесенных в «черный список» (например, за попытку что-то украсть), проанализировать поведение покупателя / клиента (например, его покупки, привычки, маршрут перемещения по территории торгового комплекса), его эмоции и удовлетворенность посещением магазина / кафе (система анализирует – есть ли на его лице улыбка и сигнализирует, обнаружив недовольного клиента), с тем чтобы увеличить продажи и повысить лояльность к сети [13, 14]. Заодно некоторые системы осуществляют среди посетителей поиск по базам правоохранительных органов [13].

Другие направления применения данной технологии еще более явно вторгаются в частную жизнь граждан. Например, в одной из школ китайского города Ханьчжоу появилась система, которая каждые несколько минут анализирует выражение лиц учащихся, отслеживает, чем занимаются дети и что они едят в школьной столовой [15]. Это вызывает страх того, что с развитием технологий видеонаблюдения и распознавания лиц право граждан на неприкосновенность частной жизни может быть фактически утрачено. По мере того как алгоритмы компьютерного зрения становятся все эффективнее, у людей почти не остается шансов вырваться из-под негласного наблюдения. Причем, как уже было показано, собранные данные могут использоваться не только для правительственного контроля, но и в коммерческих целях.

Другая проблема применяемых технологий распознавания лиц – их несовершенство, ведущее к возможности ошибочного распознавания. Конечно, его точность сильно возросла за последние несколько лет. Согласно оценкам самих компаний, разрабатывающих соответствующие алгоритмы, на сегодняшний день точность распознавания колеблется от практически 100% в ситуации, когда решается проблема верификации, т.е. проверки тождества личности (например, при работе в системах охраны), до примерно 80% точности, когда речь идет об огромных выборках (более полумиллиарда фотографий). Более того, производители, например, утверждают, что современные технологии позволяют узнать человека, даже если 40% его лица закрыта, в дальнейшем этот критерий планируется довести до 50%. Не являются для них помехой и очки, борода, усы, прическа, парик, макияж. Более того, утверждается, что если нужно идентифицировать человека, а его исходная фотография двадцати- или тридцатилетней давности, для системы никакой разницы нет: она убирает все возрастные изменения лица и практически мгновенно выдает результат [16]. Оценки, сформированные в ходе практики применения интеллектуальных систем видеонаблюдения, более чем существенно отличаются от декларируемых. Так, в 2018 г. сообщалось, что в Лондоне, где тестируется технология распознавания лиц (AFR) на публичных мероприятиях, концертах, фестивалях и футбольных матчах, AFR распознает правильно только 2% лиц, остальные случаи являются

ложными, поскольку система неправильно идентифицирует людей. Из двух правильных совпадений полиция не смогла никого арестовать – один из людей оказался из старой базы данных, второй – психически нездоровым человеком [17].

Существуют и опасения, связанные с «предвзятостью» искусственного интеллекта в системах распознавания лиц. Так, в 2017 г. разработчик системы распознавания лиц Gfycat удивился, когда его система не распознала некоторых азиатских сотрудников. Исследование аналогичных систем Microsoft и IBM показало, что они были на 95% точнее при распознавании женщин со светлой кожей. Есть признаки того, что система Amazon Rekognition чаще ошибается при сравнении чернокожих лиц, особенно женщин. Причина в том, что нейросеть учится распознавать лица самостоятельно, основываясь на предоставленных ей фотографиях и видео. Поэтому качество обучения нейросети зависит напрямую от качества предоставленных данных. Если в выборке, по которой обучается нейросеть, например, азиатов или темнокожих в десять раз меньше, чем европейцев, то нейросеть будет хуже распознавать представителей этих рас [18, 19]. Таким образом, ошибки распознавания все-таки возможны, они могут быть выше для отдельных категорий населения, особенно для немногочисленных и редко встречающихся этнических групп. Эти ошибки распознавания могут привести, например, к ошибочным задержаниям.

Опасения утраты конфиденциальности, приватности, страх неоправданного вторжения в право на частную жизнь приводят к тому, что начинает развиваться общественное противодействие широкому применению интеллектуальных систем видеонаблюдения, технологий распознавания лиц. Оно, во-первых, выражается в исследовании того, как можно «обмануть» искусственный интеллект, противодействовать реализации используемых им алгоритмов. Например, специалисты в области искусственного интеллекта из компании Facebook разработали систему для «деидентификации» пользователей в режиме реального времени. По результатам раннего тестирования, искусственный интеллект (ИИ) способен обойти современные системы распознавания лиц [20]. Создаются украшения, препятствующие тому, чтобы программы могли распознавать лица пользователей на фотографиях, исследуются варианты «обхода» используемых алгоритмов работы нейросетей [21, 22]. Обсуждаются перспективы применения масок-анонимайзеров и других средств, маскирующих лица и затрудняющих распознавание [23].

Во-вторых, появились первые попытки защиты права на неприкосновенность частной жизни с применением правовых инструментов: обращения к судебной защите и лоббированию принятия нормативных актов, направленных на ограничение и строгую регламентацию применения интеллектуальных систем видеонаблюдения. Так, Британская правозащитная организация Liberty назвала технологию распознавания лиц угрозой для демократии. По словам активистов, ее применение в Великобритании, где плотность камер видеонаблюдения выше, чем в какой-либо другой западной стране, означает полную утрату частной жизни. Российская общественная организация «Роскомсвобода» запустила кампанию с требованием ввести мораторий на использование этой технологии. Роскомсвобода выступает за принятие законодательных либо судебных мер для введения моратория на использование систем распознавания лиц, которые являются технологиями двойного назначения и должны быть запрещены до тех пор, пока не будет обеспечена полная прозрачность и безопасность их использования для граждан [24].

Начиная с июня 2018 г. Liberty представляет в суде интересы жителя Кардиффа Эда Бриджеса, который обвинил полицию Южного Уэльса в незаконном применении технологии автоматического распознавания лиц [25]. 7 октября 2019 г. в России политическая активистка Алена Попова подала в Савеловский суд Москвы иск с требованием признать незаконным применение столичным правительством технологии распознавания лиц в городской системе видеонаблюдения [26]. Оба иска были проиграны в первой судебной инстанции, оба истца планируют продолжать отстаивать свою позицию в вышестоящих судебных инстанциях. Однако следует отметить, что основания, по которым суды признали отсутствие нарушения закона в отношении истцов, сильно различались. Британский суд исследовал конкретные правила применения технологии и принял во внимание непродолжительный срок хранения фотографий лиц на сервере правоохранительных органов. Российский же – согласился с ответчиками, которые отрицали, что при использовании технологии распознавания лиц ведется работа с данными, которые позволяют идентифицировать лицо, и поэтому не нарушается законодательство об обработке персональных данных.

В качестве примера противоположного подхода к проблеме можно привести недавнее решение властей г. Сан-Франциско о запрете на передачу органам правопорядка в режиме реального времени информации, зафиксированной камерами видеонаблюдения. Исключение сделано только для объектов транспортной инфраструктуры (аэропорты, вокзалы), безопасность на которых обеспечивают не местные, а федеральные органы правопорядка. Принятое решение было обосновано опасениями бесконтрольного и безосновательного вторжения государства в сферу личных прав человека и в первую очередь его права на приватность, а также возможностью ошибок в распознавании, в особенности в отношении афроамериканок или представительниц других этнических групп, где вероятность ошибки выше. В качестве компромисса местные жители планируют пересмотреть вопрос использования данной технологии, когда та будет усовершенствована, поскольку, по их словам, технология распознавания лиц может сыграть важную роль в поиске пропавших без вести или жертв торговли людьми, а также в вычислении потенциальных террористов. Однако правозащитники считают, что, даже если распознавание лиц было бы на 100% точным, полиция все равно могла бы злоупотреблять этой технологией в отношении протестующих или представите-

лей некоторых общин, например в отношении мусульман, посещающих мечети.

Предложения о введении аналогичного запрета рассматриваются в Окленде, штат Калифорния, и Сомервилле, штат Массачусетс. Так, власти калифорнийского Окленда обосновали свое решение тем, что «умные камеры» приведут к вторжению в частную жизнь (нарушение права на неприкосновенность частной жизни) и нарушениям прав меньшинств. Как ожидается, в ближайшее время аналогичные запреты будут введены и в других городах США. В перспективе – федеральный запрет на распознавание лиц по всей стране. Теперь в Окленде запрещено покупать и использовать технологии распознавания лиц. Запрет распространяется и на полицию. Как ожидается, к трем американским городам, запретившим распознавание лиц, присоединятся и другие. Например, подобные меры обсуждают в калифорнийском Беркли. Аналогичные проекты внесены в законодательные собрания штатов Массачусетс и Мичиган [27, 28].

В Сенат США внесен законопроект под названием «Акт о приватности при коммерческом распознавании лиц, 2019» (Commercial Facial Recognition Privacy Act of 2019). Авторы этого законопроекта являются членами сенатского Комитета по торговле, науке и транспорту и представляют разные партии. Предлагаемый для рассмотрения Сенатом закон запретит коммерческим заказчикам систем распознавания лиц собирать и передавать куда-либо получаемые данные по идентификации и отслеживанию людей без их информированного согласия. Законопроект также требует проводить независимое тестирование системы до ее внедрения. Цель – подтвердить, что система работает точно и не подвержена систематической ошибке, ставящей людей в неравное положение, например по расовым признакам, а также избежать причинения вреда тем, чьи лица распознаются. Кроме того, законопроект задает условия для составления четких требований к тем, кто разрабатывает и внедряет системы распознавания лиц, а также хранит данные [29].

Из изложенного видно, что при переходе к новому технологическому укладу, связанному с «цифровой революцией» (в частности, в связи с развитием технологий искусственного интеллекта, использованием их для видеонаблюдения, распознавания лиц и их поведения), возникает ряд этико-правовых проблем, практически не имеющих национальной и региональной специфики, носящих фундаментальный характер. Конечно, в наиболее общем виде границы применения рассматриваемых технологий уже закреплены в нормативно-правовых актах высшей юридической силы: национальных конституциях и в международных договорах. Например, для России это будут наиболее общие нормы, содержащиеся в положениях Конституции РФ и ратифицированных РФ международных договоров, в разделах, закрепляющих право человека на неприкосновенность личной жизни / права на частную жизнь, а также допустимых оснований, порядка и пределов его ограничения (ст. 23, 46 и 56 Конституции РФ, ст. 8 и 6 Конвенции о защите прав человека и основных свобод). Однако эти права и возможности их ограничения в данных актах сформулированы настолько широко, что требуют непременной конкретизации в других правовых актах и / или сформированной судебной практике, поскольку иначе сохраняется ситуация неопределенности. Так, на сегодняшний день нет единого мнения по вопросу о том, «вторгается» ли видеофиксация происходящего в общественных местах, сопряженная с возможностью распознавания лиц, в право человека на частную жизнь, в каких ситуациях она допустима, как можно выстраивать в новых технологических условиях баланс между различными частными интересами (интересом лица на неприкосновенность его частной жизни и интересом организации на контроль происходящего на ее территории) и интересами общества / государства (на раскрытие преступлений, обеспечение безопасности, на упрощение ряда процедур (проверка билетов на мероприятие, посадка в самолет, и пр.)).

Для Европейского Союза основным нормативным актом в области защиты персональных данных является Регламент Европейского Парламента и Совета Европейского Союза 2016 / 679 от 27 апреля 2016 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных / General Data Protection Regulation / GDPR), который вступил в силу в мае 2018 г. Данный регламент применяется в отношении обработки персональных данных, производимой полностью либо частично при помощи автоматизированных средств. Его действие не распространяется на деятельность правоохранительных органов, осуществляемую в целях предупреждения, расследования, выявления уголовных преступлений, или привлечения к ответственности, или приведения в исполнение уголовных наказаний, включая защиту и предотвращение угроз общественной безопасности (статья 2 Регламента). Данный документ рассматривает право на защиту персональных данных в качестве нового самостоятельного права лица, которое должно быть уравнено с другими основными правами в соответствии с принципом пропорциональности. Согласно ему, фотографии человеческого лица считаются «биометрической информацией», которую разрешено обрабатывать только в случаях, прямо перечисленных в статье 9 этого Регламента. К числу исключений, делающих возможной обработку персональных данных, относятся, например, наличие прямого согласия субъекта на обработку его персональных данных, а также наличие особого общественного интереса, в случаях, предусмотренных законодательством. При этом ограничение права лица на защиту его персональных данных должно быть пропорционально преследуемой цели, соответствовать сущности права на защиту данных и предусматривать приемлемые и конкретные меры для защиты основных прав и интересов субъекта данных. Таким образом, законодательство государств – членов Европейского Союза должно предусматривать меры защиты лиц от обработки их биометрических данных без их прямого согласия. Как уже указывалось ранее в данной статье, такое законодательство на настоящий момент отсутствует.

В действующем российском законодательстве пока нет единого кодифицированного акта, регулирующего деятельность по организации и осуществлению видеонаблюдения, использованию биометрических данных. Действующее правовое регулирование отдельных правовых аспектов видеонаблюдения крайне фрагментарно. Видеоизображение человека, полученное с помощью камер видеонаблюдения, относится к персональным данным этого человека. Однако жестких правил сбора, обработки и распространения таких сведений в настоящее время не существует. Есть лишь разрозненное рамочное упоминание этого явления в отдельных законах (см. например: ст. 152.1 ГК РФ, ст. 3 ФЗ РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных»).

Согласно ст. 11 ФЗ РФ «О персональных данных», сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, прямо предусмотренных законом. Возникает вопрос – можно ли считать биометрическими персональными данными видеоизображения лица, сделанные в публичных местах. До появления интеллектуальных систем распознавания ответ был отрицательным. Например, в силу п. 2 ч. 1 ст. 152.1. Гражданского Кодекса РФ не требуется согласие гражданина на использование его изображения, полученного в публичном месте, при условии, что такое изображение не является основным объектом использования. То есть информация из публичных мест не считалась информацией о частной жизни отдельного гражданина. Кроме того, сам факт нахождения гражданина в публичном месте ранее однозначно расценивался как действия за рамками частной жизни. Следует согласиться с тем, что данный принцип отграничения частной жизни от публичной был справедлив только до появления систем распознавания и отслеживания [30].

Согласно разъяснениям Роскомнадзора, данным в 2013 г., материалы видеосъемки в публичных местах и на охраняемой территории не являются биометрическим персональными данными до момента их передачи для установления личности запечатленного на них человека. Достаточно того, чтобы посетители указанных публичных мест заранее предупреждались их администрацией о возможной фото-, видеосъемке соответствующими текстовыми и / или графическими сообщениями. По мнению Роскомнадзора, при соблюдении указанных условий согласие субъектов на проведение указанных мероприятий не требуется [31].

С использованием систем распознавания информация, полученная в результате наблюдения за неопределенным кругом лиц, может быть трансформирована в информацию о каждом заснятом гражданине. При этом распространенность наблюдения приводит к возникновению большого объема данных, которые могут быть автоматически обработаны и привязаны к конкретному лицу. Следует согласиться с тем, что применение систем распознавания лиц в общественном наблюдении должно признаваться сбором информации о частной жизни гражданина, невзирая на то, что место является публичным и наблюдение ведется за неопределенным кругом лиц [30], а фото и видеоизображения лица, сделанные в ходе такого видеонаблюдения, должны обрабатываться по правилам работы с биометрической информацией. Это требует внесения в законодательство изменений, которые верно определяли бы статус таких материалов и предусматривали такие правила работы с ними, которые будут соответствовать новым технологическим реалиям и выстраивать справедливый баланс между правом человека на тайну личной жизни и на тайну персональных данных с интересами общества, государства, коммерческих субъектов на обработку такой информации при помощи интеллектуальных систем.

Таким образом, мы видим, что реакция государства «не успевает» за бурным развитием технологий, за появлением все новых вызовов и потенциальных проблем, требующих своевременного разрешения на уровне создания правового регулирования, отличающегося достаточной точностью и четкостью формулировок. Законодатели всех государств вынуждены действовать практически «наобум», «латая дыры» в системе нормативно-правового регулирования применения современных IT-технологий. Попытаемся определить хотя бы в общей форме, каким же должно быть специфическое нормативно-правовое регулирование для применения технологий распознавания лиц, основанных на использовании искусственного интеллекта, на каких основаниях оно должно быть построено.

1. Для интеллектуального видеонаблюдения, распознавания лиц в настоящее время, как правило, используются системы, основанные на технологиях машинного обучения (искусственного интеллекта). Их функционирование вызывает ряд проблем, опасений, которые связаны как с особенностями искусственного интеллекта вообще, так и с применением его в рассматриваемых в статье целях. Это опасения того, что ИИ будет использован во зло, для манипуляции людьми и тотальной слежки; опасность ошибки, неверного распознавания лица; возможного дискриминационного характера решений, принятых на основе его деятельности. Так, 44% опрошенных россиян обеспокоены возможными этическими проблемами использования искусственного интеллекта. Еще 35% тревожатся из-за непрозрачности решений ИИ (против 31% в среднем по миру). В целом 49% россиян усомнились в способности ИИ формировать точные результаты и корректный анализ. 51% опрошенных не согласны с применением ИИ для определения виновности в уголовном процессе. 40% россиян не хотят, чтобы искусственный разум определял методы лечения [32].

С учетом этого первая группа оснований законодательства, регламентирующего возможность использования ИИ вообще и его применения в системах видеонаблюдения в частности, должна быть связана с определением правил «взаимодействия» между искусственным интеллектом и человеческим обществом.

Представляется, что достаточные оптимальные правила для такого взаимодействия сформулированы в Хартии об этических принципах применения искусственного интеллекта в судебных системах, принятой Европейской комиссией по эффективности правосудия. Согласно этой Хартии, внедрение искусственного интеллекта должно производиться ответственным образом и не нарушать положений Европейской Конвенции и Конвенции о защите личных данных. В Хартии обозначено пять основных принципов:

– принцип уважения фундаментальных прав – разработка и внедрение искусственного интеллекта не должны нарушать фундаментальные права человека;

– принцип отказа от дискриминации – предотвращение появления или усиления дискриминации в отношении отдельных людей и групп;

– принцип качества и безопасности – обработка судебных решений и данных должна проводиться в технически защищенной обстановке, на основании проверенных источников и с применением моделей, разработанных специалистами нескольких научных дисциплин;

– принцип открытости, беспристрастности и честности – методы обработки данных должны быть доступными и понятными для возможности проверки третьей стороной;

– принцип контроля со стороны пользователя – пользователи должны владеть правом выбора и необходимой информацией [33].

2. Вторая группа оснований предопределяется необходимостью соблюдения баланса частных и публичных интересов и отражает пределы вмешательства государства в сферу частных интересов, обязанности государства по защите права граждан на частную жизнь от вторжения в сферу действия этого права других частных субъектов. Ранее мы уже формулировали общие подходы к определению такого баланса [34–36]. Поэтому только обозначим сейчас нашу позицию, согласно которой для определения оптимального соотношения необходимо проведение исследований практики, ожиданий и опасений общества. При его определении могут быть использованы сформулированные Европейским Судом по правам человека (ЕСПЧ) правила, на основе чего должны быть выработаны как позитивные обязанности государства (меры к защите прав и интересов, которые оно обязано предпринять), так и его негативные обязанности, предопределяющие допустимые пределы его вмешательства в частную жизнь граждан. Основой для решения указанных проблем может стать концепция, в рамках которой конституционное право каждого на судебную защиту (принадлежащее как всем гражданам, так и обществу, заинтересованному в судебной защите от правонарушений, в целом) рассматривается как универсальный способ согласования, гармонизации различных интересов, как необходимое средство для их реализации, для пресечения злоупотребления правом.

Что же касается подходов Европейского Суда по правам человека к обеспечению баланса интересов при использовании интеллектуальных систем видеонаблюдения, то ЕСПЧ обращался к проблемам видеонаблюдения несколько раз по жалобам на установление скрытого видеонаблюдения за сотрудниками на их рабочем месте в аудиториях университета (дело «Антович и Миркович против Черногории»), за кассирами в магазине (дело «Лопес Рибалда и другие против Испании»), на осуществление видеонаблюдения в рамках осуществления оперативно-розыскной деятельности (Постановление ЕСПЧ по делу «Зубков и другие против Российской Федерации»). Однако в этих Постановлениях речь шла об обычном, «традиционном» видеонаблюдении. Применительно к интеллектуальным системам видеонаблюдения решения ЕСПЧ пока отсутствуют, но нам кажется возможным опереться на правовые позиции Суда, сформированные и отраженные в Постановлении ЕСПЧ по делу «Big Brother Watch и другие против Соединенного Королевства» [37]. Это дело касается практики перехвата данных неопределенно широкого круга лиц и применения интеллектуальных методик их анализа. В данном деле речь шла о том, что сведения о переговорах неопределенно широкого круга лиц подвергались проверке: сначала с автоматическим применением через компьютер простых фильтров (таких как адрес электронной почты или телефонные номера) и первоначальных критериев поиска, а впоследствии путем применения комплексных поисковых систем. ЕСПЧ четко сформулировал шесть минимальных требований, которые должны быть отражены в законодательстве каждого государства с тем, чтобы избежать злоупотребления полномочиями со стороны органов государства при перехвате данных неопределенного количества лиц. По его мнению, соответствующее законодательство непременно должно содержать:

– указание на характер правонарушения, которое может обусловить выдачу ордера на перехват данных;

– определение категории лиц, чьи переговоры могут быть перехвачены;

– установление ограничения по продолжительности периода перехвата данных;

– определение процедуры для исследования, использования и хранения полученных данных;

– меры предосторожности при передаче данных третьим лицам;

– определение обстоятельств, при которых перехваченные данные могут и должны быть стерты или уничтожены.

При этом, по мнению ЕСПЧ, такое законодательство может не включать требования наличия объективного доказательства разумного подозрения в отношении лиц, о которых собирается информация, получения предварительного независимого судебного разрешения на перехват данных и последующего уведомления объекта наблюдения о принятых мерах.

В том же, что касается фильтрации переговоров для анализа, ЕСПЧ указал, что фильтры и критерии поиска, используемые для обработки перехваченной информации, должны подвергаться независимой проверке. При неизбирательном перехвате данных, когда решение о перехвате информации не ограничивалось существенным образом условиями ордера, гарантии, применимые к фильтрации и отбору для исследования

информации, обязательно должны быть тщательно проработанными, исключать возможность анализа переговоров некоторых категорий лиц (адвокаты, журналисты, судьи) без индивидуально принятого решения.

Представляется, что эти критерии могут и должны быть адаптированы к неизбирательному применению видеозаписи и ее интеллектуальному анализу с применением различного рода фильтров (поведение лица, признаки его внешности, совпадение с признаками конкретного лица).

3. Третья группа оснований вызывается к жизни общим характером уже рассмотренных выше этических проблем, возникающих в связи с использованием технологий искусственного интеллекта, и выражается в необходимости разумного сочетания нормативно-правового регулирования применения таких технологий и «саморегуляции» деятельности профессионального сообщества их разработчиков, регламентации их поведения самостоятельно выработанными кодексами этики. С одной стороны, такого рода «саморегуляция» защищает интересы профессионалов в сфере IT, создавая четкую систему правил их поведения, давая возможность с достаточной определенностью предвидеть последствия своего поведения, исключить или урегулировать возможные противоречия между этическими воззрениями специалистов и предписаниями нормативных актов. С другой стороны, такой системой добровольного самоограничения профессиональные сообщества вызывают доверие гражданского общества, что повышает как их авторитет, так и доверие граждан к применению возможностей искусственного интеллекта.

В литературе рассматриваются вопросы о необходимости существования этических кодексов различных профессий и их функциональном предназначении. Отдельные авторы обоснованно признают за профессиональными этическими кодексами ряд важных функций, в числе которых:

– способность являться основой для коллективного признания членами определенной профессии своих обязанностей;

– способствование созданию среды, в которой этичное поведение является нормой;

– способность служить в качестве руководства или напоминания об обязанностях в конкретных ситуациях;

– ценность для профессии самого процесса разработки и модификации этического кодекса как средства самоидентификации;

– способность демонстрировать обществу, что члены той или иной профессиональной группы признают свои обязанности по отношению к обществу и серьезно обеспокоены тем, чтобы гарантировать ответственное, профессиональное поведение представителей данной профессии [38].

Ряд компаний уже принимает на себя добровольно обязательства, выполнение которых направлено на гарантирование прав частных лиц, предупреждение дискриминации при использовании технологий распознавания лиц. Так, заявление, появившееся сравнительно недавно в блоге Amazon, перечисляет пять правил правомочной системы распознавания лиц:

1) распознавание должно всегда использоваться в соответствии с законом, включая законы, защищающие гражданские права;

2) когда технологию применяют правоохранительные органы, необходим человеческий надзор как гарантия того, что использование прогнозов в принятии решений не нарушает гражданских прав;

3) когда технология распознавания лиц применяется правоохранительными органами для идентификации или другим способом, способным нарушить гражданские свободы, рекомендована 99-процентная степень уверенности;

4) правоохранительные органы должны быть прозрачны в применении технологии распознавания лиц;

5) следует уведомлять о совместном применении видеонаблюдения и технологии распознавания лиц в местах общественного и коммерческого использования.

Проведенное исследование свидетельствует, что, несмотря на многочисленные проблемы и неоднозначность взглядов на вопрос об использовании систем видеонаблюдения, они могут существенно повысить эффективность деятельности правоохранительных органов при раскрытии и расследовании преступлений. Без помощи видеонаблюдения будет гораздо меньше шансов установить и задержать лиц, совершивших преступления, защитить права, свободы и законные интересы потерпевших. Системы видеонаблюдения способны предоставить веские доказательства по уголовному делу. Благодаря видеозаписям становится проще установить личность преступника, способы совершения правонарушений, последовательность событий. С другой стороны, объединение видеокамер в единую сеть с возможностью анализа записей и идентификации человека по признакам внешности является существенным ограничением прав человека и вторжение в эту сферу возможно только при обеспечении существенных гарантий их защиты. Повсеместное внедрение камер видеонаблюдения, бесконтрольное развитие и применение современных технологий, использование систем видеонаблюдения искусственного интеллекта в уголовном судопроизводстве способно существенным образом ограничить права лиц, вовлеченных в уголовное судопроизводство [39, 40].

Это означает, что необходимо уже сейчас попытаться спрогнозировать, какие возможности использования интеллектуальных систем видеонаблюдения должны быть урегулированы уголовно-процессуальным законодательством, и определить, хотя бы в общей форме, подходы к такому нормативно-правовому регулированию. Полагаем, что пока эта технология находится в стадии совершенствования и апробации, до ее полномасштабного внедрения и применения еще есть время, в течение которого и предстоит выработать необходимые правила, позволяющие использовать систему распознавания лиц без угрозы нарушения прав человека.

Представляется, что в уголовно-процессуальном законе со временем должны найти отражение следующие возможности использования интеллектуальных технологий видеонаблюдения и обработки их результатов:

1. Контроль передвижений конкретного лица с применением систем видеонаблюдения. Увеличение количества используемых систем видеонаблюдения, объединение их в единую сеть способно дать возможность отслеживать перемещения конкретного лица в режиме реального времени или ретроспективно. Такой контроль со стороны государства является существенным ограничением прав лица, в отношении которого он осуществляется, поэтому одним из вариантов его применения может рассматриваться предварительный судебный контроль. Необходимо убедиться в наличии достаточных данных, дающих основания для подозрения лица в совершении серьезного преступления, и ограничить применение этой меры определенным сроком.

2. Результаты применения систем распознавания внешности в современных реалиях не могут использоваться в качестве доказательств по делу. Полученный результат можно сравнить с наиболее близким и понятным доказательством – заключением судебно-портретной экспертизы. В заключении эксперта традиционно содержатся не только выводы, предполагающие, наряду с прочим, решение вопроса о тождестве, но и исследовательская часть, в которой описан процесс получения результата (ответа на вопрос о наличии или отсутствии тождества). Результаты применения искусственного интеллекта сегодня не предполагают проверяемости полученных результатов. Это и является неопровержимым доводом в подтверждение тезиса о невозможности использования таких результатов в качестве доказательств. Любые попытки преодолеть этот запрет (например, путем осмотра видеозаписей и т.п.) должны в современных реалиях жестко пресекаться. Для этого целесообразно выработать соответствующий запрет в отечественном законодательстве.

3. Сохранение в качестве основного средства фиксации протокола не соответствует потребностям использования в доказывании цифровой информации, представленной в электронном виде: материалов видеофиксации, полученной в результате функционирования автоматизированных систем контроля в общественных местах. Бесполезным и бессмысленным является копирование такой информации в протокол следственного действия [41].

Считаем, что рассмотренная проблема требует более детального исследования. Невозможно отрицать распространение описанных технологий и их внедрение во все сферы нашей жизни. Представляется, что тщательная проработка этой проблемы должна осуществляться не только юристами, но и специалистами иных областей знаний.

ЛИТЕРАТУРА

1. Нестеров А.Ю. Семиотические основания техники и технического сознания. Самара: Изд-во Самарской гуманитарной академии, 2017. 155 с.
2. Иванов В.В., Нестеров А.Ю. Право в искусственной среде третьей природы: юридический статус цифрового двойника // Мир человека: Нормативное измерение – 6. Нормы мышления, восприятия, поведения: сходство, различие, взаимосвязь : сб. трудов междунар. конф. Саратов, 2019. С. 234–240.
3. В Китае создают тотальную систему распознавания лиц граждан. Она поможет ловить преступников и собирать данные на всех остальных. URL: https://meduza.io/feature/2018/02/11/v-kitae-sozdayut-totalnuyu-sistemu-raspoznavaniya-lits-grazhdan-ona-pomozhet-lovit-prestupnikov-i-sobirat-dannye-na-vseh-ostalnyh (дата обращения: 19.11.2019).
4. Факты о распознавании лиц с помощью искусственного интеллекта. URL: https://aws.amazon.com/ru/rekognition/the-facts-on-facial-recognition-with-artificial-intelligence/ (дата обращения: 19.11.2019).
5. Макаров В. Видеокамерам нужно улучшить «зрение». URL: http://static.mvd.ru/upload/site1/document_journal/M7o6MfghTi.pdf (дата обращения: 19.11.2019).
6. В Домодедово заработала система распознавания лиц. URL: https://hightech.plus/2019/07/05/v-domodedovo-zarabotala-sistema-raspoznavaniya-lic (дата обращения: 19.11.2019).
7. Тищенко Е.В., Саядова А.С. Технологические инновации в области профилактики преступности: тенденции и риски // Российский следователь. 2019. № 5. С. 62–66.
8. Найдутся все: какие стартапы в сфере распознавания лиц есть в России. URL: https://vc.ru/future/70147-naydutsya-vse-kakie-startapy-v-sfere-raspoznavaniya-lic-est-v-rossii (дата обращения: 19.11.2019).
9. Умные камеры в Москве помогли задержать более 100 человек. URL: https://hightech.plus/2019/06/27/umnie-kameri-v-moskve-pomogli-zaderzhat-bolee-100-chelovek (дата обращения: 19.11.2019).
10. На улицах Екатеринбурга апробируют систему по распознаванию лиц. URL: https://tagilcity.ru/news/society/06-08-2019/na-ulitsah-ekaterinburga-aprobiruyut-sistemu-po-raspoznavaniyu-lits?utm_source=yxnews&utm_medium=desktop&utm_referrer=https%3A%2F%2Fyandex.ru%2Fnews (дата обращения: 10.11.2019).
11. На ж/д вокзале Самары внедряется система цифрового распознавания лиц. URL: https://news.mail.ru/society/38732060/?frommail=1 (дата обращения: 10.11.2019).
12. Искусственный интеллект раскрыл убийство, взглянув на лицо жертвы. URL: https://hi-news.ru/technology/iskusstvennyj-intellekt-pomog-raskryt-ubijstvo-vzglyanuv-na-lico-zhertvy.html (дата обращения: 19.11.2019).
13. Кто и как использует технологии распознавания лиц в России. URL: https://rb.ru/longread/facial-recognition/ (дата обращения: 19.11.2019).
14. Распознавание лиц для бизнеса – обзор. URL: https://www.liveintellect.ru/tags/raspoznavanie_lic/ (дата обращения: 19.11.2019).
15. В китайской школе используют распознавание лиц для контроля за учениками. URL: https://rb.ru/story/chinese-schools/ (дата обращения: 19.11.2019).
16. Технология распознавания лиц: есть ли шанс обмануть искусственный интеллект? URL: https://futurerussia.gov.ru/nacionalnye-proekty/16564651646 (дата обращения: 19.11.2019).
17. Полиция Лондона «полностью довольна» системой распознавания лиц, которая ошибается в 98% случаях. URL: https://hightech.fm/2018/07/06/london (дата обращения: 19.11.2019).
18. Вежливая сеть: как научить искусственный интеллект относиться к людям непредвзято. URL: https://www.forbes.ru/tehnologii/360537-vezhlivaya-set-kak-nauchit-iskusstvennyy-intellekt-otnositsya-k-lyudyam (дата обращения: 19.11.2019).
19. Система распознавания лиц Amazon Rekognition приняла 28 конгрессменов США за преступников. URL: https://habr.com/ru/post/418509/ (дата обращения: 19.11.2019).
20. ИИ от Facebook позволяет обмануть системы распознавания лиц. URL: https://www.securitylab.ru/news/502092.php (дата обращения: 19.11.2019).

21. Польские дизайнеры создали украшение, которое не дает сработать технологии распознавания лиц. URL: https://birdinflight.com/ru/novosti/20190731-noma-against-face-recognition.html (дата обращения: 19.11.2019).
22. Исследователи из Бельгии обманули систему компьютерного зрения листком бумаги. URL: https://tjournal.ru/tech/95255-issledovateli-iz-belgii-obmanuli-sistemu-kompyuternogo-zreniya-listkom-bumagi (дата обращения: 19.11.2019).
23. Юдников А. Скрываться от камер – не самое лучшее решение: все, что вам нужно знать о распознавании лиц. URL: https://rb.ru/opinion/raspoznavanie-lic/ (дата обращения: 19.11.2019).
24. Кампания против распознавания лиц. URL: https://bancam.ru/ (дата обращения: 19.11.2019).
25. Апелляционный суд Англии изучит законность использования системы распознавания лиц. URL: http://rapsinews.ru/international_news/20191121/305078513.html (дата обращения: 21.11.2019).
26. Суд не признал систему распознавания лиц незаконной. Комментарий РосКомСвободы. URL: https://roskomsvoboda.org/51831/ (дата обращения: 19.11.2019).
27. В Калифорнии подписан закон о запрете использования распознавания лиц госорганами. URL: https://roskomsvoboda.org/51048/ (дата обращения: 19.11.2019).
28. Законодатели рассмотрят мораторий на использование распознавания лиц. URL: http://www.secnews.ru/digest/24020.htm#axzz65boZgQYI (дата обращения: 19.11.2019).
29. Законопроект ограничивает использование распознавания лиц коммерческими компаниями. URL: http://www.secnews.ru/ foreign/24065.htm#axzz65boZgQYI (дата обращения: 19.11.2019).
30. Поздняков В. Законность распознавания лиц с камер в общественных местах. URL: http://www.it-lex.ru/faq/zakonnost-raspoznavaniya-lic/ (дата обращения: 19.11.2019).
31. Разъяснения по вопросам отнесения фото-, видеоизображений, дактилоскопических данных и иной информации к биометрическим персональным данным и особенностей их обработки. URL: https://pd.rkn.gov.ru/press-service/subject1/news2729/ (дата обращения: 19.11.2019).
32. Виноградова Е. Искусственный интеллект: опасно для жизни? URL: https://kp.vedomosti.ru/humans/article/2019/05/13/801190-gore-ot-uma (дата обращения: 19.11.2019).
33. Европейская этическая хартия об использовании искусственного интеллекта в судебных системах и окружающих их реалиях. URL: https://rm.coe.int/ru-ethical-charter-en-version-17-12-2018-mdl-06092019-2-/16809860f4 (дата обращения: 19.11.2019).
34. Андреева О.И., Трубникова Т.В. Принятие судом решения о наличии в деянии лица злоупотребления правом и его последствия // Вестник Томского государственного университета. 2019. № 438. С. 194–200.
35. Андреева О.И., Григорьев В.Н., Зайцев О.А., Трубникова Т.В. Злоупотребление правом, его предупреждение и пресечение в уголовном процессе России: некоторые итоги исследования // Всероссийский криминологический журнал. 2018. Т. 12, № 6. С. 914–924.
36. Трубникова Т.В. Обеспечение права на справедливое судебное разбирательство и права потерпевшего на безопасность и тайну личной жизни: поиск баланса // Уголовная юстиция. 2017. № 2 (10). С. 81–88.
37. Постановление ЕСПЧ по делу «Big Brother Watch и другие против Соединенного Королевства» от 13.09. 2018 г. (жалобы № 58170/13, 62322/14 и 24960/15). URL: https://hudoc.echr.coe.int/rus#{%22fulltext%22:[%2258170/13%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22]} (дата обращения: 19.11.2019).
38. Harris, Charles E. et al. Engineering Ethics: Concepts and Cases. Belmont, CA : Wadsworth Publishing, 1995. P. 35.
39. Иванов В.В. Использование систем видеоконференцсвязи в современном уголовном процессе // Уголовное судопроизводство. 2011. № 3. С. 25–27.
40. Иванов В.В. Использование современных технологий в уголовном процессе: польза и риски // Уголовный процесс как средство обеспечения прав человека в правовом государстве : материалы Междунар. науч.-практ. конф. / ред. В.И. Самарин. 2017. С. 121–127.
41. Андреева О.И., Зайцев О.А. Проблемы использования в уголовном судопроизводстве электронных доказательств // Правовые проблемы укрепления российской государственности. Томск : Издательский Дом Том. гос. ун-та. 2018. Ч. 79. С. 4–16.

Статья представлена научной редакцией «Право» 25 ноября 2019 г.

Facial Recognition Technologies in Criminal Proceedings: Problems of Grounds for the Legal Regulation of Using Artificial Intelligence

Vestnik Tomskogo gosudarstvennogo universiteta – Tomsk State University Journal, 2019, 449, 201–212.
DOI: 10.17223/15617793/449/25

Olga I. Andreeva, Tomsk State University (Tomsk, Russian Federation). E-mail: andreevaoi_70@mail.ru
Viacheslav V. Ivanov, Samara National Research University (Samara, Russian Federation). E-mail: Ivanov_sl@rambler.ru
Aleksandr Yu. Nesterov, Samara National Research University (Samara, Russian Federation). E-mail: aynesterow@yandex.ru
Tatiana V. Trubnikova, Tomsk State University (Tomsk, Russian Federation). E-mail: trubn@mail.ru

Keywords: digitalisation in criminal proceedings; legal regulation of using artificial intelligence; ethics of artificial intelligence; technologies of facial recognition; third nature.

The study aims to determine requirements for the legal regulation of using technologies based on artificial intelligence in general and facial recognition in particular. To achieve the aim, the authors overviewed Russian and foreign experience in implementing video observation and facial recognition technologies in public life. The authors analysed the statutory regulation of the activity in different counties. The ethical and legal problems, arising when transferring to a new technological mode related to "digital revolution", are of a fundamental character. The moral-ethical problems, arising in society due to the wide spread of video observation and facial recognition technologies, and the need for a legal regulation of these technologies' use have no (with single exceptions) prominent national specificity. The legal and ethical gaps, which demand a reaction from the legal systems, are shown. This reaction "lags behind" the rapid development of technologies, the all new challenges and potential problems, which require appropriate solutions in the form of legal regulations with sufficient accuracy and clarity of expressions. Therefore, legislators of all countries have to act almost "randomly" when "patching the holes" in the legal regulation of the use of modern IT-technologies. The authors suggest three groups of grounds for the legal regulation of the use of facial recognition technologies: (1) defining the rules of interaction between artificial intelligence and human society; (2) determining the balance of public and private interests and limits of the state's action in the sphere of private interests, the state's obligations on the protection of citizens' rights to private life from the penetration of other private subjects into this sphere; (3) combining the legal regulation of the use of technologies based on artificial intelligence and the "self-control" of the professional community of the authors of these technologies, regulation of their behaviour with field-specific ethical codes. Based on the consideration of Russian and foreign practice of introducing video observation and facial recognition technologies, the authors suggest the possible forms of using these technologies in criminal proceedings in the

nearest future. The application of the grounds specified in the study to the features of criminal proceedings allowed the authors to propose several requirements to the legal regulation.

REFERENCES

1. Nesterov, A.Yu. (2017) *Semioticheskie osnovaniya tekhniki i tekhnicheskogo soznaniya* [The Semiotic Foundations of Technology and Technical Consciousness]. Samara: Samara Humanitarian Academy.
2. Ivanov, V.V. & Nesterov, A.Yu. (2019) [Law in an Artificial Environment of the Third Nature: The Legal Status of a Digital Double]. *Mir cheloveka: Normativnoe izmerenie – 6. Normy myshleniya, vospriyatiya, povedeniya: skhodstvo, razlichie, vzaimosvyaz'* [Human World: Normative Dimension–6. Norms of Thinking, Perception, Behaviour: Similarity, Difference, Relationship]. Proceedings of the International Conference. Saratov: Saratov State Academy of Law. pp. 234–240.
3. Meduza.io. (2018) *V Kitae sozdayut total'nuyu sistemu raspoznavaniya lits grazhdan. Ona pomozhet lovit' prestupnikov i sobirat' dannye na vsekh ostal'nykh* [In China, They Create a Total Recognition System for the Faces of Citizens. It Will Help Catch Criminals and Collect Data on Everyone Else]. [Online] Available from: https://meduza.io/feature/2018/02/11/v-kitae-sozdayut-totalnuyu-sistemu-raspoznavaniya-lits-grazhdan-ona-pomozhet-lovit-prestupnikov-i-sobirat-dannye-na-vseh-ostalnyh. (Accessed: 19.11.2019).
4. Amazon.com. (n.d.) *Fakty o raspoznavanii lits s pomoshch'yu iskusstvennogo intellekta* [Facts About Facial Recognition Using Artificial Intelligence]. [Online] Available from: https://aws.amazon.com/ru/rekognition/the-facts-on-facial-recognition-with-artificial-intelligence/. (Accessed: 19.11.2019).
5. Makarov, V. (2013) *Videokameram nuzhno uluchshit' "zrenie"* [Video Cameras Need to Improve "Vision"]. [Online] Available from: http://static.mvd.ru/upload/site1/document_journal/M7o6MfghTi.pdf. (Accessed: 19.11.2019).
6. Hightech.plus. (2019) *V Domodedovo zarabotala sistema raspoznavaniya lits* [Domodedovo Has Launched a Facial Recognition System]. [Online] Available from: https://hightech.plus/2019/07/05/v-domodedovo-zarabotala-sistema-raspo znavaniya-lic. (Accessed: 19.11.2019).
7. Tishchenko, E.V. & Sayadova, A.S. (2019) Technological Innovations in Crime Prevention: Tendencies and Risks. *Rossiyskiy sledovatel' – Russian Investigator*. 5. pp. 62–66. (In Russian).
8. Vc.ru. (2019) *Naydutsya vse: kakie startapy v sfere raspoznavaniya lits est' v Rossii* [There Is Everything: Startups in the Field of Facial Recognition in Russia]. [Online] Available from: https://vc.ru/future/70147-naydutsya-vse-kakie-startapy-v-sfere-raspoznavaniya-lic-est-v-rossii. (Accessed: 19.11.2019).
9. Hightech.plus. (2019) *Umnye kamery v Moskve pomogli zaderzhat' bolee 100 chelovek* [Smart Cameras in Moscow Helped Detain More Than 100 People]. [Online] Available from: https://hightech.plus/2019/06/27/umnie-kameri-v-moskve-pomogli-zaderzhat-bolee-100-chelovek. (Accessed: 19.11.2019).
10. Tagilcity.ru. (2019) *Na ulitsakh Ekaterinburga aprobiruyut sistemu po raspoznavaniyu lits* [In the Streets of Yekaterinburg, a Facial Recognition System Is Being Tested]. [Online] Available from: https://tagilcity.ru/news/society/06-08-2019/na-ulitsah-ekaterinburga-aprobiruyut-sistemu-po-raspoznavaniyu-lits?utm_source=yxnews&utm_medium=desktop&utm_referrer=https%3A%2F%2Fyandex.ru%2Fnews. (Accessed: 10.11.2019).
11. News.mail.ru. (2019) *Na zh/d vokzale Samary vnedryaetsya sistema tsifrovogo raspoznavaniya lits* [At the Samara Railway Station, a Digital Facial Recognition System Is Being Introduced]. [Online] Available from: https://news.mail.ru/society/38732060/?frommail=1. (Accessed: 10.11.2019).
12. Hi-news.ru. (2019) *Iskusstvennyy intellekt raskryl ubiystvo, vzglyanuv na litso zhertvy* [Artificial Intelligence Uncovered the Killing by Looking at the Victim's Face]. [Online] Available from: https://hi-news.ru/technology/iskusstvennyj-intellekt-pomog-raskryt-ubijstvo-vzglyanuv-na-lico-zhertvy.html. (Accessed: 19.11.2019).
13. Rb.ru. (2019) *Kto i kak ispol'zuet tekhnologii raspoznavaniya lits v Rossii* [Who Uses Facial Recognition Technology in Russia, and How]. [Online] Available from: https://rb.ru/longread/facial-recognition/. (Accessed: 19.11.2019).
14. Liveintellect.ru. (2019) *Raspoznavanie lits dlya biznesa – obzor* [Facial Recognition for Business: An Overview]. [Online] Available from: https://www.liveintellect.ru/tags/raspoznavanie_lic/. (Accessed: 19.11.2019).
15. Rb.ru. (2019) *V kitayskoy shkole ispol'zuyut raspoznavanie lits dlya kontrolya za uchenikami* [A Chinese School Uses Facial Recognition to Control Students]. [Online] Available from: https://rb.ru/story/chinese-schools/. (Accessed: 19.11.2019).
16. Futurerussia.gov.ru. (2019) *Tekhnologiya raspoznavaniya lits: est' li shans obmanut' iskusstvennyy intellekt?* [Facial Recognition Technology: Is There a Chance to Deceive Artificial Intelligence?]. [Online] Available from: https://futurerussia.gov.ru/nacionalnye-proekty/16564651646. (Accessed: 19.11.2019).
17. Hightech.fm. (2018) *Politsiya Londona "polnost'yu dovol'na" sistemoy raspoznavaniya lits, kotoraya oshibaetsya v 98% sluchayakh* [The London Police Are "Completely Satisfied" with the Facial Recognition System, Which Makes Mistakes in 98% of Cases]. [Online] Available from: https://hightech.fm/2018/07/06/london. (Accessed: 19.11.2019).
18. Forbes.ru. (2018) *Vezhlivaya set': kak nauchit' iskusstvennyy intellekt otnosit'sya k lyudyam nepredvzyato* [Polite Network: How to Teach Artificial Intelligence to Treat People Unbiasedly]. [Online] Available from: https://www.forbes.ru/tehnologii/360537-vezhlivaya-set-kak-nauchit-iskusstvennyy-intellekt-otnositsya-k-lyudyam. (Accessed: 19.11.2019).
19. Habr.com. (2018) *Sistema raspoznavaniya lits Amazon Rekognition prinyala 28 kongressmenov SShA za prestupnikov* [Amazon Recognition Facial Recognition System Has Taken 28 US Congressmen for Criminals]. [Online] Available from: https://habr.com/ru/post/418509/. (Accessed: 19.11.2019).
20. Securitylab.ru. (2019) *II ot Facebook pozvolyaet obmanut' sistemy raspoznavaniya lits* [Facebook AI allows cheating facial recognition systems]. [Online] Available from: https://www.securitylab.ru/news/502092.php. (Accessed: 19.11.2019).
21. Birdinflight.com. (2019) *Pol'skie dizaynery sozdali ukrashenie, kotoroe ne daet srabotat' tekhnologii raspoznavaniya lits* [Polish Designers Have Created a Jewelry That Blocks Facial Recognition Technology]. [Online] Available from: https://birdinflight.com/ru/novosti/20190731-noma-against-face-recognition.html. (Accessed: 19.11.2019).
22. Tjournal.ru. (2019) *Issledovateli iz Bel'gii obmanuli sistemu komp'yuternogo zreniya listkom bumagi* [Researchers from Belgium Tricked a Computer Vision System with a Piece of Paper]. [Online] Available from: https://tjournal.ru/tech/95255-issledovateli-iz-belgii-obmanuli-sistemu-kompyuternogo-zreniya-listkom-bumagi. (Accessed: 19.11.2019).
23. Yudnikov, A. (2019) *Skryvat'sya ot kamer – ne samoe luchshee reshenie: vse, chto vam nuzhno znat' o raspoznavanii lits* [Hiding from Cameras Is Not the Best Solution: Everything You Need to Know About Facial Recognition]. [Online] Available from: https://rb.ru/opinion/raspoznavanie-lic/. (Accessed: 19.11.2019).
24. *Campaign Against Facial Recognition*. [Online] Available from: https://bancam.ru/. (Accessed: 19.11.2019). (In Russian).
25. Rapsinews.ru. (2019) *Apellyatsionnyy sud Anglii izuchit zakonnost' ispol'zovaniya sistemy raspoznavaniya lits* [The Court of Appeal of England Will Examine the Legality of Using a Facial Recognition System]. [Online] Available from: http://rapsinews.ru/international_news/20191121/305078513.html. (Accessed: 21.11.2019).
26. Roskomsvoboda.org. (2019) *Sud ne priznal sistemu raspoznavaniya lits nezakonnoy. Kommentariy RosKomSvobody* [The Court Did Not Find the Facial Recognition System Illegal. Comment by Roskomsvoboda]. [Online] Available from: https://roskomsvoboda.org/51831/. (Accessed: 19.11.2019).

27. Roskomsvoboda.org. (2019) *V Kalifornii podpisan zakon o zaprete ispol'zovaniya raspoznavaniya lits gosorganami* [In California, a Law Has Been Signed Banning the Use of Face Recognition by Government Agencies]. [Online] Available from: https://roskomsvoboda.org/51048/. (Accessed: 19.11.2019).
28. Secnews.ru. (2019) *Zakonodateli rassmotryat moratoriy na ispol'zovanie raspoznavaniya lits* [Lawmakers Will Consider a Moratorium on the Use of Facial Recognition]. [Online] Available from: http://www.secnews.ru/digest/24020.htm#axzz65boZgQYI. (Accessed: 19.11.2019).
29. Secnews.ru. (2019) *Zakonoproekt ogranichivaet ispol'zovanie raspoznavaniya lits kommercheskimi kompaniyami* [The Bill Restricts the Use of Facial Recognition to Commercial Companies]. [Online] Available from: http://www.secnews.ru/foreign/24065.htm#axzz65boZgQYI. (Accessed: 19.11.2019).
30. Pozdnyakov, V. (n.d.) *Zakonnost' raspoznavaniya lits s kamer v obshchestvennykh mestakh* [Legality of Facial Recognition from Cameras in Public Places]. [Online] Available from: http://www.it-lex.ru/faq/zakonnost-raspoznavaniya-lic/. (Accessed: 19.11.2019).
31. Pd.rkn.gov.ru. (2013) *Raz"yasneniya po voprosam otneseniya foto-, videoizobrazheniy, daktiloskopicheskikh dannykh i inoy informatsii k biometricheskim personal'nym dannym i osobennostey ikh obrabotki* [Clarifications Regarding the Assignment of Photo, Video, Fingerprint Data and Other Information to Biometric Personal Data and the Features of Their Processing]. [Online] Available from: https://pd.rkn.gov.ru/press-service/subject1/news2729/. (Accessed: 19.11.2019).
32. Vinogradova, E. (2019) *Iskusstvennyy intellekt: opasno dlya zhizni?* [Artificial Intelligence: Life Threatening?]. [Online] Available from: https://kp.vedomosti.ru/humans/article/2019/05/13/801190-gore-ot-uma. (Accessed: 19.11.2019).
33. Rm.coe.int. (2018) *Evropeyskaya eticheskaya khartiya ob ispol'zovanii iskusstvennogo intellekta v sudebnykh sistemakh i okruzhayushchikh ikh realiyakh* [Uropean Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment]. [Online] Available from: https://rm.coe.int/ru-ethical-charter-en-version-17-12-2018-mdl-06092019-2-/16809860f4. (Accessed: 19.11.2019).
34. Andreeva, O.I. & Trubnikova, T.V. (2019) A Court's Decision on the Presence of Abuse of Right in the Act of a Person and Its Consequences. *Vestnik Tomskogo gosudarstvennogo universiteta – Tomsk State University Journal*. 438. pp. 194–200. (In Russian). DOI: 10.17223/15617793/438/26
35. Andreeva, O.I. et al. (2018) Abuse of Rights, Its Prevention and Suppression in Russian Criminal Process: Some Research Results. *Vserossiyskiy kriminologicheskiy zhurnal – Russian Journal of Criminology*. 12 (6). pp. 914–924. (In Russian). DOI: 10.17150/2500-4255.2018.12(6).914-924
36. Trubnikova, T.V. (2017) Enforcement of the Right to Fair Trial and the Right of the Victim to Security and Privacy: Search for Balance. *Ugolovnaya yustitsiya – Russian Journal of Criminal Law*. 2 (10). pp. 81–88. (In Russian). DOI: 10.17223/23088451/10/14
37. ECHR. (2018) *Postanovlenie ESPCh po delu "Big Brother Watch i drugie protiv Soedinennogo Korolevstva" ot 13.09. 2018 g. (zhaloby № 58170/13, 62322/14 i 24960/15)* [ECHR Judgment in Case of Big Brother Watch and Others v. the United Kingdom of 13 September 2018 (Applications No. 58170/13, 62322/14 and 24960/15)]. [Online] Available from: https://hudoc.echr.coe.int/rus#{%22fulltext%22:[%2258170/13%22],%22documentcollectionid2% 22:[%22GRANDCHAMBER%22,%22CHAMBER%22]}. (Accessed: 19.11.2019).
38. Harris, Ch.E. et al. (1995) *Engineering Ethics: Concepts and Cases*. Belmont, CA: Wadsworth Publishing.
39. Ivanov, V.V. (2011) Ispol'zovanie sistem videokonferentssvyazi v sovremennom ugolovnom protsesse [The Use of Video Conferencing Systems in the Modern Criminal Procedure]. *Ugolovnoe sudoproizvodstvo*. 3. pp. 25–27.
40. Ivanov, V.V. (2017) [The Use of Modern Technology in the Criminal Procedure: Benefits and Risks]. *Ugolovnyy protsess kak sredstvo obespecheniya prav cheloveka v pravovom gosudarstve* [The Criminal Procedure as a Means of Ensuring Human Rights in the Rule of Law]. Proceedings of the International Conference. Minsk: Belarussian State University. pp. 121–127. (In Russian).
41. Andreeva, O.I. & Zaytsev, O.A. (2018) Problemy ispol'zovaniya v ugolovnom sudoproizvodstve elektronnykh dokazatel'stv [Problems of Using Electronic Evidence in Criminal Proceedings]. In: Andreeva, O.I. & Trubnikova, T.V. (eds) *Pravovye problemy ukrepleniya rossiyskoy gosudarstvennosti* [Legal Problems of Strengthening Russian Statehood]. Is. 79. Tomsk: Tomsk State University. pp. 4–16.

Received: 25 November 2019