

Научная статья

УДК 347.121.2

DOI 10.25205/2542-0410-2023-19-3-47-56

Проблемы защиты персональных данных в условиях цифровой трансформации

Яна Александровна Карунная

Новосибирский государственный университет

Новосибирск, Россия

advokat2631@bk.ru

Аннотация

В статье представлен анализ отечественного законодательства, регламентирующего защиту персональных данных; рассмотрены проблемы защиты персональных данных в условиях усиления роли цифровых ресурсов, использования технологии трекинга и цифровых технологий, позволяющих фиксировать, осуществлять сбор и обрабатывать персональные данные физических лиц; аргументирована необходимость разрабатывать современные эффективные методы, технические средства обнаружения и предотвращения несанкционированного использования персональных данных, а также потребность в обсуждении и последующей корректировке дополнительной правовой регламентации института защиты персональных данных, в частности, отдельных положений закона.

Ключевые слова

цифровые технологии, искусственный интеллект, системы видеонаблюдения, персональные данные, биометрические данные, big data

Для цитирования

Карунная Я. А. Проблемы защиты персональных данных в условиях цифровой трансформации // Юридическая наука и практика. 2023. Т. 19, № 3. С. 47–56. DOI 10.25205/2542-0410-2023-19-3-47-56

Problems of Personal Data Protection in the Context of Digital Transformation

Yana A. Karunnaya

Novosibirsk State University,

Novosibirsk, Russia

advokat2631@bk.ru

Abstract

The article presents an analysis of domestic legislation regulating the protection of personal data; the problems of personal data protection in the context of increasing the role of digital resources, the use of tracking technology and digital technologies that allow recording, collecting and processing personal data of individuals are considered; the argumentation is given to substantiate the need to develop modern effective methods, technical means of detecting and preventing unauthorized use of personal data, additional legal regulation of the institute of personal data protection, and certain provisions of the law – in discussion and subsequent correction.

Keywords

Digital technologies, artificial intelligence, video surveillance systems, personal data, biometric data, Big data

© Карунная Я. А., 2023

For citation

Karunnaya Ya. A. Problems of personal data protection in the context of digital transformation. *Juridical Science and Practice*, 2023, vol. 19, no. 3, pp. 47–56. (in Russ.) DOI 10.25205/2542- 0410-2023-19-3-47-56

Резкое ускорение трансформирующих изменений в сфере информатики и цифровых технологий предопределило вектор развития общественных отношений в условиях цифровизации. Цифровая трансформация – одна из целей развития Российской Федерации до 2030 г., в соответствии с которой ориентир направлен на следующие целевые показатели: достижение «цифровой зрелости» ключевых отраслей экономики и социальной сферы, в том числе здравоохранения и образования, а также государственного управления; увеличение доли массовых социально значимых услуг, доступных в электронном виде, до 95 %; рост доли домохозяйств, которым обеспечена возможность широкополосного доступа к информационно-телекоммуникационной сети «Интернет», до 97 %; увеличение вложений в отечественные решения в сфере информационных технологий в четыре раза по сравнению с показателем 2019 г.¹ В соответствии со Стратегией цифровой трансформации, в регионах, в том числе в Новосибирской области, для обеспечения государственного управления, развития экономики и социальной сферы внедряются следующие технологии: «нейротехнологии и искусственный интеллект; технологии беспроводной связи и промышленный интернет вещей IoT; новые производственные технологии, в том числе технология «цифровой двойник»; системы распределенного реестра; технологии виртуальной и дополненной реальности»². Цифровая трансформация повлекла за собой масштабное использование персональных данных, в связи с чем для проведения комплекса значимых реформ в Российской Федерации особое значение приобретают вопросы разработки эффективного правового регулирования отношений для защиты данных, составляющих персональную информацию граждан. Отечественное законодательство в результате его реформирования совершенствуется. Тем не менее следует констатировать, что практика использования современных технологий, в том числе доступа к информации посредством онлайн-сервисов, распространяется более быстрыми темпами, в сравнении с разработкой комплекса технических средств и положений, направленных на обеспечение механизма, с помощью которого можно было максимально надежно обеспечить защиту персональных данных и предотвратить несанкционированное вторжение в сферу личной жизни граждан.

Актуальными представляются вопросы защиты личных данных в условиях повсеместного применения технологии трекинга, цифровых технологий, используемых для машинного обучения и хранения больших объемов информации (big data).

Для целей настоящего исследования под использованием технологии трекинга понимается практика размещения видеокамер наблюдения – начиная от их размещения в домофонах многоквартирного дома, при входе и внутри помещений сферы обслуживания, образовательных, медицинских и иных учреждений, местах парковки, светофорах, вдоль дорог и др., заканчивая камерами в аэропортах и вокзалах. Современные системы наблюдения позволяют отследить передвижения практически каждого человека. По данным TelecomDaily, Россия занимает второе место по темпу роста видеонаблюдения за гражданами, число видеокамер в общественных местах за год выросло на 10 %. В первой половине 2021 г. число камер, установленных

¹ О национальных целях развития Российской Федерации на период до 2030 года: Указ Президента Российской Федерации от 21.07.2020 № 474 // Собрание законодательства Рос. Федерации. 2018. № 20. Ст. 2817; № 30. Ст. 4717.

² Стратегия цифровой трансформации ключевых отраслей экономики, социальной сферы и государственного управления Новосибирской области, утв. постановлением губернатора от 31.08.22 №161 // Официальный интернет-портал правовой информации Новосибирской области: <https://pravo.nso.ru> (дата обращения: 05.06.2023).

в парках, на улицах, вокзалах, магазинах, превысило 15 млн штук. По количеству работающей техники видеонаблюдения РФ уже на третьем месте после Китая, где на октябрь 2021 г. работают 200 млн видеокамер³. В настоящее время в России реализуются мероприятия по массовому производству IP-камер видеонаблюдения в соответствии планом, предусмотренным дорожной картой развития высокотехнологичного направления (области) «Новое промышленное программное обеспечение» на период до 2030 г.⁴ При этом в результате расширения технических возможностей систем видеонаблюдения появилась возможность распознавать и идентифицировать лица, в том числе в плотном потоке людей. Такие системы применяются для фейсконтроля в различных заведениях, в целях распознавания отдельных лиц при организации системы управления доступом. С помощью IP-камеры возможно определить нахождение на территории объекта посторонних лиц, информация о которых отсутствует в базе, произвести зональное сканирование в целях поиска и опознания системой лица, занесенного в базу для допуска на объект. Распознавание осуществляется благодаря функции выбранного алгоритма, в соответствии с которым полученное отсканированное изображение лица «гостя» сравнивается с эталонными картинками, которые уже имеются в базе. Технология, используемая в IP-камере, используется для анализа потока и передачи на сервер уже обработанных данных, в соответствии с которыми определяются условия доступа на объект – доступ становится возможным или невозможным.

В условиях цифровой трансформации распространение практики использования систем видеонаблюдения неизбежно. Благодаря поддержанию систем видеонаблюдения обеспечивается общественный порядок, оперативное раскрытие правонарушений, допуск в определенные помещения лиц, имеющих разрешение на это, соблюдение правил дорожного движения, предотвращение дорожно-транспортных происшествий и др. Кроме того, записи с камер наблюдения могут иметь доказательственное значение по уголовным и гражданским делам, при установлении обстоятельств совершения административного правонарушения. Вместе с тем практика использования систем видеонаблюдения обнаруживает и некоторые проблемы, необходимость в разрешении которых настоятельна как с позиции теории, так и правоприменения. Ключевая проблема заключается в возможности накапливать (записывать) информацию, содержащую персональные данные о конкретном лице, в том числе сведения, составляющие медицинскую, адвокатскую, банковскую или иную тайну.

В соответствии со ст. 24 Конституции РФ, сбор, хранение, использование и распространение информации о частной жизни человека без его согласия не допускаются. Согласно ст. 3 Федерального закона «О персональных данных» (далее – Закон о персональных данных), персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных). К такой информации Закон относит и биометрические данные, т. е. 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 данных⁵.

³ Видеонаблюдение (рынок_России). URL: <https://www.tadviser.ru/index.php/> (дата обращения: 10.06.2023).

⁴ Распоряжение Правительства Российской Федерации от 28 декабря 2022 г. № 4263-р // Собрание законодательства Рос. Федерации. 2023. № 1 (ч. III). Ст. 424.

⁵ О персональных данных: Федеральный закон от 27 июля 2006 г. № 152-ФЗ (ред. от 06.02.2023) // Собрание законодательства Рос. Федерации. 31 июля 2006 г. № 31 (часть I). Ст. 3451; Об определении состава сведений, размещаемых в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица, включая вид биометрических персональных данных, а также о внесении

В ст. 152.1 ГК РФ закреплено положение, в силу которого обнародование и дальнейшее использование изображения гражданина (в том числе его фотографии, а также видеозаписи или произведения изобразительного искусства, в которых он изображен) допускаются только с согласия этого гражданина. Такое согласие не требуется в случаях, когда: использование изображения осуществляется в государственных, общественных или иных публичных интересах; изображение гражданина получено при съемке, которая проводится в местах, открытых для свободного посещения, или на публичных мероприятиях (собраниях, съездах, конференциях, концертах, представлениях, спортивных соревнованиях и подобных мероприятиях), за исключением случаев, когда такое изображение является основным объектом использования; гражданин позировал за плату. Анализ положений, закрепленных в п. 1 ст. 22 и ч. 2 ст. 11 Закона о персональных данных, показывает, что все сведения, на основании которых может быть выполнена идентификация личности, приравниваются к персональным; биометрические данные могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных. В ст. 7 указанного Закона закреплена обязанность операторов и иных лиц, получивших доступ к персональным данным, не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных.

Важно признать, что современные системы видеонаблюдения фиксируют именно биометрические персональные данные, т. е. физиологические и биологические особенности человека, на основании которых можно установить его личность. Однако, по смыслу Закона, само по себе видеонаблюдение в общественных местах не является сбором персональных данных, в связи с чем не требует согласия субъекта персональных данных, за исключением случаев передачи записи третьим лицам или использования ее в целях установления личности человека. Таким образом, если камеры установлены для идентификации конкретного лица, например, для того чтобы он был идентифицирован через систему лояльности, то для осуществления такой записи необходимо получить согласие субъекта о персональных данных. Напротив, если речь идет об использовании систем видеонаблюдения с целью контроля обстановки, то такое использование не подпадает под действие приведенных правовых положений, так как в данном случае имеет место мониторинг ситуации с помощью камер, а не идентификация субъекта по видеозаписи на основании его биометрических данных. При регистрации правонарушений с помощью задействования функции видеонаблюдения установление правонарушителя может проводиться в порядке, который регламентируется процессуальным законодательством. Однако в практике имеется немало примеров, когда вопрос о границах полномочий лиц, осуществляющих проверочные мероприятия (расследование), был предметом отдельного рассмотрения. Проблема обнаруживается в случае бесконтрольного получения записей с камер видеонаблюдения и не во всех случаях для оценки их доказательственного значения, но для получения информации о конкретном лице. При этом для получения записи с камер видеонаблюдения разрешения суда не требуется. Чрезмерная экстенсивная слежка за гражданами без каких-либо ограничений (подтверждений) того, зачем ведется наблюдение, как долго оно может продолжаться, а главное – какова в дальнейшем должна быть судьба собранных материалов, несет риски утечки персональной информации и, как следствие, возникновения неблагоприятных последствий для субъекта персональных данных. Представляется, что наблюдение, в том числе использование записи, допустимо и необходимо в демократическом обществе, однако его пределы должны быть четко установлены законом, с тем чтобы защитить право граждан на неприкосновенность частной жизни. Полученные доказательства должны быть надлежащим образом задокументированы, а затем, после минования надобности, уничтожены. Принимая во внимание заметный рост киберпреступлений, риск несанкционированного использования информации, содержащей персональные данные, достаточно велик.

изменений в некоторые акты Правительства Российской Федерации: Постановление Правительства РФ от 30.06.2018 № 772 (ред. от 12.07.2022) // Собрание законодательства РФ. 2018. № 28. Ст. 4234.

Гарантий, что персональная информация, равно как сведения о личной жизни, не будет не-санкционированно использована, – нет. К тому же изначально информация может быть получена на законных основаниях. Вместе с тем при предоставлении информации с камер видеонаблюдения, как правило, не всегда возможно вычленить сведения относительно конкретного лица. Зачастую в объектив камеры по воле случая попадают и другие лица, не являющиеся фигурантами, т. е. лицами, в отношении которых оперативных, следственных и иных мероприятий не проводится. Такие «случайные» лица могут не догадываться о том, что информация о них, например, наличествует в материалах уголовного, административного или гражданского дела, могут не знать о том, что их персональные данные фигурируют в материалах служебной проверки (служебного расследования), но при этом доступ к этим материалам может иметь не только гражданин, в отношении которого проводилась проверка (расследование), обвиняемый и его защитник, но и потерпевший, стороны по делу и иные лица, участвующие в деле (их представители), эксперт и др. Например, распространена практика, когда для подтверждения информации о передвижения конкретного гражданина, в отношении которого проводятся проверочные мероприятия (расследование), запрашивается запись с камер видеонаблюдения, фиксирующих обстоятельства его нахождения в конкретном месте, участия в каких-либо мероприятиях, где одновременно могут находиться его друзья, родственники или иные лица, в отношении которых указанные мероприятия не проводятся. Запись с камеры видеонаблюдения может зафиксировать факты обращения гражданина за медицинской или правовой помощью. Информация, зафиксированная камерами видеонаблюдения, установленными в местах общего пользования, предоставляется собственникам многоквартирного дома для установления каких-либо обстоятельств. Например, есть практика, когда для установления лиц, причастных к порче общедомового имущества, просматриваются записи, фиксирующие отдельных лиц, не причастных к устанавливаемым обстоятельствам. При таких обстоятельствах основания считать, что информация о передвижениях, встречах, знакомствах, отношениях и др. может стать известной третьим лицам или окажется составной частью досье на человека, довольно весомые. При этом установить лицо, распространившее такие сведения или их накапливающее, сложно. Кроме того, работоспособность систем видеонаблюдения, как правило, поддерживается коммерческими организациями, репутация которых в обеспечении защиты сведений, составляющих персональные данные, небезупречна.

Приведенные обстоятельства указывают на то, что нормативные положения, включая норму ст. 7 Закона о персональных данных, носят скорее дискретный характер и не обеспечивают должный уровень защищенности.

Следующая важная проблема – обеспечение механизма защиты данных в процессе их сбора и обработки с использованием цифровых технологий и для усовершенствования цифровых технологий, в том числе для обучения искусственного интеллекта. Например, с целью выполнения задачи распознавания физического лица обрабатывается большой массив информации, в том числе той, которая содержит персональные данные. В частности, в целях машинного обучения исследуются и анализируются параметры готовых образов и на основании полученных данных с помощью технологии искусственного интеллекта становится возможным определить пол, возраст, индивидуальные особенности человека. Сфера использования таких технологий обширна. Видеокамеры могут быть установлены в рекламных баннерах, и тот, кто знакомится с рекламной информацией, не знает, что его изображение может быть зафиксировано и использовано для определения, к примеру, круга потребителей, заинтересовавшихся рекламной информацией. С. М. Пястолов определяет целевую рекламу как прием, который «увеличивает вероятность покупки или определенных действий потребителя. Чтобы добиться этого, компании собирают данные о поведении своих потребителей или покупают кейсы и применяют методы машинного обучения, чтобы прогнозировать модели будущего потребительского поведения» [1, с. 87]. С помощью нейронных сетей возможно получить качественное распознавание отдельных лиц при минимальных временных затратах. Многослойное сканирование лица позво-

ляет определить соответствие полученного изображения с тем, которое имеется в базе данных. Однако для статистического сравнения полученных изображений с теми эталонами, которые внесены в базу, необходимо машинное обучение, в результате которого система способна учесть антропометрические точки, наиболее ярко характеризующие человека, в том числе высоту и ширину лба, линию положения глазной щели, ширину спинки носа, высоту верхней губы, ушной раковины и др. Таким образом, с помощью «умной системы», в том числе для ее совершенствования, сканируются и обрабатываются изображения разных лиц, которые даже не подозревают, что их биометрические данные могут использоваться и храниться. Более того, технологический процесс обуславливает необходимость пополнения базы новыми эталонами и образцами для их статистики, сравнения и исследования для более точного определения биометрических параметров. Разработка систем распознавания лиц в настоящее время востребована, следовательно, со временем будет только совершенствоваться. Так, в онлайн-презентации новой версии Macroscop 4.1 демонстрируются возможности модуля распознавания лиц, которые обеспечивают высокую точность распознавания лиц. Заявляется, что важным применением модуля может быть автоматическая идентификация гостей отеля, клиентов ресторана, а также посетителей других подобных предприятий. При этом указывается, что для работы с модулем необходимо загрузить базу данных лиц или добавить лица из видеоархива в ПО Macroscop. База данных лиц может содержать фотографии или скриншоты с лицами людей. К изображениям можно добавлять имена, фамилии и любые комментарии, а также добавлять фотографии в такие списки, как VIP-клиенты, нежелательные посетители и др. В качестве эталонного изображения используется цифровое изображение, предварительно загруженное в базу данных лиц модуля, или изображение, снятое камерой системы на контрольно-пропускном пункте, оборудованном системой видеонаблюдения. При работе с видеоархивом можно фильтровать все события по фотографии человека. Таким образом, возможно найти все события, произошедшие с конкретным человеком, а также увидеть, где находился этот человек и что он делал⁶.

Венчурная студия Synesis, работающая над проектами в области умных городов, ПО для организации мероприятий, мессенджеров и онлайн-казино, заявляет о разработке Kipod, которая помогает всем – от правоохранительных органов, государственных и общественных организаций безопасности до частных служб безопасности и коммерческих структур – извлекать выгоду из больших массивов видеоданных. Уникальная облачная платформа обеспечивает мгновенный поиск видеоконтента и непрерывный мониторинг событий по миллионам камер, обслуживая при этом миллионы пользователей на любом устройстве. Задействование искусственного интеллекта дает следующие возможности: идентификация личности, обнаружение внештатных ситуаций, аудиоаналитика, идентификация автомобилей, межкамерное слежение, классификация объектов big data, глобальный поиск по тысячам мест, фасетные фильтры, неограниченные списки поиска людей и транспортных средств. Kipod производит практически в режиме момента поиск в огромном количестве данных. Задействованные алгоритмы позволяют идентифицировать конкретного человека. В результате возможно определить местонахождение человека и время его нахождения в определенном месте. С помощью заявленных функций обнаружение человека возможно также и без его фотографии при имеющихся других данных, таких как пол, раса, возраст и др. С помощью технологии Big Data API можно наблюдать общую картину того, что происходит в городе, посчитать людей и транспортные средства, используя стандартные камеры видеонаблюдения, заявляется на сайте компании⁷.

Умное видеонаблюдение с применением технологии распознавания лиц планомерно интегрируется практически во все города. На основе биометрических данных граждан создаются

⁶ Онлайн-презентация новой версии Macroscop 4.1 «Распознавание лиц Light». URL: <https://macroscop.com/produkty/programma-dlya-ip-kamer/raspoznavanie-lic> (дата обращения: 05.07.2023).

⁷ Интернет-сайт kipod.com // URL: <https://kipod.com/ru/features> (дата обращения: 08.07.2023).

базы фотографий лиц со статусами «доверенное» и «черный список». Без специальных исследований и обучения искусственного интеллекта на основе конкретных изображений это было невозможно. По общему правилу, закрепленному в ч. 3 ст. 18 Закона о персональных данных, если персональные данные получены не от субъекта персональных данных, оператор до начала обработки таких персональных данных обязан предоставить субъекту персональных данных информацию относительно наименования либо фамилии, имени, отчества и адреса оператора или его представителя; цели обработки персональных данных и ее правового основания; перечня персональных данных; предполагаемых пользователей персональных данных; источника получения персональных данных. Однако, в силу ч. 4 приведенной нормы, оператор освобождается от обязанности предоставить субъекту персональных данных перечисленную информацию, если осуществляет обработку персональных данных для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта персональных данных. При таком нормативном исключении возникает вопрос о правомерности использования персональных данных в процессе проведения различного рода исследований для обучения искусственного интеллекта, равно как и объеме самих исследований, а также пределах использования полученных результатов.

Таким образом, следует констатировать, что цифровая трансформация повлекла за собой масштабное использование персональных данных, которые стали одной из составляющих big data. Рассматривая в ретроспективе замысел big data, можно проследить определенный процесс его эволюции. В литературе отмечается, что «в начале 2000-х годов он стал определяться как модель 3V: объем (volume), скорость (velocity) и вариативность (variety). Эта модель эволюционировала, приспосабливаясь к новой цифровой реальности, и превратилась в модель 4V: был добавлен такой параметр, как ценность (value) – процесс извлечения ценной информации из набора данных, известный как «аналитика больших данных». В настоящее время большие данные чаще определяют уже в терминах модели 5V, в которую добавлен параметр достоверности (veracity), означающий адекватное управление данными и соблюдение права на частную жизнь» [2, с. 53]. Поскольку «в сущности, понятие Big Data подразумевает работу с информацией огромного объема и разнообразного состава, которая часто обновляется и может располагаться в различных информационных источниках» [3, с. 320], вопрос относительно целей использования аккумулируемой информации лицами, владеющими ею, оказывается непростым. М. О. Лихачев справедливо акцентирует внимание на том, «сбор данных «ведет к тотальной «датафикации»: наблюдению и сбору данных о происходящих процессах, поведении людей и взаимосвязях, возникающих между ними. Практически любая активность в Интернете в настоящее время – это основа для формирования баз данных, которые не просто являются информацией, отражающей реальный мир, а используются для того, чтобы воздействовать на него, изменять его в интересах тех, кто владеет этой информацией» [4, с. 73].

Совершенствование технологий, позволяющих собирать различные данные и предоставляющие возможность персонифицировать людей с использованием биометрических данных, индивидуальных особенностей, деятельности и т. д., влечет за собой серьезные риски утечки информации, составляющей персональные сведения. При этом возможность трансграничной передачи таких сведений, а также наличие инновационных разработок, предлагающих сходные решения, но контролируемые разными разработчиками и компаниями, затрудняет установление лиц, ответственных за утечку персональных данных либо делает это невозможным. Как показывает практика, предупредительные меры оказываются недейственными. Так, по мнению экспертов InfoWatch, «в России за год утекло более 667 млн записей с персональными данными – это в 4,5 раза больше населения страны... По подсчетам Group-IB, количество утекших записей в прошлом году в десять раз превысило население России: строчки включают имена клиентов, их телефоны, адреса, даты рождения, а в некоторых можно найти хеш-пароли, паспортные данные, подробности заказов и другую чувствительную информа-

цию. Общее количество строк данных пользователей в утечках в 2022 году составило 1,4 млрд, для сравнения: в 2021 году их насчитывалось всего 33 млн»⁸. Отток информации имел место в самых различных сферах: финансовой, энергетической, промышленной, строительной, транспортной, развлекательной, образовательной, страховой, IT-компаний, сервиса доставки, онлайн-обслуживания и др.⁹

По мнению В. К. Шайдулиной, «В настоящее время, когда сбор информации о пользователях обладает массовым характером, даже самый безобидный фрагмент подобных сведений, будучи соединенным с другим, способен дать гораздо больше данных о человеке, чем его анкета. Значительные массивы сведений о пользователях, циркулирующие в цифровой форме, привели к возникновению за рубежом новых игроков на информационном рынке. В частности, появились информационные брокеры, которые на основе стекающихся к ним из разных интернет-сервисов данных, составляют детальные профайлы людей и предоставляют к ним доступ заинтересованным субъектам» [5, с. 4].

Несмотря на определенную нормативную обеспеченность защиты персональных данных, в современной действительности именно потребитель (пользователь приложения) при оказании услуги или приобретении товара, раскрывая информацию о себе и соглашаясь на ее обработку, несет риск возникновения негативных последствий от их использования. При этом масштабное распространение цифровых технологий в практическом плане зачастую не дает потребителю (пользователю) возможности выбора – не дал согласие на обработку – не получил услугу или доступ к приложению. Вместе с тем получение сведений, составляющих определенный объем персональных данных, не всегда необходимо для работы приложения, оказания услуги или выполнения работы. Представляется, что учитывая коммерческую составляющую клиентской базы, сбор персональных данных может осуществляться целенаправленно, при этом, соглашаясь на обработку данных, гражданин (потребитель) не имеет гарантий и уверенности, что они будут использованы по декларируемому назначению, следовательно, в принципе не может предотвратить риск наступления неблагоприятных последствий от несанкционированного использования его данных. Акцентируя внимание на вопросе влияния проблемы персональных данных на этику искусственного интеллекта, доктор философских наук Н. А. Ястреб приходит к обоснованному выводу: «Парадокс информированного согласия состоит в том, что без специальных знаний и владения цифровыми навыками на высоком уровне человек не может быть информирован о том, согласие на что он дает. Поскольку в реальности практически никто из пользователей не в состоянии спрогнозировать, какие именно данные о нем получит система искусственного интеллекта и как они могут быть использованы, то совершенно точно можно утверждать, что права человека нарушаются. Особенно это касается тех случаев, когда человек не может по объективным причинам отказаться от взаимодействия с искусственным интеллектом, например, если речь идет о медицинском реанимационном оборудовании или системах отслеживания нарушителей карантина. Согласие в этом случае, будучи формально добровольным, фактически является вынужденным» [6, с. 12].

Проблема защиты персональных данных осложняется и тем, что полный перечень согласий, уже выданных гражданином, составить затруднительно. Следовательно, отследить, проконтролировать и «управлять» своими личными данными в практическом плане крайне затруднительно или невозможно.

Таким образом, в условиях цифровой трансформации общественных отношений, когда обнаруживаются новые способы взаимодействия человека и искусственного интеллекта, тре-

⁸ В России за год утекло более 660 млн записей с персональными данными // Подробнее на РБК: https://www.rbc.ru/technology_and_media/17/04/2023/643936229a7947134f0ce21c (дата обращения: 10.07.2023).

⁹ Сливной год: злоумышленники выложили 1,4 млрд строк из утекших баз российских компаний. URL: <https://www.facct.ru/media-center/press-releases/database-2022/>

бующие адекватной интерпретации в правоприменительной практике, учитывая возможность трансграничного распространения персональных данных, рамки существующих и ожидаемых параметров правовой системы диктуют необходимость поиска оптимального варианта обеспечения защиты личной информации граждан. Ввиду неизбежности процесса внедрения цифровых технологий приоритетным направлением следует признать разработку современных эффективных методов, технических средств обнаружения и предотвращения несанкционированного использования данных, содержащих персональную информацию. Учитывая необходимость максимального информирования конкретного субъекта об использовании его личных данных, обработка персональных данных для статистических или иных исследовательских целей не должна наличествовать в списке исключений, предусмотренном ч. 4 ст. 18 Закона о персональных данных, поскольку заявленные цели не исключают использование личных данных и их хранение, в том числе в целях усовершенствования технологии искусственного интеллекта, посредством которой даже обезличенные персональные данные могут быть со временем идентифицированы. С учетом приведенной аргументации видится целесообразным корректировка подп. 4 ст. 18 Закона о персональных данных.

Список литературы

1. **Пястолов С. М.** Экономические и социальные ценности, риски и организационные парадоксы больших данных: обзор // Большие данные в социальных и гуманитарных науках: Сб. обзоров и рефератов / РАН. ИНИОН. Центр науч.-информ. исслед. по науке, образованию и технологиям; отв. ред. Е. Г. Гребенщикова. М., 2019. 193 с.
2. **Виноградова Т. В.** Реферат. **Бласкес Д., Доменеч Х.** Источники и методы изучения больших данных для социального и экономического анализа // Большие данные в социальных и гуманитарных науках: Сб. обзоров и рефератов / РАН. ИНИОН. Центр науч.-информ. исслед. по науке, образованию и технологиям; отв. ред. Гребенщикова Е. Г. М., 2019. 193 с.
3. **Менщиков А. А., Перфильев В. Э., Федосенко М. Ю., Фабзиев И. Р.** Основные проблемы использования больших данных в современных информационных системах // Столыпинский вестник. 2022. №1. С. 316–329. URL: <https://cyberleninka.ru/article/n/osnovnye-problemy-ispolzovaniya-bolshih-dannyh-v-sovremennyh-informatsionnyh-sistemah/viewer> (дата обращения: 02.07.2023).
4. **Лихачев М. О.** Реферат Ж. Садовский. Данные как капитал: датафикация, аккумулирование и извлечение // Большие данные в социальных и гуманитарных науках: Сб. обзоров и рефератов / РАН. ИНИОН. Центр науч.-информ. исслед. по науке, образованию и технологиям; отв. ред. Гребенщикова Е. Г. М., 2019. 193 с.
5. **Шайдулина В. К.** Большие данные и защита персональных данных: основные проблемы теории и практики правового регулирования. 2019. С. 1-5. URL: <https://cyberleninka.ru/article/n/bolshie-dannye-i-zaschita-personalnyh-dannyh-osnovnye-problemy-teorii-i-praktiki-pravovogo-regulirovaniya/viewer>. (дата обращения: 10.07.2023).
6. **Ястреб Н. А.** Как проблема персональных данных меняет этику искусственного интеллекта? // Философские проблемы информационных технологий и киберпространства. 2020. № 1 (17). С. 1–16. URL: <https://cyberleninka.ru/article/n/kak-problema-personalnyh-dannyh-menyaet-etiku-iskusstvennogo-intellekta/viewer>.

References

1. **Pyastolov S. M.** Economic and social values, risks and organizational paradoxes of big data: a review // Big data in the social and human sciences: Sat. reviews and abstracts / RAS. INION.

- Center for Scientific Information researched in science, education and technology; open ed. Grebenshchikova E. G. M., 2019. 193 p.
2. **Vinogradova T. V. Abstract. Blaskes D., Domenech H.** Sources and methods of studying big data for social and economic analysis // Big data in the social and human sciences: Sat. reviews and abstracts / RAS. INION. Center for Scientific Information researched in science, education and technology; open ed. Grebenshchikova E. G. M., 2019. 193 p.
 3. **Menshchikov A. A., Perfiliev V. E., Fedosenko M. Yu., Fabziev I. R.** The main problems of using big data in modern information systems // Stolypin Bulletin. 2022. No. 1. Pp. 316–329. URL: <https://cyberleninka.ru/article/n/osnovnye-problemy-ispolzovaniya-bolshih-dannyh-v-sovremennyh-informatsionnyh-sistemah/viewer> (accessed: 02.07.2023).
 4. **Likhachev M. O.** Abstract Zh. Sadovsky. Data as a capital: datafication, accumulation and extraction // Big data in the social and human sciences: Sat. reviews and abstracts / RAS. INION. Center for Scientific Information researched in science, education and technology; open ed. Grebenshchikova E. G. M., 2019. 193 p.
 5. **Shaidulina V. K.** Big data and personal data protection: the main problems of theory and practice of legal regulation. URL: <https://cyberleninka.ru/article/n/bolshie-dannye-i-zaschita-personalnyh-dannyh-osnovnye-problemy-teorii-i-praktiki-pravovogo-regulirovaniya/viewer>. 2019. pp.1-5 (accessed: 10.07.2023).
 6. **Yastrebnik N. A.** How does the problem of personal data change the ethics of artificial intelligence? // Philosophical problems of information technologies and cyberspace. 2020. No.1(17). Pp. 1–16. URL: <https://cyberleninka.ru/article/n/kak-problema-personalnyh-dannyh-menyat-etiku-iskusstvennogo-intellekta/viewer>.

Информация об авторе

Яна Александровна Карунная, кандидат юридических наук

Information about the Author

Yana A. Karunnaya, PhD in Law

*Статья поступила в редакцию 11.07.2023;
одобрена после рецензирования 21.07.2023; принята к публикации 31.07.2023*
*The article was submitted 11.07.2023;
approved after reviewing 21.07.2023; accepted for publication 31.07.2023*