https://doi.org/10.17816/RJLS46378

Особенности правового регулирования использования биометрических персональных данных[1]

Петрова Дарья Анатольевна,
кандидат политических наук, доцент
кафедры теории и истории государства и права
Юридической школы
Дальневосточного федерального университета
E-mail: Petrova.dan@dvfu.ru

Мартьянов Никита Русланович,
Студент 3 курса
Юридической школы
Дальневосточного федерального университета
E-mail: martianov.nr@mail.ru

Аннотация. *В настоящей работе авторы освещают правовые основы использования биометрических персональных данных, уделяя особое внимание рассмотрению главной инициативы государства в указанной области — созданию Единой биометрической системы.*

Особенную актуальность исследование приобретает в связи с выходом нового Федерального закона № 168-ФЗ от 8 июня 2020 г. «О едином федеральном информационном регистре, содержащем сведения о населении Российской Федерации». В частности, острой проблемой является возможность интеграции сведений Единой биометрической системы и создаваемого федерального регистра.

Ключевые слова: *Единая биометрическая система, цифровизация, правовая политика, оцифровывание, персональные данные, биометрические персональные данные.*

В современном мире грань между абстрактной категорией «информация» и реальным человеком, носителем этой информации, стирается. Информация о человеке, его персональные данные сегодня превратились в дорогой товар, который можно использовать по-разному:

- при помощи рекламы продать что-либо непосредственно владельцу данных. В настоящий момент широко используются технологии контекстной рекламы, основанной на обработке данных интернет-пользователя;
- составить досье на человека из различных источников, отразив в нем уровень его дохода, предпочтения в еде, часто используемые сайты, круг знакомств в соцтетях и т.д., а затем передать эту информацию заинтересованным организациям, такой практикой занимаются информационные брокеры или брокеры данных — компании, специализирующиеся на сборе и продаже личных данных;
- очернить, выставить пользователя в дурном свете, создать плохую репутацию и тому подобное;
- шантажировать, совершать мошеннические и иные противоправные действия с целью получить прибыль или выгоду[2] [1, с. 45].

Ввиду серьезности вопроса защита информации о человеке может приравниваться к защите реальной личности, поэтому государство производит нормативно-правовое регулирование деятельности, связанной с персональными данными. Для начала необходимо установить терминологию и определить, что персональные данные — это любая информация, относящаяся к прямо или косвенно определенному или

[1] Работа выполнена при финансовой поддержке Гранта Президента РФ № НШ-2668-2020.6 «Национально-культурные и цифровые тренды социально-экономического и политико-правового развития Российской Федерации в XXI веке».

[2] Урманцева А. Переход на личное: в 2019 году утекло вдвое больше персональных данных // Известия iz. URL: https://iz.ru/958561/anna-urmantceva/perekhod-na-lichnoe-v-2019-godu-uteklo-vdvoe-bolshe-personalnykh-dannykh (дата обращения: 04.02.2020).

определяемому физическому лицу (субъекту персональных данных) (п. 1 ст. 3 ФЗ от 27.07.2006 № 152-ФЗ «О персональных данных»)[3]. Несмотря на дискуссию в научных кругах [2, с. 16], персональными данными обладает только физическое лицо.

В соответствии с п. 5 Постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при обработке в информационных системах персональных данных» персональные данные подразделяются на:

- специальные категории персональных данных (персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных);
- общедоступные персональные данные (персональные данные субъектов персональных данных, полученные только из общедоступных источников персональных данных, созданных в соответствии со ст. 8 Федерального закона «О персональных данных»);
- биометрические персональные данные;
- иные категории персональных данных, не относящиеся к названным категориям;
- персональные данные сотрудников оператора, если в информационной системе обрабатываются персональные данные только указанных сотрудников.

В настоящей статье будет уделено внимание правовому режиму использования биометрических персональных данных и последним веяниям правовой политики в отношении указанного вопроса.

В п. 1 ст. 11 ФЗ от 27.07.2006 № 152-ФЗ «О персональных данных» закреплено законодательное определение биометрических персональных данных. Под биометрическими персональными данными понимаются сведения, характеризующие физиологические и биологические особенности человека, на основании которых можно установить его личность[4].

Исходя из данного определения, к биометрическим персональным данным можно отнести физиологические данные (дактилоскопические данные, радужная оболочка глаз, анализы ДНК, рост, вес и др.), а также иные физиологические или биологические характеристики человека. К иным характеристикам относится в том числе изображение человека (фотография или видеозапись), которое позволяет установить его личность и используется оператором для установления личности субъекта. Кроме того, согласно разъяснению Роскомнадзора[5] информация о температуре, получаемая при помощи тепловизора, также относится к биометрическим персональным данным.

В соответствии с вышеуказанной статьей 11 ФЗ «О персональных данных» биометрические персональные данные могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных. Однако предусмотрены и исключения их этого правила:

- в связи с реализацией международных договоров РФ о реадмиссии;
- в связи с осуществлением правосудия и исполнением судебных актов;
- в связи с проведением обязательной государственной дактилоскопической регистрации;
- в случаях, предусмотренных законодательством РФ об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-розыскной деятельности, о государственной службе, уголовно-исполнительным законодательством РФ, законодательством РФ о порядке выезда из РФ и въезда в РФ, о гражданстве РФ.

Существует два способа определения, является ли фотография или видеосъемка биометрическими персональными данными. Первый — самый простой — согласно законодательству. Так, биометрическими данными признаются цветные цифровые фотографические изображения лица владельца документов, удостоверяющих личность гражданина Российской Федерации, по которым граждане Российской Федерации осуществляют выезд из Российской Федерации и въезд в Российскую Федерацию[6]. Однако такой подход очень узок и не может описать практику использования фотографических изображений.

Второй способ — определение по тому, в каких целях оператор обрабатывает данные. Так, если обработка фото или видеосъемка ведется оператором в целях установления личности субъекта персональных данных, то в этом случае согласие субъекта на обработку данных является обязательным (если не попадает

[3] Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // СПС КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_61801/4f41fe599ce341751e4e34dc50a4b676674c1416/ (дата обращения: 05.05.2020).

[4] Там же.

[5] Разъяснения Роскомнадзора «Особенности использования тепловизоров работодателями — операторами персональных данных — с целью предотвращения распространения коронавируса». URL: http://www.consultant.ru/document/cons_doc_LAW_347310/ (дата обращения: 06.04.2020).

[6] Постановление Правительства Российской Федерации от 04.03.2010 № 125 / Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102136321 (дата обращения: 05.05.2020).

под описанные выше исключения)[7]. То есть до момента идентификации субъекта персональных данных фотография или видеоизображение является изображением, правовой режим использования которого регламентирует ст. 152.1 Гражданского кодекса Российской Федерации. С момента же, когда изображение используется в качестве идентификатора личности, изображение признается биометрическими персональными данными, работа с которыми требует обязательного согласия в соответствии с ФЗ № 152 «О персональных данных». Таким образом, хранение фотографий и ксерокопий паспортов граждан РФ в части изображений, если таковые не применяются для установления личности субъекта персональных данных (но если их обработка прямо или косвенно вытекает из требований законодательства и соотносится с целями обработки персональных данных), не влечет за собой правовых последствий [3, с. 40].

Использование изображения как идентификатора личности происходит при помощи биометрических технологий. Под биометрическими технологиями понимаются автоматические или автоматизированные методы распознавания личности человека по его биологическим характеристикам или проявлениям. Основные составляющие биометрического метода — это сканер для измерения биометрической характеристики и алгоритм, позволяющий сравнить ее с предварительно зарегистрированной той же характеристикой (биометрическим шаблоном). Возможны два режима работы системы — верификация (сравнение одного с одним) и идентификация (сравнение одного с многими). При всем теоретическом многообразии возможных биометрических методов (отпечаток пальца, геометрия кисти рук, форма лица, радужная оболочка глаза, сетчатка глаза) применимых на практике среди них немного. Основных методов несколько — распознавание по отпечатку пальца, по изображению лица (двухмерному, трехмерному или 3D фото), по радужной оболочке глаза[8], голосу и венам[9].

В России начало активной работы с биометрическими данными можно связать со сбором сведений о правонарушителях. Отпечатки пальцев, например, являются одним из классических доказательств при расследовании преступления. Правоохранительные органы, взаимодействуя с подозреваемыми, обвиняемыми, осужденными, фиксируют рост человека и его характерные приметы внешности. При этом стоит отметить, как было указано выше, при осуществлении правосудия или оперативно-розыскных мероприятий согласие субъекта на сбор биометрических персональных данных не требуется.

Настоящий расцвет использования систем идентификации пришелся на время пандемии коронавируса. В Москве соблюдение мер безопасности контролировалось в том числе с помощью автоматизированных систем распознавания лиц. Городская система видеонаблюдения включает камеры, установленные во дворах, в подъездах жилых домов, в парках, школах, поликлиниках, магазинах и на стройках, а также в помещениях административных зданий и других общественных местах. С помощью данной системы полиция г. Москвы обнаружила немалое количество нарушителей режима двухнедельной самоизоляции. Однако эта система не может гарантировать абсолютную правильность собранных ею сведений. Так, 19 апреля 2020 г. камерой видеонаблюдения был зафиксирован брат-близнец гражданина, находящегося на обязательной самоизоляции, вследствие чего на данного гражданина, который не нарушал режим обязательной самоизоляции, был выписан штраф в размере 4000 рублей[10].

Также в настоящий момент в России ведется создание Единой биометрической системы, цифровой платформы, которая является одним из ключевых элементов механизма удаленной идентификации человека по его биометрическим характеристикам. Указанная система создается по инициативе Министерства связи и массовых коммуникаций Российской Федерации и Центрального банка Российской Федерации.

Заявленной целью внедрения Единой биометрической системы является повышение доступности услуг, требующих юридически значимого подтверждения личности. Платформа дает возможность заменить личное посещение получением удаленной услуги через Интернет. Внедрение Единой биометрической системы сделает сначала финансовые услуги, а затем и другие

[7] Роскомнадзор разъясняет вопросы отнесения фото-, видеоизображений, дактилоскопических данных к биометрическим персональным данным и особенности их обработки. URL: https://pd.rkn.gov.ru/press-service/subject1/news2729/ (дата обращения: 06.07.2020).

[8] Мазниченко Н.И. Области применения и принципы построения биометрических систем идентификации личности // Вестник Национального технического университета Харьковский политехнический институт. Серия: Информатика и моделирование. 2007. URL: https://cyberleninka.ru/article/n/oblasti-primeneniya-i-printsipy-postroeniya-biometricheskih-sistem-identifikatsii-lichnosti/viewer (дата обращения: 04.03.2020).

[9] Вихман В.В., Якименко А.В. Внедрение биометрической идентификации в системы контроля и управления доступом. Учебное пособие для вузов. М.: Издательство НГТУ, 2018. С. 25.

[10] Морозова О. Москвича с коронавирусом по ошибке оштрафовали за нарушение карантина. Система распознавания лиц перепутала его со здоровым братом-близнецом. URL: https://snob.ru/society/moskvicha- s-koronavirusom-po-oshibke-oshtrafovali-za-narushenie-karantina-sistema-raspoznavaniya-lic-pereputala-ego-so-zdorovym-bratom-bliznecom/ (дата обращения: 15.05.2020).

цифровые сервисы более доступными для граждан из отдаленных регионов, а также для маломобильных граждан, сообщается на официальном сайте Единой биометрической системы «Ростелеком»[11].

Возможность создания Единой биометрической системы привела к изменениям в Федеральном законе № 149 от 27.07.2020 «Об информации, информационных технологиях и о защите информации». В закон была добавлена статья 14.1, регламентирующая создание Единой биометрической системы. Размещать биометрические данные в системе могут «государственные органы, банки и иные организации в случаях, определенных федеральными законами, после проведения идентификации при личном присутствии гражданина Российской Федерации с его согласия на безвозмездной основе...». Таким образом, во-первых, речь в законе далеко не ограничивается банковской сферой, а во-вторых, использовать биометрические данные могут любые организации, определенные Правительством.

О планах на Единую биометрическую систему (ЕБС) уже заявлено на расширительном заседании Комиссии Общественной палаты Москвы по гражданскому обществу и общественному контролю. 6 июля 2020 г. заместитель председателя ЦИК РФ Николай Булаев упомянул о разработке программно-технического комплекса, который для подтверждения личности избирателей будет использовать ЕБС. Также Булаев подчеркнул, что система для голосования с использованием биометрии концептуально будет готова до конца 2020 г., и не исключено, что она будет использоваться в Единый день голосования в сентябре 2021 г., в том числе на выборах в Государственную Думу РФ[12].

Несмотря на то, что обработка персональных данных, согласно п. 1 ст. 14.1, осуществляется при согласии гражданина, необходимо иметь в виду п. 16 ст. 14.1 ФЗ № 149. Согласно указанному пункту оператор ЕБС отправляет биометрические данные граждан «*в федеральный орган исполнительной власти, осуществляющий функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере внутренних дел, и федеральный орган исполнительной власти в области обеспечения безопасности в целях обеспечения обороны страны, безопасности государства, охраны правопорядка и противодействия терроризму*». Таким образом, органы внутренних дел и безопасности имеют доступ к биометрическим данным граждан и право обработки этих данных без согласия граждан.

Указанный выше факт того, что органы госбезопасности будут обрабатывать биометрические данные граждан, также коррелируется с принятым недавно Федеральным законом от 8 июня 2020 г. № 168-ФЗ «О едином федеральном информационном регистре, содержащем сведения о населении Российской Федерации». Перечень сведений, вносимый в регистр (определен в п. 2 ст. 7), может быть расширен органами, уполномоченными на решение задач в области обеспечения безопасности Российской Федерации в рамках реализации своих полномочий (п. 15 ст. 8). Полный перечень органов, которые могут вносить изменения, а также порядок внесения сведений будут определяться Указом Президента и Постановлением Правительства. Таким образом, можно говорить о том, что перечень вносимых в регистр сведений не является исчерпывающим, и это оставляет возможность для внесения биометрических данных.

Также стоит отметить, что при разработке ЕБС используются более совершенные алгоритмы идентификации. Для идентификации применяются совместно два типа биометрии: голос и лицо. По заявлению «Ростелекома», именно такой способ является самым эффективным и удобным на данный момент. Также он позволит точно различать в том числе и близнецов, так как биометрические алгоритмы, заложенные в системе, обладают высокой точностью. Исходя из этого, можно заметить, что такая ситуация, как было указано выше, при неразличении камерой видеофиксации близнецов, может повториться с меньшей долей вероятности.

Большое значение в Единой биометрической системе уделено безопасности. Порог точности распознавания системы определен Приказом Министерства цифрового развития, связи и массовых коммуникаций РФ № 321 от 25 июня 2018 г.[13] Единая биометрическая система имеет точность распознавания 10^{-7}, т.е. она пропустит одного человека на 10 млн. При этом в системе используется дополнительная связка с логином и паролем от Госуслуг, поэтому, по заявлению ПАО «Ростелеком», обмануть систему практически невозможно. Также для обеспечения информационной безопасности биометрических данных пользователей системы реализовано распределенное хранение данных: биометрический

[11] О единой биометрической системе. URL: https://bio.rt.ru/faq/project/ (дата обращения: 14.04.2020).

[12] При онлайн-голосовании в РФ будет использоваться биометрия. URL: https://www.interfax.ru/russia/716074 (дата обращения: 14.04.2020).

[13] Приказ Министерства цифрового развития, связи и массовых коммуникаций РФ от 25.06.2018 № 321 «Об утверждении порядка обработки, включая сбор и хранение, параметров биометрических персональных данных в целях идентификации…» // Информационно-правовое обеспечение Гарант.ру. URL: http://base.garant.ru/71985302/ (дата обращения: 22.03.2020).

шаблон хранится в обезличенной форме отдельно от персональных данных — ФИО, паспортных данных, СНИЛС и др., включенных в базы ЕСИА (портал Госуслуг).

Однако по информации «Лаборатории Касперского», международной компании, работающей в сфере информационной безопасности с 1997 г., существующие системы биометрической аутентификации оказались не лишены существенных родовых недостатков, а именно проблемы их информационной безопасности. Представления о биометрических данных как об уникальном неподделываемом идентификаторе человека изначально неверны и могут внушать ложное чувство защищенности.

«Лаборатория Касперского» указала на определенные особенности обработки и хранения биометрических данных, в том числе[14]:

1) точность их распознавания системами аутентификации, хотя относительно высока, может оказаться все-таки недостаточной для многих применений; биометрические системы имеют обычно ненулевые вероятности ложноотрицательного и ложноположительного срабатывания;

2) многие из биометрических характеристик человека могут быть фальсифицированы злоумышленником, а скопировать оцифрованные биометрические данные может быть даже проще, чем физические;

3) однажды скомпрометированные биометрические данные скомпрометированы навсегда — пользователь не сможет поменять украденные отпечатки пальцев, как меняет пароль в случае его кражи; потенциально человек может страдать от этой проблемы на протяжении всей оставшейся жизни. Указанная проблема является достаточно серьезной, поскольку вместе с развитием информационных технологий совершенствуются и схемы мошенничества и краж. Так, например, участились случаи использования нейролингвистического программирования, при которых жертвы самостоятельно раскрывают мошенникам пароли, данные и иную запрашиваемую информацию, биометрические ключи не являются в этой схеме исключениями.

По данным Kaspersky Security Network в третьем квартале 2019 г. вредоносное ПО было заблокировано на 37 % компьютеров, выполняющих функции сбора, обработки и хранения биометрических данных, т.е. фактически каждый третий компьютер подвергся риску заражения вредоносным ПО. В числе прочих вредоносных объектов продуктами «Лаборатории Касперского» были заблокированы современные троянские программы для удаленного доступа к системе (5,4 % всех исследованных компьютеров), вредоносные программы, используемые в фишинговых атаках (5,1 %), программы-вымогатели (1,9 %) и банковские троянцы (1,5 %)[15].

Несмотря на угрозы извне существует не менее опасная внутренняя угроза принудительной цифровизации, против которой выступает значительная часть населения. При первоначальной передаче биометрических персональных данных в обязательном порядке требуется согласие владельца данных, однако в дальнейшем согласие гражданина не требуется. При этом данные людей, не совершивших преступлений, передаются в органы внутренних дел и госбезопасности, а также всем операторам, работающим с Единой биометрической системой. На наш взгляд, в этом случае возникают две серьезные проблемы, уже ставшие традиционными для российской цифровизации. Первая — отсутствие у гражданина права влиять на обработку своих персональных данных. В мире же существует практика получения предварительного согласия национального органа по защите персональных данных для обеспечения надлежащей защиты личной информации [4, с. 100]. Вторая проблема — отсутствие механизма по удалению данных из систем учета по желанию гражданина. Отсутствие диалога по решению указанных проблем будет только усугублять недоверие граждан к руководству страны.

Список литературы

1. Савельев А.И. Проблемы применения законодательства о персональных данных в эпоху «Больших данных» (Big Data) // Право. Журнал Высшей школы экономики. 2015. № 1. С. 224.
2. Петрыкина Н.И. Правовое регулирование оборота персональных данных. Теория и практика. М.: Статут, 2019. С. 16.
3. Брызгин А.А., Минбалеев А.В. Правовой режим биометрических персональных данных // Вестник УРФО. Безопасность в информационной сфере. 2012. № 2. С. 40.
4. Кривогин М.С. Предпосылки формирования специальной правовой защиты биометрических персональных данных // Общество: политика, экономика, право. 2016. № 8. С. 100.

[14] Круглов К. Угрозы безопасности для систем обработки и хранения биометрических данных. Kaspersky ICS CERT. URL: https://ics-cert.kaspersky.ru/reports/2019/12/02/biometric-data-processing-and-storage-system-threats (дата обращения: 12.02.2021).

[15] Круглов К. Угрозы безопасности для систем обработки и хранения биометрических данных. URL: https://securelist.ru/biometric-data-processing-and-storage-system-threats/95221/ (дата обращения: 16.05.2020).

Features of the Legal Regulation of the Use of Biometric Personal Data[1]

Petrova Daria,
PhD in Political Science,
Associate Professor
School of Law
Far Eastern Federal University
E-mail: Petrova.dan@dvfu.ru

Martianov Nikita,
3rd year Student
School of Law
Far Eastern Federal University
E-mail: martianov.nr@mail.ru

Abstract. *In this paper, the authors highlight the legal basis for the use of biometric personal data, and also pay attention to the main initiative of the state in this area: the creation of a unified biometric system.*
The study is particularly relevant in connection with the release of the new Federal law No. 168-FZ on June 8, 2020: "On the unified Federal information register containing information about the population of the Russian Federation." In particular, an acute problem is the ability to integrate information from the unified biometric system and the Federal register that is being created.
Keywords: *Unified biometric system, digitalization, legal policy, digitization, personal data, biometric personal data..*

References

1. Savel'ev A.I. Problemy primeneniya zakonodatel'stva o personal'nyh dannyh v epohu «Bol'shih dannyh» (Big Data). *Pravo. Zhurnal Vysshej shkoly ekonomiki.* 2015;(1):224. (In Russ.).
2. Petrykina N.I. Pravovoe regulirovanie oborota personal'nyh dannyh. Teoriya i praktika. Moscow: Statut, 2019. P. 16. (In Russ.).
3. Bryzgin A.A., Minbaleev A.V. Pravovoj rezhim biometricheskih personal'nyh dannyh. *Vestnik URFO. Bezopasnost' v informacionnoj s*fere. 2012;(2):40. (In Russ.).
4. Krivogin M.S. Predposylki formirovaniya special'noj pravovoj zashchity biometricheskih personal'nyh dannyh. *Obshchestvo: politika, ekonomika, pravo*. 2016;(8):100. (In Russ.).

[1] This work was financially supported by the Russian Federation Presidential Grant No. НШ-2668-2020.6 "National-Cultural and Digital Trends in the Socio-Economic, Political, and Legal Development of the Russian Federation in the 21st Century."