И. М. Рассолов*,
С. Г. Чубукова**,
И. В. Микурова***

БИОМЕТРИЯ В КОНТЕКСТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ И ГЕНЕТИЧЕСКОЙ ИНФОРМАЦИИ: ПРАВОВЫЕ ПРОБЛЕМЫ[1]

Аннотация. *В современном обществе активно развиваются методы идентификации лиц на основе их физических, биологических или поведенческих характеристик. Европейские страны находятся в процессе создания целостной доктрины по вопросу биометрического контроля и уточняют собственную позицию в отношении тех ситуаций, когда биометрические данные используются частными лицами.*

С позиции информационного права в статье представлен новый авторский подход к проблеме обработки биометрических данных, а также генетической информации. Существующее много лет деление биометрии на «следовую» и «неследовую» теряет свое значение. Предложена новая классификация биометрии на цифровую и аналоговую.

Биометрический контроль доступа не должен становиться рутинным явлением в рамках организации, предприятия и без каких-либо оснований заменять другие существующие виды контроля. Заинтересованному лицу можно самостоятельно доверить хранение собственных биометрических данных, чтобы уменьшить риски утечки и последствия воздействия на них. Биометрические данные должны храниться на серверах компании в зашифрованной форме, что делает невозможным их использование при отсутствии согласия заинтересованного лица.

Биометрические данные должны быть защищены специальным правовым режимом. Предпринятый анализ европейского и российского законодательства позволил сделать следующие выводы: биометрические данные являются особым видом персональных данных, для них должен быть установлен специальный правовой режим и регулирование; цифровая биометрия нуждается в особом правовом регулировании, так как она наиболее уязвима;

* *Рассолов Илья Михайлович,* доктор юридических наук, и. о. заведующего кафедрой информационного права и цифровых технологий Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)
ilyarassolov@mail.ru
125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

** *Чубукова Светлана Георгиевна,* кандидат юридических наук, доцент кафедры информационного права и цифровых технологий Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)
sgchubukova@msal.ru
125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

*** *Микурова Ирина Владимировна,* кандидат юридических наук, доцент кафедры государственно-правовых и уголовно-правовых дисциплин Российского экономического университета имени Г.В. Плеханова
fille-en-rouge@yandex.ru
117997, Россия, г. Москва, Стремянный пер., д. 36

генетическая информация в полной мере не соответствует понятию персональных данных, так как может относиться к неограниченному кругу лиц. Это определяет необходимость разработки специального закона «О генетической информации».

Ключевые слова: *информация, информационное право, биометрия, биометрические данные, цифровая биометрия, биометрический контроль, ДНК, генетическая информация, персональные данные, идентификация лица.*

DOI: 10.17803/1729-5920.2019.146.1.108-118

В различных сферах сегодня активно используются методы биометрии — компьютерные методы, которые позволяют автоматически распознавать человека на основе его физических, биологических или поведенческих характеристик.

Биометрия лежит в основе идентификационных документов (биометрических паспортов, идентификационных карт, ID-карт), стандартизацией которых в мире занимается Международная организация гражданской авиации (ИКАО)[2] при ООН. С 2002 г. в ее документах биометрия признается основным способом идентификации[3]. Страны — участницы ИКАО принимают технологию распознавания лица как основной и обязательный способ идентификации, а также по своему усмотрению могут применять технологию идентификации с помощью отпечатков пальцев и сканирования радужной оболочки глаза. Такие биометрические паспорта уже используются во многих странах: в Белоруссии, Казахстане, Молдавии, Монголии, Пакистане, США, Израиле, Туркмении, Узбекистане, на Украине, в странах Евросоюза.

Пока государства делают робкие попытки регулирования отношений в сфере обработки биометрической информации. Примерно с 2016 г. руководство Европейского Союза пытается сформулировать собственный подход к биометрической обработке данных. Европейские страны вырабатывают доктрину по вопросу биометрического контроля и уточняют собственную позицию в отношении тех ситуаций, когда биометрические данные используются частными лицами.

В России также активно идут общественные обсуждения по поводу внедрения электронных паспортов — внутренних удостоверений личности, содержащих биометрические данные[4].

Как мы считаем, данная работа должна ориентироваться на следующие правовые цели: во-первых, дать физическим лицам возможность лучше контролировать собственные данные; во-вторых, государство должно более эффективно управлять системами обработки таких данных; в-третьих, следует предвидеть последствия применения европейского Регламента General Data Protection Regulation (GDPR)[5], который будет обязывать ответственных лиц, осуществляющих обработку такой информации, вводить новые меры эффективной защиты электронных документов.

Анализ современной правовой доктрины и зарубежного законодательства о биометри-

---

[1] Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-29-14033.

[2] International Civil Aviation Organization, ICAO.

[3] Стандарты на биометрические паспорта содержатся в документе ИКАО Doc9303: ICAO Document 9303, Part 1, Volume 1 (OCR машиночитаемые паспорта); ICAO Document 9303, Part 1, Volume 2 (е-паспорта или паспорта с RFID-чипом); ICAO Document 9303, Part 3 (идентификационные пластиковые карточки).

[4] *Михайлов М. А., Волеводз А. Г.*, *Сидоренко Э. Л.* Международная научно-практическая конференция в Государственной Думе «Совершенствование системы дактилоскопической регистрации» // Библиотека криминалиста. Научный журнал. 2016. № 1 (24). С. 368—378 ; *Аюпова А. Р.*, *Ахатов Р. Р.* Биометрический паспорт: зло или добро // Здоровый образ жизни как условие устойчивого развития государства : сборник материалов Всерос. науч.-практ. конференции. 2017. С. 35—38 ; *Фахреева Д. Р.*, *Фахреев Н. Н.* Биометрический документ как элемент противодействия коррупции // Наука, техника и образование. 2016. № 3 (21). С. 208—209 ; *Соколов Ю. Н.* Электронный паспорт в уголовном судопроизводстве // Евразийский юридический журнал. 2017. № 4 (107). С. 265—267.

[5] The EU General Data Protection Regulation (GDPR) is the most important change in data privacy regulation in 20 years // URL: https://eugdpr.org (дата обращения: 15.11.2018).

ческих данных позволяет сформулировать один из важных постулатов о том, что этот вид социальной информации должен быть предметом особого внимания со стороны государств. Мы считаем, что биометрические данные не являются обычными персональными данными. Они являются результатом особой технической обработки физических, физиологических или поведенческих характеристик людей и позволяют автоматически идентифицировать граждан. В самом начале биометрия использовалась только для судебной идентификации, сегодня же она интегрирована во многие акты нашей повседневной жизни и используется для предварительной идентификации людей. Например, это контроль доступа работников к офисным, банковским помещениям; входы в компьютерные системы; доступ к онлайн-сервисам; распознавание личности при переходе государственной границы и др. В некоторых странах это также средство подтверждения подключения пользователя к телевизионным услугам; механизм замены электронных ключей в процессе осуществления онлайн платежей или процедура защиты оборота медицинских данных.

Биометрия часто представляется как эффективная альтернатива использованию множества паролей, которые сложны для запоминания. Биометрические данные позволяют в любой момент идентифицировать заинтересованное лицо по присущим только ему биологическим особенностям (отпечатки пальцев, сетчатка глаза, рисунок вен рук). Поэтому их обработка создает значительные риски для защиты прав и свобод граждан.

Очевидно, что в отличие от пароля, невозможно просто избавиться от биометрических индивидуальных характеристик или их легко изменить. Утечка биометрических данных (например, путем воспроизведения отпечатка пальца и повторного его использования без ведома соответствующего лица) может иметь ощутимые последствия для заинтересованного лица: он больше не сможет использовать скомпрометированные биометрические данные, а также впоследствии надежно себя идентифицировать.

В этой связи биометрическая обработка данных не являются безобидным явлением и требует особого правового регулирования. Именно поэтому, как мы считаем, законодатель должен предусмотреть усиленный контроль процедуры оборота подобной информации, которая должна быть предметом предварительного обсуждения в Государственной Думе и в Совете Федерации.

Кроме того, необходимо серьезное правовое исследование данных проблем на государственном уровне, которое бы впоследствии послужило основой при разработке новейшего законодательства. Так, например, Европейский регламент GDPR, вступивший в силу с мая 2018 г., признал особый характер исследуемых данных и квалифицировал их как наиболее «уязвимые» в современном информационном обществе, так как они могут касаться здоровья, частной жизни, политических или религиозных убеждений граждан, обработка которых ограничена. Таким образом, европейский законодатель признает эти данные особыми.

В этом контексте мы считаем важным рассмотреть историю вопроса. Исторически выделяются два вида биометрии — «следовая» и «не следовая».

«Следовая» биометрия. Очевидно, что некоторые части тела человека оставляют следы (например, отпечаток пальца на стакане), которые можно легко воспроизвести и использовать с помощью информационных технологий. Поэтому биометрическая обработка исследуемых данных представляет собой высокий риск. Централизованное и локальное регулирование оборота подобной информации должно исходить из важного постулата о том, что лица должны сохранять контроль за собственными биометрическими данными; сведения следует надежно защищать при помощи технических механизмов защиты, принадлежащих лицу (например, карточка прохода в здание, электронный пропуск, USB-ключ и др.). Централизация анализируемых биометрических данных на серверах, контролируемых специальным оператором, должна допускаться исключительно при соблюдении «сильного предписания по безопасности» и быть связана с целями такой обработки.

Биометрия «без следа». «Не следовая» биометрия, например рисунок вен руки, считается менее рискованной с точки зрения последствий, поэтому при соблюдении необходимых правил эти данные могут быть централизованы в базах данных. На протяжении многих лет был разработан большой инструментарий для сбора и анализа характерных черт людей. Например, для распознавания лиц повсеместно используются камеры видеонаблюдения. Это также фотографии, которые организации выкладывают на официальных порталах, а также

сами работники в Интернете, оставляя многочисленные «цифровые следы». Аналогичное заключение может быть сделано в отношении распознавания речи и разработки устройств записи голоса; в отношении распознавания рисунка вен руки и возможностей анализа и обработки подобной информации с помощью инфракрасной камеры.

Предпринятый анализ позволяет нам сделать вывод о том, что отныне все биометрические данные нужно рассматривать именно как «следовые» или оставляющие многочисленные **цифровые следы**.

Итак, любая биометрия (как «следовая», так и «не следовая») представляет собой высокий риск для индивидов. Поэтому в целях дальнейшего исследования представляется важным сформулировать несколько правовых рекомендаций, позволяющих гражданам осуществлять контроль в отношении собственных биометрических данных.

Мы считаем, что биометрический контроль доступа не должен становиться рутинным явлением в рамках организации, предприятия и без каких-либо оснований заменять другие существующие виды контроля, порой менее обременительные (бейдж, ключ, электронная карта и др.). Здесь следует отдавать предпочтение средствам, гарантирующим контроль отдельных лиц за биометрической информацией по принципу «минимизации данных».

Данное умозаключение позволяет нам сформулировать два важных принципа. Во-первых, заинтересованному лицу можно доверить самостоятельное хранение собственных биометрических данных, чтобы уменьшить риски утечки и последствия воздействия на них, например, в случае кражи или взлома системы. В случае потери или кражи биометрических данных будут скомпрометированы данные только этого лица, а не биометрия всех лиц, находящихся в базе. Во-вторых, биометрические данные должны храниться на серверах компании в зашифрованной форме, что делает невозможным их использование при отсутствии согласия заинтересованного лица. На практике биометрические данные должны быть защищены специальным режимом: заинтересованное лицо может единолично использовать информацию при собственной аутентификации. Например, в целях обеспечения безопасности (в чрезвычайных ситуациях, в целях производственной необходимости) атомная электростанция может иметь возможность централизовать биометрические данные сотрудников, имеющих право на доступ к помещениям. В этих случаях организация должна будет доказать, что ее работа не может быть осуществлена без подобных действий, то есть без биометрической обработки и, с другой стороны, без успешной увязки с хранилищем биометрических данных. После документального подтверждения значимости этих действий должностное лицо (уполномоченный по обработке данных) должен будет соблюдать условия, приняв все меры по минимизации рисков, связанных с обработкой анализируемой информации.

В этом контексте особое значение приобретает биометрическая обработка данных именно физических лиц. Очевидно, что контроль доступа по биометрическим данным пользуется большим успехом у людей и организаций, желающих упростить собственную работу, включая разблокировку смартфонов, доступ к мобильным приложениям, осуществлению оплаты товаров и др. Эта деятельность значительно распространилась благодаря внедрению функции аутентификации отпечатков пальцев в дополнение к паролям в последних моделях телефонов крупных производителей. В этой связи следует более детально определить правовую базу, применимую к использованию этих функций на различных устройствах в процессе осуществления биометрической обработки данных, включая надлежащую их защиту. Обозначим некоторые важные положения, связанные с последним заключением.

Во-первых, обработка, выполняемая по инициативе и под контролем соответствующего лица, должна осуществляться в личных целях и для приватного пользования. Таким образом, компании, использующие биометрическое распознавание, интегрированное в их устройства, не должны спрашивать разрешения на подобные действия, если данная обработка соответствует всем следующим критериям, обозначенным ниже:

Пользователь использует устройство конфиденциально, используя свои собственные биометрические данные, чтобы разблокировать свой телефон или получить доступ к приложениям, которые он загрузил автономно.

Пользователь самостоятельно решает, использовать биометрическую аутентификацию или нет, встроенную в его устройство. За исключением биометрической аутентификации, предложенной его работодателем, если устройство было предоставлено работнику в процессе

его профессиональной деятельности; это предполагает, что разработчики приложений предлагают также альтернативный режим аутентификации для биометрии (например, ввод кода) без дополнительных ограничений.

Биометрические данные хранятся в устройстве в изолированной среде и недоступны для передачи вне системы: за исключением биометрической обработки на устройствах, отправляющих сведения в удаленную базу данных, а также любой возможности внешнего вмешательства в систему по биометрическим данным (например, производитель устройства или разработчик приложения).

Биометрические данные хранятся в зашифрованном виде с использованием криптографического алгоритма, защищенного ключами в соответствии с уровнем техники. Устройства, работающие в этих условиях, включают по умолчанию механизмы защиты конфиденциальности. Действительно, биометрические данные вряд ли будут перенаправлены третьим лицам, если они остаются внутри технического устройства и если это устройство остается под контролем его пользователя. Помимо этого, выбор применения биометрической аутентификации принадлежит главному заинтересованному лицу, то есть самому пользователю. Следует указать на тот факт, что в этом случае разработчик приложения или оператор связи не отвечает за обработку соответствующих биометрических данных пользователя, но он по-прежнему несет ответственность за безопасность разработанного им приложения. Таким образом, он должен обеспечить надежность системы биометрической аутентификации, с которой его приложение может обмениваться, в частности:

— проверяя ложные попытки ввода информации;
— проверяя, что поставляемое им программное обеспечение устойчиво к атакам и возможным фальсификациям (например, в настоящее время распространено использование ложных фотографий для обмана распознавания лиц; использование ложных отпечатков пальцев для распознавания отпечатков пальцев);
— количество попыток аутентификации должно быть также ограничено.

Кроме того, ответственные за обработку данных лица, осуществляющие свои полномочия, должны будут доказать посредством документации, что условия осуществления контроля доступа оправданы целями использования биометрической обработки и что принимаются все необходимые технические меры для ограничения рисков, связанных с использованием исследуемых данных.

Во-вторых, если биометрическое распознавание, предлагаемое человеку на его устройстве, работает во взаимодействии с удаленными серверами, контролируемыми третьими лицами, соответствующая организация (разработчик приложения, производитель устройства и т.д.) должна получить разрешение на такую обработку от пользователя.

Например, в популярном немецком банке Commerzbank была внедрена система распознавания речи, которая запускается перед началом предварительного заполнения формы онлайн-платежей. Голосовая запись хранится на серверах банка в зашифрованном виде с помощью ключа, находящегося под контролем клиента. Таким образом, использование этих данных невозможно без согласия клиента; невозможна также передача банковской информации третьим лицам. То же самое касается биометрической аутентификации для приложений для загрузки на смартфоны. Отпечаток пальца владельца хранится в зашифрованном виде, прикрепляется и выводится из системы (открепляется) в приложении. Затем он может быть сравнен оператором при помощи бесконтактной связи с оригиналом с помощью специального биометрического считывателя.

Итак, анализ показывает, что законодательное регулирование должно быть направлено в первую очередь на то, чтобы сохранить контроль пользователя над биометрическими данными, уважать его свободу выбора, а также минимизировать риски вмешательства в частную жизнь граждан.

Как представляется, операторы обработки данных должны будут провести оценку достаточности собственных технических средств в отношении защиты данных, если биометрическая обработка будет проводиться в больших масштабах.

Необходимо указать на тот факт, что система предварительного контроля, связанная с выдачей специального согласия на обработку биометрических данных, которое предшествует процедуре обработки, была изменена новым Регламентом GDPR. Это будет способствовать в скором времени переходу к системе эффективного **последующего контроля** (то есть контроля апостериори).

В этой связи ответственный за обработку биометрических данных будет должен:

— документировать свою обработку и принимать меры по соблюдению информационной безопасности;
— в определенных законом случаях проводить оценку собственного воздействия в соответствии со ст. 35 Регламента;
— хранить документацию и предоставлять ее в распоряжение контролирующих органов в случае последующего контроля.

Анализ показывает, что особое значение приобретает биометрическая **обработка данных, осуществляемая государством**. Как представляется, аналогичный подход должен быть предложен для решения вопроса биометрической обработки данных, осуществляемой органами публичной власти. Многочисленные обсуждения за рубежом позволили государственным служащим лучше контролировать данные, но послужили причиной усиления контроля в исследуемой сфере. Например, в отношении обработки данных автоматизированной системой пограничного контроля мы считаем, что используемый механизм защиты соответствует целям обработки, будь то использование отпечатков пальцев лиц, пересекающих государственную границу, или фотографирование для распознавания лиц. Поскольку процедура основана на принципе добровольности и предполагает сохранение этих биометрических данных именно в системе, в которой эти данные обращаются и используются.

Однако согласие лиц может быть исключено в контексте определенных целей обработки, а также защиты публичных интересов. Технические файлы полиции, такие как автоматизированный файл отпечатков пальца (например, во Франции он называется FAED[6]), одной из целей которого является идентификация лица, чья идентичность неизвестна, являются типичным примером использования подобных биометрических данных. С точки зрения информационного права должен быть использован единый подход как в государственном, так и в частном секторе: очевидно, что многочисленные цели требуют фиксации информации, основанной на биометрических данных, как в частной, так и в публичной сфере. Однако должны быть предусмотрены гарантии, а также меры информационной безопасности, которые вводятся для смягчения рисков, связанных с несанкционированным использованием таких данных.

Мы считаем, что введение в оборот новых электронных паспортов (метапаспортов) и внутренних биометрических удостоверений личности должно быть предметом многочисленных обсуждений, которые бы четко определили возможности использования таких смешанных электронных документов. В этой связи интересен европейский опыт решения этих задач. Например, французская система файлов TES[7], созданная специальным Декретом от 28 октября 2016 г.[8] в отношении международных паспортов и национальных удостоверений личности, предназначена для объединения (консолидации) всех оцифрованных документов и персональных данных, собранных в рамках специальной процедуры. Это, в частности, сканированные изображения лиц, фиксация отпечатков пальцев просителей этих документов.

Тем не менее мы считаем, что введение такой централизованной системы в России не является в достаточной мере гарантией для обеспечения высокого уровня информационной безопасности граждан.

Действительно, объединение в единую базу всех этих важных сведений приведет к значительным изменениям в масштабах и в характере обработки. Очевидно, что обработка путем

---

[6] Le Fichier Automatisé des Empreintes Digitales (FAED) был официально введен французским Декретом от 8 апреля 1987 г. Этот файл (или досье) включает автоматическую обработку следов и отпечатков пальцев, осуществляемую французской полицией и жандармерией. Целью этого файла является выявление краж персональных данных на французской территории, а также идентификация цифровых следов, обнаруженных на местах преступления. Досье включает следующие данные: отпечатки пальцев лиц, причастных к уголовному делу; отпечатки пальцев лиц, помещенных в пенитенциарные учреждения; вещественные доказательства и отпечатки пальцев, переданные агентствами международного сотрудничества; следы и отпечатки, обнаруженные на месте преступления.

[7] Файл защищенных электронных документов (файл TES) представляет собой базу данных, в которую Министерство внутренних дел Франции собирает биометрические данные французов для управления системой внутренних удостоверений личности и французских паспортов для зарубежных поездок.

[8] Например, Декрет № 2016-1460 от 28 октября 2016 г., разрешающий осуществление обработки персональных данных, касающихся паспортов и национальных удостоверений личности.

включения биометрических данных почти всего населения страны является беспрецедентным случаем. Однако все нюансы, а также альтернативы внедрения такой базы данных должны быть хорошо изучены и оценены, независимо от того, идет ли речь об использовании системы распознавания лиц, или о записи данных в рамках судебных процессов, или об обороте данных в сфере телемедицины.

Мы считаем необходимым дальнейшее обсуждение этого вопроса. Эта рекомендация основывается на двойном постулате: с одной стороны, это касается масштабности и значимости такой обработки, которая включает конфиденциальные данные большого числа наших сограждан, а с другой стороны, это связано с выбором специальной ответственной компании, осуществляющей такие важные функции.

Особый интерес сегодня представляют генетические исследования и статус генетической информации. В рамках темы данной статьи необходимо разобраться: **является ли генетическая информация биометрическими персональными данными**?

ДНК (дезоксирибонуклеиновая кислота) — носитель генетической информации о человеке, записанной в виде последовательности нуклеотидов с помощью генетического кода. ДНК каждого живого существа уникальна и является своеобразным индивидуальным «отпечатком», позволяющим идентифицировать человека. А следовательно, генетическая информация, наряду с такими физиологическими характеристиками человека, как отпечатки пальцев, рисунок вен руки, радужная оболочка глаз и др., должна быть отнесена к биометрическим персональным данным.

Вместе с тем, как отмечают некоторые исследователи, с молекулой ДНК, помимо ее индивидуальности, связано и другое основополагающее свойство — наследственность и способ передачи наследственной информации. Таким образом, молекула ДНК является носителем информации не только о конкретном индивидууме, но и о его родителях и родственниках[9].

Из этого следует, что, давая согласие на обработку своей генетической информации, субъект персональных данных также разрешает доступ к генетической информации своих родственников. А это с точки зрения законодательства о персональных данных требует получения их согласия.

Эти особенности генетической информации позволяют сделать вывод, что неправильно относить ее только к персональным данным конкретного лица. Такая информация в значительной мере относится и к неограниченному кругу лиц — родственников, предков и потомков. Поэтому генетическая информация представляет собой самостоятельный вид конфиденциальной информации, сбор, хранение, использование и распространение которой возможны только в соответствии с положениями законодательства и не определяются лишь согласием субъекта.

В практике многих стран первоначально методы генетической регистрации использовались только в отношении граждан, которые совершали преступления или являлись подозреваемыми в их совершении[10].

Данная проблема была предметом судебного разбирательства в деле S. and Marper v. The United Kingdom[11]. В своем решении ЕСПЧ подчеркнул, что концепция частной жизни является весьма широкой по своей природе и ей нельзя дать исчерпывающее определение. Само хранение информации о физическом лице является вмешательством в частную жизнь, однако необходимость и обоснованность такого вмешательства следует рассматривать применительно к конкретному делу и учитывать тип информации, способ ее использования и получаемый результат. Суд также указал на то, что хранение самих образцов ДНК в течение длительного времени является вмешательством в частную жизнь гражданина, поскольку существует вероятность того, что в будущем, при развитии технологий в сфере генетики, будет существовать возможность нарушения прав человека.

Еще одним важным моментом является регулирование количества информации, которое может быть получено в результате такой регистрации. В европейском законодательстве

---

[9] *Кубитович С. Н.* ДНК как носитель информации неограниченного круга лиц // Вестник экономической безопасности. 2017. № 4. С. 186.

[10] Criminal Justice and Police Act 2001 // URL: http://www.legislation.gov.uk/ukpga/2001/16/section/82 (дата обращения: 15.11.2018)

[11] Case of S. and Marper v. The United Kingdom // URL: http://www.bailii.org/eu/cases/ECHR/2008/1581.html (дата обращения: 15.11.2018)

происходит разделение понятий «некодирующие» и «кодирующие» сегменты ДНК. Целью анализа «кодирующих» последовательностей является получение информации о здоровье соответствующего лица (например, генетическое уродство, предрасположенность к заболеванию). «Некодирующие» сегменты ДНК предназначены для идентификации человека.

Так, ст. 706-54 Уголовно-процессуального кодекса Франции предусматривает, что генетические отпечатки пальцев, сохраненные в FNAEG[12], производятся только из «некодирующих» сегментов ДНК. Единственная цель, которую преследует эта обработка, —получить «генетическую подпись» человека, а не информацию о его физиологических, морфологических, наследственных характеристиках. Генетическая идентификация направлена на идентификацию человека, а не на его изучение[13].

Данную норму разъясняет решение Конституционного суда Франции, согласно которому данный файл составлен только для облегчения идентификации и исследований лиц, совершивших определенные преступления, и не позволяет изучать генетические характеристики лиц, которые были объектом такого отбора[14]. На этом основании запрещено использовать кодирующую часть ДНК. Только пол подозреваемого может быть раскрыт следователям, другие элементы его личности (возраст, рост, вес, этническое происхождение, цвета глаз и т.п.) не должны определяться.

Однако есть несколько причин предполагать, что с учетом последних достижений в области генетики различие «кодирующей» и «некодирующей» частей ДНК стало менее заметно. Методы анализа ДНК быстро развиваются. По общему признанию, генетические характеристики, содержащиеся в «кодирующих» областях, сохраняются и используются только в медицинских целях или для научных исследований, тогда как генетические отпечатки пальцев, используемые полицией и правосудием, касаются только маркеров пола и идентификации. Однако развитие генетических методов привело к тому, что некоторые из сегментов, входящих в FNAEG, позволяют определять наследственные морфологические, физиологические, патологические, этнические и другие характеристики. Генетики продемонстрировали, что по крайней мере три из сегментов, зарегистрированных в FNAEG с самого начала, являются значимыми маркерами, поскольку они генетически связаны с генетическим заболеванием[15].

Эти открытия привели к тому, что Советом ЕС в 1997 г. было принято решение, что государства не должны больше использовать маркер при обмене результатами ДНК, если научная эволюция показала, что он содержит информацию о наследственных характеристиках. Кроме того, рекомендуется, чтобы государства-члены были готовы уничтожить результаты анализов ДНК, которые они получили, если окажется, что эти результаты включают информацию о конкретных наследственных характеристиках[16].

Таким образом, во всех странах Европейского Союза в настоящее время происходит обработка исключительно «некодирующих» частей ДНК. Именно этот вид информации может рассматриваться с позиций законодательства о персональных данных.

На основе «некодирующих» элементов ДНК создается генетический паспорт — документ, содержащий информацию о генетической индивидуальности человека. Содержащаяся в нем информация универсальна и достаточна для идентификации конкретного индивида. Молекулярно-генетическую экспертизу зачастую называют генетической дактилоскопией. Используемая в паспорте кодировка генетической информации не несет сведений о признаках человека, его физиологических и психических особенностях, а также о наследственных заболеваниях. Сверяя данные, полученные с помощью анализа любого биологического материала, с информацией, указанной в генетическом паспорте, специалист-генетик с точностью делает заключение о принадлежности биологического материала человеку, генетический паспорт которого подготовлен зара-

[12] Fichier national automatisé des empreintes génétiques (FNAEG) — Национальный автоматизированный файл генетических отпечатков пальцев.

[13] *Collignon N., Diamant-Berger O.* Le consentement aux empreintes génétiques en matière pénale // Médecine et Droit. 2000. № 42. P. 8.

[14] Conseil constitutionnel. Décision no2010-25 QPC. 16 septembre 2010.

[15] CCNE. Avis № 98 «Biométrie, données identifiantes et droits de l'homme».

[16] Résolution du Conseil du 9 juin 1997 relative à l'échange des résultats des analyses d'ADN.

нее[17]. Единственная проблема — это половая принадлежность индивида, т.к. при операциях по смене пола меняется только внешность, генетическая же половая принадлежность остается неизменной.

В России генетические исследования регулируются Федеральными законами от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»[18], от 5 июля 1996 г. № 86-ФЗ «О государственном регулировании в области генно-инженерной деятельности»[19] и от 3 декабря 2008 г. № 242-ФЗ «О государственной геномной регистрации в Российской Федерации»[20].

В настоящее время практически не урегулированной остается деятельность по получению и обработке ДНК-информации в случаях, не связанных с раскрытием и расследованием преступлений, т.е. вне рамок Федерального закона «О государственной геномной регистрации в Российской Федерации».

Отдельной задачей является правовое регулирование деятельности с применением ДНК-технологий при проведении в научных целях добровольных массовых ДНК-скринингов населения, стремительно развивающегося и таящего серьезные правовые проблемы исследования ДНК в медицинских целях[21] и иные виды генетических исследований.

Поэтому мы считаем, что необходима комплексная работа по правовому обеспечению деятельности, связанной с получением, обработкой, накоплением и дальнейшим использованием ДНК-информации, а также биологического материала государственными органами, научно-исследовательскими институтами и коммерческими организациями.

Итак, предпринятый анализ позволил сделать следующие выводы:

Во-первых, биометрические данные являются особым видом персональных данных. Для них должен быть установлен специальный правовой режим и регулирование.

Во-вторых, существующее много лет деление биометрии на «следовую» и «не следовую» теряет свое значение. Должна быть введена новая классификация: это выделение биометрии, которая оставляет цифровые следы (цифровую), и биометрии, которая не оставляет цифровые следы (аналоговую).

В-третьих, мы считаем, что именно цифровая биометрия нуждается в особом правовом регулировании, так как она наиболее уязвима. В этой связи нами разрабатывается концепция федерального закона «О защите биометрической информации физических лиц», которую мы в ближайшее время предоставим для обсуждения широкой общественности.

В-четвертых, генетическая информация в полной мере не соответствует понятию персональных данных, так как может относиться к неограниченному кругу лиц. Это определяет необходимость разработки специального закона «О генетической информации».

БИБЛИОГРАФИЯ

1. *Аюпова А. Р., Ахатов Р. Р.* Биометрический паспорт: зло или добро // Здоровый образ жизни как условие устойчивого развития государства : сборник материалов Всероссийской научно-практической конференции. — 2017. — С. 35—38.
2. *Кубитович С. Н.* ДНК как носитель информации неограниченного круга лиц // Вестник экономической безопасности. — 2017. — № 4. — С. 184—188.
3. *Михайлов М. А., Волеводз А. Г., Сидоренко Э. Л.* Международная научно-практическая конференция в Государственной Думе «Совершенствование системы дактилоскопической регистрации» // Библиотека криминалиста. Научный журнал. — 2016. — № 1 (24). — С. 368—378.

---

[17] *Попов В. В.* Идентификация личности молекулярно-генетическими методами // Юристъ-Правоведъ. 2018. № 3 (86). С. 169—175.

[18] СЗ РФ. 2011. № 48. Ст. 6724.

[19] СЗ РФ. 1996. № 28. Ст. 3348.

[20] СЗ РФ. 2008. № 49. Ст. 5740.

[21] Направления развития генетических исследований станут темой для обсуждения ведущих мировых экспертов на Втором международном саммите по редактированию генома человека, который стартует в Гонконге 27 ноября 2018 г.

4. *Попов В. В.* Идентификация личности молекулярно-генетическими методами // Юристъ-Правоведъ. — 2018. — № 3 (86). — С. 169—175.
5. *Соколов Ю. Н.* Электронный паспорт в уголовном судопроизводстве // Евразийский юридический журнал. — 2017. — № 4 (107). — С. 265—267.
6. *Фахреева Д. Р., Фахреев Н. Н.* Биометрический документ как элемент противодействия коррупции // Наука, техника и образование. — 2016. — № 3 (21). — С. 208—209.
7. *Collignon N., Diamant-Berger O.* Le consentement aux empreintes génétiques en matière pénale // Médecine et Droit. — 2000. — № 42. — P. 6—9.

Материал поступил в редакцию 4 декабря 2018 г.

BIOMETRICS IN THE CONTEXT OF PERSONAL DATA AND GENETIC INFORMATION: LEGAL ISSUES[22]

RASSOLOV Ilya Mikhailovich, Doctor of Law, Acting Head of the Department of Information Law and Digital Technologies of the Kutafin Moscow State Law University (MSAL)
ilyarassolov@mail.ru
125993, Russia, Moscow, ul. Sadovaya-Kudrinskaya, d. 9

CHUBUKOVA Svetlana Georgievna, PhD in Law, Associate Professor of the Department of Information Law and Digital Technologies of the Kutafin Moscow State Law University (MSAL)
sgchubukova@msal.ru
125993, Russia, Moscow, ul. Sadovaya-Kudrinskaya, d. 9

MIKUROVA Irina Vladimirovna, PhD in Law, Associate Professor of the Department of Public Law Disciplines and Criminal Law Disciplines of the Plekhanov Russian University of Economics "Plekanov Russian University of Economics"
fille-en-rouge@yandex.ru
117997, Russia, Moscow, Stremyanny pereulok, d. 36

Abstract. *In modern society, methods of identification of persons on the basis of their physical, biological or behavioral characteristics are actively developing. European countries are in the process of developing a holistic doctrine on biometric control and are clarifying their position on situations where biometric data are used by individuals.*
From the position of information law, the paper presents a new author's approach to the problem of processing biometric data and genetic information. The division of biometrics into "trace" and "non-trace" is losing its meaning. A new classification of biometrics into digital and analog is proposed.
Biometric access control should not become a routine phenomenon in the framework of the organization of the company and without any reason to replace other existing types of control. The interested person can be entrusted with the storage of their own biometric data to reduce the risks of leakage and the consequences of exposure to them. Biometric data must be stored on the company's servers in encrypted form, which makes it impossible to use them without the consent of the person concerned.
Biometric data should be protected by a special legal regime. The analysis of the European and Russian legislation made it possible to draw the following conclusions: biometric data is a special type of personal data, a special legal regime and regulation should be established; digital biometrics needs special legal regulation, since it is the most vulnerable type; genetic information does not fully correspond to the concept of personal data, as it can relate to an unlimited number of persons. This determines the need to develop a special law "on genetic information".

Keywords: *information, information law, biometrics, biometric data, digital biometrics, biometric control, DNA, genetic information, personal data, face identification.*

[22] The study is performed with the financial support of RFBR, research project No. 18-29-14033.

REFERENCES

1. Ayupova A.R., Akhatov R.R. *Biometricheskiy pasport: zlo ili dobro* [Biometric passport: evil or good]. Zdorovyy obraz zhizni kak uslovie ustoychivogo razvitiya gosudarstva: sbornik materialov vserossiyskoy nauchno-prakticheskoy konferentsii [Healthy lifestyle as a condition of sustainable development of the state: Proc. All-Russian Scientific and Practical conference]. 2017. Pp. 35—38.
2. Kubitovich S.N. *DNK kak nositel informatsii neogranichennogo kruga lits* [DNA as an information carrier unlimited]. *Vestnik ekonomicheskoy bezopasnosti* [Bulletin of Economic Security]. 2017. No. 4. Pp. 184—188.
3. Mikhailov M.A., Volevodz A.G., Sidorenko E.L. Mezhdunarodnaya nauchno-prakticheskaya konferentsiya v Gosudarstvennoy Dume «Sovershenstvovanie sistemy daktiloskopicheskoy registratsii» [International Scientific and Practical Conference in the State Duma "Improving the System of Fingerprint Registration"]. *Biblioteka kriminalista. Nauchnyy zhurnal* [Criminalist's Library Scientific Journal]. 2016. No. 1 (24). Pp. 368—378.
4. Popov V.V. Identifikatsiya lichnosti molekulyarno-geneticheskimi metodami [Identification of personality by molecular genetic methods]. 2018. No. 3 (86). Yurist-Pravoved [Jurist]. Pp. 169—175.
5. Sokolov Yu.N. *Elektronnyy pasport v ugolovnom sudoproizvodstve* [Electronic passport in criminal proceedings]. *Evraziyskiy yuridicheskiy zhurnal* [Eurasian Law Journal]. 2017. No. 4 (107). Pp. 265—267.
6. Fakhreeva D.R., Fakhreev N.N. *Biometricheskiy dokument kak element protivodeystviya korruptsii* [Biometric document as an element of corruption]. *Nauka, tekhnika i obrazovanie* [Science, technology and education]. 2016. No. 3 (21). Pp. 208—209.
7. Collignon N., Diamant-Berger O. Le consentement aux empreintes génétiques en matière pénale. Médecine et Droit. 2000. No. 42. Pp. 6-9.