Вестник РУДН. Серия: Юридические науки 2025 Т. 29. № 4. 981–994
RUDN JOURNAL OF LAW. ISSN 2313-2337 (Print), ISSN 2408-9001 (Online) http://journals.rudn.ru/law

https://doi.org/10.22363/2313-2337-2025-29-4-981-994
EDN: LNXXGQ

Научная статья / Research Article

Биометрические данные как средство удаленной идентификации человека

Д.С. Запорожцев

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации, *г. Москва, Российская Федерация*
✉ dmitriaugust@yandex.ru

Аннотация. Цель работы – исследование биометрических данных в качестве инструмента удаленной идентификации личности человека. Биометрические данные (голосовые данные, отпечатки пальцев, сканирование сетчатки глаза и иные материалы) характеризуются особой значимостью, так как позволяют с высокой степенью точности установить личность человека, что обуславливает актуальность выбранной темы исследования. Рассматриваются правовые аспекты понятия «биометрические данные», основы их использования, преимущества и недостатки такого использования в целях анализа специфики использования биометрических данных как средства удаленной идентификации. Сделан вывод о необходимости доработки положений действующего законодательства посредством унификации и детализации понятийного аппарата, позволяющей построить четкие взаимосвязи между используемыми в правовом регулировании понятиями биометрических персональных данных, удаленной идентификации и аутентификации соответствующей сферы правового регулирования.

Ключевые слова: биометрические персональные данные, конфиденциальность биометрических данных, персональные данные, защита персональных данных

Конфликт интересов. Автор заявляет об отсутствии конфликта интересов.

Поступила в редакцию: 07 июля 2024 г.
Принята к печати: 15 октября 2025 г.

Для цитирования:

Запорожцев Д.С. Биометрические данные как средство удаленной идентификации человека // RUDN Journal of Law. 2025. Т. 29. № 4. С. 981–994. https://doi.org/10.22363/2313-2337-2025-29-4-981-994

Biometric data as a tool for remote personal identification

Dmitry S. Zaporozhtsev ✉

Ministry of Digital Development, Communications and Mass Media
of the Russian Federation, *Moscow, Russian Federation*
✉ dmitriaugust@yandex.ru

Abstract. The article examines biometric data as a tool for remote identification. Biometric data, including voice recording, fingerprints, retinal scans, and otheridentities, hold special significance because they enable the accurate establishment of a person's identity, undersoring the relevance of this research topic. The author analyzes legal aspects of the concept of "biometric data", principles governing their use, and the advantages and disadvantages of such applications to explore the specifics of employing biometric data for remote identification. The article concludes that current legislation needs refinement through unification and clarification of key conceptual terms. This would enable cleaeter delineation among the concepts of biometric personal data as used in legal regulation, remote identification, authentication, and the pertinent areas of legal governance.

Key words: biometric personal data, biometric data privacy, personal data, personal data protection
Conflict of interest. The author declares no conflict of interest.

Received: 07th July 2024
Accepted: 15th October 2025

For citation:

Zaporozhtsev, D.S. (2025) Biometric data as a tool for remote personal identification. *RUDN Journal of Law.* 29 (4), 981–994. (in Russian). https://doi.org/10.22363/2313-2337-2025-29-4-981-994

Введение

Проблема контроля и информационной безопасности персональных данных является важным условием эффективности правового регулирования данной сферы. Так, биометрические персональные данные активно используются в рамках удаленной идентификации. Биометрическая идентификация считается одним из самых безопасных методов идентификации личности, что связано с ее высоким уровнем точности и способностью гарантировать присутствие верифицируемого лица.

С развитием технологий и повсеместным использованием цифровых систем все большее количество людей сталкивается с необходимостью защиты своих персональных данных и иной личной информации от киберпреступности. В этой связи биометрические данные становятся надежным и удобным средством идентификации личности человека. Представляя собой уникальные физиологические и поведенческие характеристики человека, биометрические данные служат в качестве уникального «цифрового отпечатка» каждого человека и позволяют провести идентификацию личности на расстоянии.

Одним из наиболее актуальных исследований в области биометрии является разработка систем удаленной идентификации человека на основе его «цифрового отпечатка». Такие системы позволяют ускорить процесс идентификации и обеспечить высокий уровень безопасности при доступе к различным информационным ресурсам. Кроме того, использование биометрических данных в целях идентификации человека позволяет снизить риски мошенничества и кражи личной информации.

Исследование биометрических данных как средства удаленной идентификации человека имеет огромный потенциал для различных отраслей, в особенности цифровой экономики. Развитие таких технологий позволит создать удобные и безопасные условия для повседневной жизни людей и защитить их личные данные от несанкционированного доступа. Таким образом, актуальность выбранной темы исследования неоспорима. Развитие и совершенствование технологий, позволяющих осуществлять идентификацию личности на расстоянии, играют ключевую роль в обеспечении безопасности и защиты личной информации в цифровом мире от недобросовестного завладения ею иными лицами.

Цель работы – исследование биометрических данных в качестве инструмента удаленной идентификации личности человека. Начнем изучение обозначенных аспектов с вопросов определения биометрических данных и нормативно-правовой базы, регламентирующей порядок оборота такой информации в социально-экономических сферах.

Понятие биометрических данных и правовые основы регламентации их использования

В современном мире биометрические данные все чаще используются в различных сферах деятельности, таких как безопасность, медицина, банковское дело, государственное управление, туризм и иные. Однако использование биометрических данных вызывает ряд вопросов, связанных с правовым обращением такой информации, доступом к данной информации со стороны третьих лиц, и требует строгого регулирования в целях защиты личных данных граждан и предотвращения злоупотребления в части использования личной информации о них.

Упоминание о биометрических данных содержится в ГОСТ Р ИСО/ТО 13569-2007, согласно которому биометрические данные (biometric) представляют собой измеримую биологическую или поведенческую характеристику, с достоверностью отличающую одного человека от другого, используемую для установления либо подтверждения личности человека[1] (п. 3.11).

Вместе с тем поведенческие характеристики отнесены ГОСТ ISO/IEC 19794-1-2015 к биологическим данным, который регламентирует возможность фиксации таких данных посредством регистрации и их дальнейшее использование для распознавания личности в автоматизированном режиме[2]. Таким образом, с помощью биометрических данных устанавливается идентификация личности (согласно ГОСТ Р ИСО/ТО 13569-2007 п. 3.8).

Исследуя дефиницию понятия «биометрические данные» следует обратиться к положениям действующего российского законодательства.

[1] ГОСТ Р ИСО/ТО 13569-2007. Национальный стандарт Российской Федерации. Финансовые услуги. Рекомендации по информационной безопасности (утв. Приказом Ростехрегулирования от 27.12.2007 № 514-ст). Режим доступа: https://cloud.consultant.ru/cloud/cgi/online.cgi?req=doc&base=OTN&n=24672&cacheid=3C19D227E8D4A27D082F2953BC3E0F00&mode=splus&rnd=1Uw8ug#g4fzM7URVefS7RtU (дата обращения: 14.03.2024).

[2] ГОСТ ISO/IEC 19794-1-2015. Межгосударственный стандарт. Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 1. Структура» (введен в действие Приказом Росстандарта от 20.11.2015 № 1928-ст). М. : Стандартинформ, 2016.

В свою очередь особая охрана и отдельная регламентация на территории России обеспечивается биометрическим данным, выступающим частью персональных данных. Соответствующее положение содержит Федеральный закон «О персональных данных», в части 1 статьи 11 которого установлено, что «биометрические персональные данные – сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных»[3].

Федеральный закон «О государственной геномной регистрации в Российской Федерации» в п. 3 ст. 1 содержит указание на то, что геномная информация относится к персональным данным[4].

Федеральный закон «О государственной дактилоскопической регистрации в Российской Федерации» в статье 1 аналогичным образом относит дактилоскопическую информацию к категории биометрических персональных данных[5].

Руководствуясь приведенными положениями, можно резюмировать, что законодательством России провозглашается охрана биометрических данных, отнесенных к категории персональных данных, под которыми понимаются лишь физиологические и биологические особенности человека: вес, рост, ДНК, данные дактилоскопии и прочие аналогичные характеристики.

Определение демонстрирует отсутствие отнесения поведенческих характеристик с охраняемой персональной биологической информации.

Кроме того, отнесение поведенческих характеристик к биологическим персональным данным распространено за рубежом (Galiullina, 2015). В частности, законодательство Аргентины и Хорватии содержит нормативную регламентацию поведенческих характеристик человека, выражающихся в динамических, подсознательных двигательных активностях[6].

Как следствие, определение, отраженное в Федеральном законе «О персональных данных», является, на наш взгляд, неполным, требующим доработки посредством дополнения перечня охраняемых биологических персональных данных поведенческими характеристиками человека.

В юридической литературе также распространена точка зрения о несовершенстве имеющейся дефиниции биометрических персональных данных в Федеральном законе «О персональных данных». Так, по мнению Г.Г. Камаловой, в утвержденной формулировке имеется логическая ошибка ввиду того, что физиологические свойства (физиология) выступают частью биологии (Kamalova, 2016).

Принимая во внимание отраслевую специфику понятийного аппарата, а также нацеленность законодателя на разграничение биологических характеристик, используемых в целях идентификации личности, позволим воздержаться от критики и поддержки приведенной точки зрения, так как считаем, что подобная тонкость не влияет

[3] Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных // Собрание законодательства Российской Федерации. 2006. № 31 (1 ч.), ст. 3451.

[4] Федеральный закон от 03.12.2008 № 242-ФЗ «О государственной геномной регистрации в Российской Федерации» // Собрание законодательства Российской Федерации. 2008. № 49, ст. 5740.

[5] Федеральный закон от 25.07.1998 № 128-ФЗ «О государственной дактилоскопической регистрации в Российской Федерации» // Собрание законодательства Российской Федерации. 1998. № 31, ст. 3806.

[6] Ley de de los datos personales de Argentina 25.326. sancionada: Octubre 4 de 2000. Available from: http://www.justicia2020.gob.ar [Accessed 14th March 2024].

на специфику применения положений Федерального закона «О персональных данных» к отношениям, складывающимся ввиду обращения биологической персональной информации.

Как следствие, несовершенство закрепленной правовой дефиниции понятия биометрических персональных данных создает определенный пробел в законодательстве, а также влечет неблагоприятные последствия для субъекта персональных данных, о чем детальнее далее также пойдет речь в настоящей статье.

Наглядно продемонстрировано несовпадение определений, содержащихся в рассмотренных выше федеральных законах, несмотря на то что указанные акты выступают отправной точной для иных подзаконных актов.

Так, в частности, в нормативном правовом акте[7] установлено, что именоваться в качестве информационной системы по обработке персональных биометрических данных может та, в которой осуществляется обработка сведений, характеризующих физиологические и биологические свойства личности, позволяющие ее идентифицировать.

На территории Европейского союза регулирование обработки биометрических данных осуществляется в соответствии с документом о защите персональных данных[8].

Учитывая, что нормативно-правовая база не должна создавать угрозу конфиденциальности персональных биологических данных, а, напротив, должна обеспечивать максимальные гарантии безопасности и защиты личных данных человека от вмешательства со стороны иных лиц (Hall, 2014).

В качестве признаков, позволяющих отличать биологические персональные данные от иных данных, выделяют уникальность, что предполагает неповторимость такой информации (радужная оболочка глаза, отпечатки пальцев), универсальность, обуславливаемая наличием биологических характеристик у каждого человека, и неизменяемость биологических данных (Smirnova, 2022).

Последний признак является достаточно спорным, так как отдельные биоданные (поведенческие характеристики или физиологические особенности) со временем могут изменяться.

Необходимо отметить, что нормативное национальное регулирование на международном уровне использования биометрических данных также регламентируется утверждаемыми стандартами и рекомендациями международных организаций. Например, Международная организация по стандартизации (ISO) разрабатывает стандарты по обработке биометрических данных, позволяющих реализовать их использование на территории различных стран в целях обеспечения надлежащего уровня защиты данных[9].

---

[7] Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // Собрание законодательства Российской Федерации. 2012. № 45, ст. 6257.

[8] Регламент Европейского парламента и Совета Европейского союза 2016/679 от 27 апреля 2016 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных / General Data Protection Regulation /GDPR). Режим доступа: https://base.garant.ru/71936226/#friends (дата обращения: 14.03.2024).

[9] Горелишвили Д. Постатейный комментарий к проекту Закона России «О персональных данных». Режим доступа: http://www.kongord.ru/Index/A_tma_05/DGorpersdatcom.html (дата обращения: 13.03.2024).

Важным аспектом в регулировании процесса использования биометрических данных является обеспечение их безопасности. Для обеспечения безопасности данных необходимы соответствующие технические и организационные меры. В данном контексте особенно важным видится полная правовая регламентация обработки и хранения биологических персональных данных, где первоочередным этапом выступает закрепление единой унифицированной дефиниции персональных биологических данных, посредством их определения как информации, определяющей уникальные физиологические, биологические и поведенческие характеристики человека, которые могут быть использованы в целях его идентификации.

Биометрические данные как средство удаленной идентификации личности

Современный мир требует от индивида постоянной готовности к внешним прогрессирующим изменениям, в качестве которых выступает в том числе возможность удаленной идентификации личности в различных сферах деятельности на основе современных технологичных разработок. Идентификация личности необходима для получения доступа к компьютерным информационным системам, прохождения паспортного контроля или даже в целях доступа лица к его рабочему месту. Такая необходимость определяет актуальность вопросов удаленной идентификации личности, обеспечения безопасного процесса идентификации, а также важность правовой регламентации процесса идентификации как для отдельных организаций внутри одной страны, так и для целых государств при взаимодействии друг с другом.

Одним из инструментов идентификации личности выступают биометрические данные. Использование биометрических данных имеет особую значимость при удаленной идентификации личности. Что же представляет собой удаленная идентификация?

Под удаленной идентификацией личности следует понимать процесс установления и подтверждения физического лица с применением специальных технических средств. Данный метод идентификации применим в различных сферах деятельности, где необходимо осуществлять проверку личности субъекта.

В свою очередь нормативная регламентация удаленной идентификации не содержит дефиниции указанного понятия. Анализируя действующую нормативно-правовую базу, можно сделать вывод, что термин «идентификация» не является универсальным. Содержание Федеральных законов «О персональных данных», «Об информации, информационных технологиях и защите информации»[10] не раскрывает существа рассматриваемого термина, несмотря на то, что именно данные правовые акты выступают основными в сфере регламентации сбора, обработки и дальнейшего использования информации, в том числе биометрической, а также в своем тексе содержат ссылки на термин «идентификация».

В научной литературе, в частности Т.А. Поляковой и Н.Б. Наумовым, отмечалось, что подобная ситуация с понятийным аппаратом представляет собой ограниченную терминологическую базу, нуждающуюся в развитии и усовершенствовании (Naumov & Polyakova, 2016).

Неясность правовых формулировок, их неполнота или расхождение приводят к появлению в законодательстве все большего количества новых дефиниций одного и

[10] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации. 2006. N 31 (1 ч.), ст. 3448.

того же понятия, конкретизирующего его для конкретной отрасли применения, что, в конечном итоге, создает угрозу двойственного правового регулирования, правовых противоречий и приводит к неверному использованию нормативных положений к однородным правоотношениям в процессе правоприменения уполномоченным субъектом.

Вывод, к которому можно прийти после ознакомления с указанными выше правовыми актами, заключается в понимании идентификации в виде процесса установления личности лица посредством совершения определенной совокупности действий по установлению признаков идентифицируемого субъекта.

В настоящее время удаленная идентификация становится все более популярной ввиду стремительно развивающегося процесса глобализации, развития цифровых технологий и интернета и упрощает достаточно большое количество взаимодействия субъекта с иными субъектами правоотношений (Khisamov, 2018).

В определенных условиях, в частности, при пандемии, удаленная идентификация выступала единственным средством, позволяющим получить населению необходимые государственные услуги (Salikhov, 2021).

Особую популярность приобретает интернет-банкинг (дистанционное банковское обслуживание), в рамках которого клиенты банка могут совершать удаленно различные операции. Для обеспечения безопасности проводимых операций банки должны надлежащим образом идентифицировать своих клиентов на расстоянии, надлежащая идентификация позволяет предотвратить мошеннические действия при совершении манипуляций с денежными средствами при проведении денежных операций в удаленном режиме (Kucherov & Sinitsyn, 2022).

По данным прогноза J'son & Partners Consulting, «применение биометрических технологий в банковской сфере, а именно открытие и ведение банковских счетов, заключение кредитных договоров, применение биометрических платежных систем, будет происходить наиболее высокими темпами по сравнению с другими отраслями финтеха» (Ruchkina, 2017).

Анализ судебной практики позволяет сделать вывод превалирующей позиции кредитных организаций. Особое распространение получили дела с требованием клиентов о взыскании денежных средств с банковских организаций по финансовым операциям ввиду отсутствия согласия клиента на совершение таких операций, в частности, относительно переводов средств с расчетных счетов клиентов.

По указанной категории дел банки отстаивают свою позицию, ссылаясь на подключение клиента к электронной системе с использованием пароля для входа, являющееся основанием для предоставления услуг банком. Обязанность по хранению пароля и недопущения к нему доступа со стороны третьих лиц возложена на клиента. При проведении успешной идентификации клиента в удаленном режиме распоряжения клиента считаются отправленными от имени клиента и имеют равную юридическую и доказательственную силу.

Судебные органы, руководствуясь вышеизложенным, принимают сторону кредитных организаций, указывая, что обязанности банка по договору были выполнены надлежащим образом, и у банка отсутствовали основания для неисполнения распоряжения клиента о переводе денежных средств[11].

[11] См., например: Апелляционное определение Московского городского суда от 6 июня 2017 г. по делу № 33-21663/2017; Апелляционное определение Московского городского суда от 12 июля 2016 г. по делу № 33-6988/2016; Апелляционное определение Московского городского суда от 14 декабря 2017 г. по делу № 33-50810/2017; Апелляционное определение Московского городского суда от 18 октября 2017 г.

Подобная практика свидетельствует о серьезной проблеме удаленной идентификации без использования биометрической информации, а также о необходимости ее серьезной доработки и совершенствовании (Sinitsyn, 2021). В свою очередь, применение биометрической информации, на наш взгляд, в рассматриваемых случаях позволило бы исключить фактически несанкционированные со стороны клиента распоряжения в удаленном режиме на проведение банком денежных операций по принадлежащим клиенту счетам.

Еще одним ярким примером использования удаленной биометрической идентификации выступает разработка ПАО «Сбербанк», реализованная совместно с сетью продуктовых магазинов «Азбука вкуса», позволяющая использовать отпечатки пальцев для совершения оплаты товаров. В рамках реализации разработки магазины были оборудованы специальными терминалами, считывающими биометрические данные субъекта в целях оплаты покупаемой продукции (Bochkov, 2019).

Практическое воплощение указанной разработки, позволяющей удаленно идентифицировать субъекта с помощью его биометрических данных, стало возможным благодаря Единой биометрической системе. Система была создана компанией ПАО «Ростелеком», а инициатором ее создания выступили Министерство связи и массовых коммуникаций РФ, а также Центральный банк РФ. Единая биометрическая система представляет собой базу биометрических данных лиц, с помощью которых последние имеют возможность получать доступ к банковским услугам удаленно (Bochkov, 2019).

Алгоритм работы с вышеуказанной системой предполагает четкое соблюдение правил, изложенных как в федеральной нормативно-правовой базе (вышеупомянутого Федерального закона «О персональных данных», актов Правительства РФ и иных НПА), так и в локальных актах, принимаемых на уровне отдельных корпораций (в качестве таковых выступают внутренние документы организаций – публичные оферты, стандарты обработки данных, положения об обработке данных, формы согласия субъектов на обработку, иные профильные соглашения и правила). Ознакомление с подобной документацией на примере ПАО «Ростелеком», размещенной на официальном сайте организации, позволяет сделать вывод о следующем.

Пределы ответственности за нарушения в сфере обработки биометрических данных для сторон не идентичны, варьируются, не конкретизированы. По внутренней документации ПАО «Ростелеком» сторона, нарушавшая условия соглашения об оказании услуги по сбору биометрических данных и их передаче в единую биометрическую систему, возмещает другой стороне убытки. В свою очередь заказчик освобождается от ответственности перед исполнителем за потерю таких данных при любых ситуациях[12].

по делу № 33-42183/2017; Апелляционное определение Московского городского суда от 6 сентября 2017 г. по делу № 33-35595/2017. Режим доступа:https://cloud.consultant.ru/cloud/cgi/online.cgi?req=card&rnd=Q3w7zQ&div=ARB#div/ (дата обращения: 14.03.2024).

[12] Публичная оферта. О заключении соглашения об оказании услуги по сбору биометрических данных и их передачи в Единую биометрическую систему ПАО «Ростелеком». Режим доступа: https://bio.rt.ru/upload/iblock/7b7/Publichnaya-oferta-o-zaklyuchenii-soglasheniya-ob-okazaniiuslugi-posboru-biometricheskikh-dannykh-i-ikhperedache-v-Edinuyu-biometricheskuyu-sistemu.pdf (дата обращения: 01.05.2024).

Анализ информации и локальной документации на примере ПАО «Сбербанк», ПАО «ВТБ»[13], АО «Почта Банк»[14], размещенной на официальном сайте банка, позволил сделать вывод об отсутствии отдельного правового документа, устанавливающего понятие биометрических данных, принципы работы с ними, а также ответственность за нарушения при работе с такими данными[15].

Думается, что настоящая ситуация является упущением. Каждый субъект вправе осуществлять оценку возможных рисков вмешательства в его биометрику, для чего он должен быть достаточно осведомлен, в том числе посредством ознакомления с локальной документацией отраслевых компаний.

Четкий и исчерпывающий перечень действий в рамках требований не прописан, и специалист получает определенную свободу действий при решении вопросов, связанных с устранением угрозы безопасности обрабатываемой информации. Возникает вопрос о том, сможет ли ответственный специалист в конкретном случае действительно выбрать наиболее правильное решение сложившейся проблемы?

К сожалению, на практике зачастую многим не хватает необходимого опыта и навыков, что по итогу приводит к утечке охраняемой персональной биометрической информации.

Более того, также возникает вопрос, связанный с тем, вовремя ли специалист осознает, что появилась угроза именно для персональных биометрических данных, и что понимать под такими данными, если ни на законодательном уровне, ни на уровне локальных правовых актов четкая и полная дефиниция биометрических данных на сегодняшний день не определена.

Можно резюмировать, что специалист в отдельном случае может и не понимать необходимость отнесения определенной информации к категории охраняемых персональных биологических данных. В данном аспекте невольно возвращаемся к проблематике отсутствия единого универсального понятия биометрических персональных данных в действующем законодательстве Российской Федерации.

Еще одним примером использования удаленной идентификации выступает обучение в режиме онлайн. На сегодняшний день большое количество образовательных учреждений как общего, так и среднего и высшего образования предлагают онлайн обучение, где обучающиеся имеют возможность получить новые знания и навыки, не покидая дом.

Для обеспечения безопасности при подтверждении личности обучающихся многие образовательные учреждения используют методы удаленной идентификации, позволяющие удостовериться, что студент сдает экзамен самостоятельно. Однако в основном в качестве методов используется предоставление паролей и других уникальных данных, позволяющих осуществить лицу в режиме онлайн вход в ту или иную информационную систему/образовательную платформу.

Вместе с тем данный алгоритм взаимодействия не исключает предоставление обучающимся таких данных иным лицам в целях совершения от его имени действий, направленных на прохождение тестирований и испытаний, предусмотренных

[13] Правила комплексного обслуживания физических лиц в Банке ВТБ (ПАО). Режим доступа: vtbrussia.ru (дата обращения: 01.12.2024).

[14] Официальный сайт АО «Почта Банк» Режим доступа: https://www.pochtabank.ru/service/ebs (дата обращения: 01.12.2024).

[15] Официальный сайт ПАО «Сбербанк». Биометрия в Сбербанке. Режим доступа: https://www.sberbank.ru/ru/person/dist_services/bio(дата обращения: 01.05.2024).

образовательной программой. Именно в данном аспекте следует говорить о необходимости более широкого внедрения системы удаленной идентификации с использованием биометрических данных в рассматриваемой сфере.

Кроме того, удаленная идентификация может быть использована в сфере здравоохранения. В целях подтверждения факта, что перед врачом удаленно на связи именно тот пациент, с которым он взаимодействует, врач может использовать методы удаленной идентификации, что позволит сократить время на определенные процедуры и обслуживание пациентов, а также решить многие проблемы без физического посещения больницы со стороны субъекта.

Преимуществом биометрической идентификации является ее удобство, так как пользователю не нужно запоминать сложные пароли или носить с собой ключи – достаточно просто просканировать свои биометрические данные в целях получения доступа к нужному ресурсу. Программа осуществляет действия в пределах заданного алгоритма и представляет собой «закон компьютерного кода» (Truntsevsky, 2020).

Сказанное обуславливает быстроту, удобство и эффективность процесса. Вместе с тем, наряду с рассмотренными преимуществами и возможными сферами применения биометрической идентификации, данный процесс имеет и ряд недостатков.

Основным риском при использовании биометрических данных личности является неправомерный доступ к личным данным. В случае определения хищения биометрических данных, человек может столкнуться с серьезными проблемами ввиду доступа злоумышленников к его личной информации и совершения от его имени различных финансовых операций.

Еще в качестве одного из рисков использования биометрической идентификации полагаем необходимым отметить сбои в работе соответствующих информационных систем или их недостаточная доработка, обуславливающая возможность подделки биометрических данных с помощью иных специальных устройств.

Указанное означает, что даже самые передовые биометрические системы не могут быть полностью надежными и безопасными на сегодняшний день.

Нельзя не отметить, что на сегодняшний день в литературе неоднократно освещены вопросы рисков удаленной идентификации и все они в основном сводятся к несовершенству технологичных процессов, приводящему к утечке данных.

Думается, что в качестве отдельного самостоятельного риска следует выделять отсутствие четкой и полной дефиниции персональных данных на федеральном правовом уровне, а также отсутствие конкретизации в положениях об ответственности уполномоченных субъектов на локальном уровне организаций за нарушения, допущенные при работе с биометрическими персональными данными.

В рамках рассматриваемых выше примеров можно убедиться, что подобные правовые пробелы и противоречия не меньшим образом создают угрозу для утечки персональных биоданных как и при сбоях в работе информационных систем или несовершенстве соответствующего информационного обеспечения.

Однако в целом, несмотря на возможные риски, использование биометрических данных для идентификации личности имеет большие перспективы и может принести пользу обществу, ведь процесс удаленной идентификации обеспечивает высокий уровень безопасности и удобства совершения отдельных операций с использованием информационных систем, а также способствует повышению эффективности работы многих организаций и государственных структур.

Учитывая необходимость дальнейшего развития и разработок информационных ресурсов, участвующих в хранении и обработке биометрических данных и позволяющих осуществить удаленную идентификацию личности, для наиболее полного и эффективного использования биометрических технологий необходимо уделять особое внимание вопросам безопасности и конфиденциальности личной информации граждан. Государство обязано строго контролировать порядок обращения и доступа к биометрическим данным со стороны иных субъектов, обеспечивать защиту таких данных на всех этапах их использования (Krivogin, 2017).

Кроме того, завершая анализ рассматриваемых вопросов, нельзя не отметить, что в настоящее время, учитывая многоаспектность и многогранность существующих правовых отношений, нормативно-правовая база России должна отвечать ряду требований, среди которых особо, на наш взгляд, должны быть выделены следующие:

– универсальность, как критерий релевантности к стремительно развивающимся технологическим процессам;

– системность, позволяющая упорядочить нормативное регулирование, начиная непосредственно с правовых норм, а также устранить противоречие правовых норм.

Учитывая указанные свойства правовые дефиниции в сфере обработки биометрических персональных данных требуют доработки посредством унификации и детализации понятийного аппарата, а также иными определениями соответствующей сферы правового регулирования.

Заключение

На основании вышеизложенного материала необходимо резюмировать, что благодаря уникальности биологических данных и неизменности отдельных параметров такой информации возможность ошибочной идентификации сводится к нулю, что делает биометрические данные одним из самых безопасных способов идентификации личности.

Вместе с тем использование биометрических данных в качестве средства удаленной идентификации вызывает определенные риски и опасения, так как существует вероятность неправомерного доступа к таким данным и их незаконного использования третьими лицами в корыстных целях.

Указанное обуславливает повышенное внимание к обработке персональных биологических данных, стимулируя как законодателя, так и субъекта, осуществляющего непосредственную обработку персональных данных, поэтому возрастает активное внедрение и применение современных технологий шифрования и защиты информационных ресурсов. Именно отсутствие профильного универсального понятийного аппарата в рассматриваемой правовой сфере также создает угрозу обеспечения прав и свобод в правовом регулировании.

Для недопущения подобных нарушений при обработке персональных биометрических данных на территории Российской Федерации предлагается заимствовать опыт Аргентины и Хорватии, где в законодательстве имеется нормативная регламентация поведенческих характеристик человека, выражающихся в динамических, подсознательных двигательных активностях, относимых к биометрическим персональным данным.

Следующим этапом должно стать приведение в соответствие вышеуказанному определению всех используемых аналогичных дефиниций в иных подзаконных нормативно-правовых актах, применяемых на территории России.

Кроме того, для снижения рисков допущения субъектами обработки персональных биометрических данных нарушений гарантий защиты конфиденциальности и безопасности указанных данных на практике в положениях Федерального закона «О персональных данных» требуется закрепление специальной нормы для уполномоченного на обработку, использование и хранение персональной биометрической информации субъекта, закрепляющей для него обязанность на локальном уровне разработки самостоятельного профильного положения или стандарта, посвященного исключительно работе с биометрической информацией.

Подобные меры позволят устранить недостаточность четкого и полного определения биометрических персональных данных может также снизят вероятность снижения гарантий защиты конфиденциальности и безопасности указанных данных на практике.

Таким образом, для четкой и всесторонней регламентации правовых отношений законодательство должно обеспечивать ясность и полноту содержащихся в нем формулировок. При необеспечении четкости правил использования новых технологий, используемых при обработке биометрической информации, приводит к злоупотреблениям со стороны третьих лиц, распространению личной информации субъектов без их согласия и уязвимости протекающих информационных процессов.

В целом, биометрические технологии представляют собой инновационный и перспективный способ идентификации личности, который в ближайшем будущем может стать стандартом в области безопасности и защиты информации. Дальнейшее совершенствование технологий использования биометрической информации при проведении удаленной идентификации, строгое и неукоснительное соблюдение принципов конфиденциальности способствуют созданию безопасного удобного цифрового общества как в рамках территории одного государства, так и в контексте межгосударственного общественного взаимодействия.

References / Список литературы

Bochkov, E.S. (2019) On the legal regulation of biometric identification in banking. *Banking law.* (4), 7–14. (in Russian). https://www.doi.org/10.18572/1812-3945-2019-4-7-14 EDN: GEIWXM.

Бочков Е.С. К вопросу о правовом регулировании биометрической идентификации в банковской деятельности // Банковское право. 2019. № 4. С. 7–14. https://www.doi.org/10.18572/1812-3945-2019-4-7-14. EDN: GEIWXM.

Galiullina, D.R. (2015) Biometric personal data. *Document. Archive. History. Modernity*. (15), 264–268. (in Russian). EDN: UIKMAT.

Галиуллина Д.Р. Биометрические персональные данные // Документ. Архив. История. Современность. 2015. № 15. С. 264–268. EDN: UIKMAT.

Hall, T.S. (2014) The Quantified Self Movement: Legal Challenges and Benefits of Personal Biometric Data Tracking. *Akron Intellectual Property Journal.* 7 (1): 3.

Kamalova, G.G. (2016) Biometric personal data: Definition and nature. *Information Law.* (3), 8–12. (in Russian). EDN: WTQNDV.

Камалова Г.Г. Биометрические персональные данные: определение и сущность // Информационное право. 2016. № 3. С. 8–12. EDN: WTQNDV.

Kashkin, S.Y. & Pokrovskiy A.V. (2019) Artificial intelligence, robotics and protection of human rights in the European Union. *Bulletin of the O.E. Kutafin Moscow State Law University (MSAL).* (4 (56)), 64–90. (in Russian). https://doi.org/10.17803/2311-5998.2019.56.4.064-090 EDN: MZYMUX.

Кашкин С.Ю., Покровский А.В. Искусственный интеллект, робототехника и защита прав человека в Европейском союзе // Вестник Университета имени О.Е. Кутафина (МГЮА). 2019. № 4 (56). С. 64–90. https://doi.org/10.17803/2311-5998.2019.56.4.064-090 EDN: MZYMUX.

Krivogin, M.S. (2017) Peculiarities of legal regulation of biometric personal data. *Law. Journal of the Higher School of Economics.* (2), 80–89. (in Russian). https://doi.org/10.17323/2072-8166.2017.2.80.89

Кривогин М.С. Особенности правового регулирования биометрических персональных данных // Право. Журнал Высшей школы экономики. 2017. № 2. С. 80–89. https://www.doi.org/10.17323/2072-8166.2017.2.80.89

Makarchuk, N.V. (2019) Public law limitations of use of digital assets and technologies. *Law and Business.* (1), 40–43. (in Russian). EDN: YYRNDV.

Макарчук Н.В. Публично-правовые ограничения использования цифровых активов и технологий // Право и Бизнес. 2019. № 1. С. 40–43. EDN: YYRNDV.

Naumov, V.B. & Polyakova, T.A. (2016) Legal problems of identification of subjects in state and non-state systems in Russia. *Bulletin of the Academy of Law and Management.* (43), 14–21. (in Russian).

Наумов В.Б., Полякова Т.А. Правовые проблемы идентификации субъектов в государственных и негосударственных системах в России // Вестник Академии права и управления. 2016. № 43. С. 14–21.

Ruchkina, G.F. (2017) Banking Activities: A Transfer to a New Carrying out Model or Fintech as the New Reality. *Banking Law.* (4), 55–62. (in Russian). EDN: ZDATIJ.

Ручкина Г.Ф. Банковская деятельность: переход на новую модель осуществления, или «Финтех» как новая реальность // Банковское право. 2017. № 4. С. 55–62. EDN: ZDATIJ.

Salikhov, D.R. (2021) The Pandemic and Personal Data: How the Spread of the New Coronavirus Infection Poses New Challenges to Personal Data. *Constitutional and Municipal law.* (3), 46–50. (in Russian). https://www.doi.org/10.18572/1812-3767-2021-3-46-50 EDN: RVDDAR.

Салихов Д.Р. Пандемия и персональные данные: как распространение новой коронавирусной инфекции бросает новые вызовы персональным данным // Конституционное и муниципальное право. 2021. № 3. С. 46–50. https://www.doi.org/18572/1812-3767-2021-3-46-50 EDN: RVDDAR.

Sinitsyn, S.A. (2021) *The Russian and Foreign Civil Law in the Conditions of Robotization and Digitalization. An Experience of an Inter-Disciplinary and Industrial Study: Scientific and practical guide.* Moscow, Infotropic Media Publ. (in Russian).

Синицын С.А. Российское и зарубежное гражданское право в условиях роботизации и цифровизации. Опыт междисциплинарного и отраслевого исследования : монография / С.А. Синицын. Москва : Инфотропик Медиа, 2021. 212 с.

Smirnova, Ya.V. (2022) Ensuring the right to privacy in biometric data processing in the European Union. *Actual Problems of Russian Law.* 17 (10), 183–192. (in Russian). https://www.doi.org/10.17803/1994-1471.2022.143.10.183-192

Смирнова Я.В. Проблемы обеспечения права на охрану частной жизни при обработке биометрических данных в Европейском союзе // Актуальные проблемы российского права. 2022. Т. 17. № 10. С. 183–192. https://www.doi.org/10.17803/1994-1471.2022.143.10.183-192.

Truntsevsky, Yu.V. (2020) A Smart Contract: From the Definition to Definitiveness. *Law Journal of the Higher School of Economics.* (1), 118–147. (in Russian). https://www.doi.org/10.17323/2072-8166.2020.1 EDN: EADNBA.

Трунцевский Ю.В. Смарт-контракт: от определения к определенности // Право. Журнал Высшей школы экономики. 2020. № 1. С. 118–147. https://www.doi.org/10.17323/2072-8166.2020.1 EDN: EADNBA.

Khisamov, A.Kh. (2018) Videoconferencing and Web-Conferencing Technologies in Civil Litigation. *Herald of Civil Procedure.* 10 (4), 254–269. (in Russian). https://www.doi.org/10.24031/2226-0781-2018-8-1-229-247

Хисамов А.Х. Тенденции интеграции информационных технологий в цивилистический процесс // Вестник гражданского процесса. 2018. № 1. С. 229–247. https://www.doi.org/10.24031/2226-0781-2018-8-1-229-247

Kucherov, I.I. & Sinitsyn, S.A. (2022) (eds.) *Digital Economy: Relevant Legal Regulation Areas.* Moscow, Norma Publ. (in Russian) https://www.doi.org/10.12737/1839690

Цифровая экономика: актуальные направления правового регулирования : научно-практическое пособие / под ред. И.И. Кучерова, С.А. Синицына. М. : Норма, 2022. 376 с. https://www.doi.org/10.12737/1839690.

Shebanova, N.A. (2019) Protection of personal data: The experience of the European Community. *Journal of the Court of Intellectual Property Rights.* (25), 5–14. (in Russian).

Шебанова Н.А. Охрана персональных данных: опыт Европейского сообщества // Журнал Суда по интеллектуальным правам. 2019. № 25. С. 5–14.

Warren, S.D. & Brandeis, L.D. (1890) The Right to Privacy. *Harvard Law Review*. 4 (5), 193–220.

Сведения об авторе:

Запорожцев Дмитрий Сергеевич – главный специалист-эксперт, Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации, 123317, Российская Федерация, г. Москва. Пресненская набережная, 10, стр. 2

ORCID: 0009-0001-2982-2353; SPIN-код: 6530-2894

e-mail: dmitriaugust@yandex.ru

About the author:

Dmitry S. Zaporozhtsev – Chief Expert Specialist, Ministry of Digital Development, Communications and Mass Media of the Russian Federation, 123317, Russian Federation, Moscow, Presnenskaya embankment, 10, building 2

ORCID: 0009-0001-2982-2353; SPIN-code: 6530-2894

e-mail: dmitriaugust@yandex.ru