

DOI: <https://doi.org/10.23670/IRJ.2024.142.109>

БИОМЕТРИЧЕСКИЕ ДАННЫЕ КАК ОБЪЕКТ ПРАВОВОЙ ОХРАНЫ И ЗАЩИТЫ: АКТУАЛЬНЫЕ ПРОБЛЕМЫ

Научная статья

Вронская М.В.^{1,*}, Виничук П.В.²

¹ ORCID : 0000-0001-5942-1158;

² ORCID : 0009-0009-4757-9762;

^{1,2} Владивостокский государственный университет, Владивосток, Российская Федерация

* Корреспондирующий автор (m.vronskaya[at]mail.ru)

Аннотация

В процессе цифровизации современного общества человек полноценно становится неразрывной частью технического прогресса, что приводит к дальнейшей идентификации физических лиц, где использование персональных биометрических создает угрозу нарушения конституционных прав и свобод личности. Данная статья освещает наиболее актуальные вопросы в области защиты персональных данных, сбор и критический анализ теоретико-практической основы научной статьи позволили авторам сформулировать выводы относительно перспектив формирования кибербезопасного общества в российской Федерации. В статье рассматривается действительное состояние законодательной основы Российской Федерации в части механизмов обеспечения и защиты персональных данных, и определяются тенденции их дальнейшего развития с учетом юридических приемов, внесения обоснованных и необходимых законодательных изменений. В рамках проведенного правового анализа статья поможет сформировать наиболее четкое представление действительного состояния, и совершенствования системы правовой защиты и охраны персональных биометрических данных.

Ключевые слова: биометрия, персональные данные, биометрические персональные данные, информация, физиологическая характеристика, правовая защита, идентификация личности.

BIOMETRIC DATA AS AN OBJECT OF LEGAL PROTECTION AND DEFENCE: CURRENT PROBLEMS

Research article

Vronskaya M.V.^{1,*}, Vinichuk P.V.²

¹ ORCID : 0000-0001-5942-1158;

² ORCID : 0009-0009-4757-9762;

^{1,2} Vladivostok State University, Vladivostok, Russian Federation

* Corresponding author (m.vronskaya[at]mail.ru)

Abstract

In the process of digitalization of modern society, a person fully becomes an inseparable part of technological progress, which leads to further identification of individuals, where the use of personal biometric creates a threat of violation of constitutional rights and freedoms of individuals. This article highlights the most relevant issues in the field of personal data protection, the collection and critical analysis of the theoretical and practical basis of the scientific article allowed the authors to formulate conclusions regarding the prospects for the formation of a cyber-secure society in the Russian Federation. The article examines the current state of the legislative framework of the Russian Federation in terms of mechanisms to ensure and protect personal data, and identifies trends in their further development, taking into account legal techniques, making reasonable and necessary legislative changes. Within the framework of legal analysis, the article will help to form the clearest idea of the actual state and improvement of the system of legal protection and safeguarding of personal biometric data.

Keywords: biometrics, personal data, biometric personal data, information, physiological characteristic, legal protection, personal identification.

Введение

В настоящее время защита прав личности является первоочередной государственной задачей на пути к построению современного информационного общества. Одним из наиболее проблемных вопросов в эру цифровых технологий является защита биометрических данных.

Наиболее острой проблематикой защиты прав и интересов физических лиц в сфере персональных данных является их утечка. На данном этапе, Роскомнадзором были опубликованы сведения в январе 2024 года посвященные тому, что утечка персональных данных выросла со 140млн до 168млн в 2023 году.

Федеральный закон о персональных данных в Российской Федерации в п. 1 ст. 11 раскрывает дефиницию персональных данных и интерпретирует ее, как информацию, которая властна характеризовать физиологические и природные особенности индивида, позволяющие определить характеристики конкретного лица в зависимости от его личности.

Субъектами персональных сведений считаются материальные носители с данной информацией; операторы, работающие с данными и наследники физического лица. Субъектом же личной жизни определен непосредственно человек, имеющий право на тайну о себе. Право на закрытую личную информацию обеспечено Основным законом [1].

В отечественной правовой науке самую объемную классификацию данных ввел А. М. Лушников [2, С. 100]. Характеристика специальных персональных данных указана в статье 10 Закона о персональных данных. К ним относится информация о национальной и расовой принадлежности, политических взглядах, состоянии здоровья, интимной жизни, отношению к религии, философских взглядах.

Основные результаты

Экономика в цифровом формате является примером многочисленных недоработок как на уровне законодательства, так и наличия возможностей обойти правила использования информационных баз.

К примеру, в суде рассматривалось дело о хищении недвижимости с помощью интернета. Истец получил информацию о смене его статуса в качестве собственника квартиры, получив квитанцию об оплате услуг ЖКХ. Бабушкинский районный суд г. Москвы в деле № 2–3237/19 в материалах дела отмечал, что ответчик является собственником недвижимости по условиям соглашения дарения, оформленного осенью 2018 года и подписанного с помощью использования подписи истца в электронном виде. Истец подобных договоров не оформлял и соглашение о дарении не подписывал. Также не принимал участия в оформлении электронной подписи [4]. Подчеркнем, что п. 1 ч. 1 ст. 18 ФЗ РФ от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» [5] предусматривает необходимость личного присутствия гражданина при оформлении квалифицированного сертификата его идентификации. Но получить данный сертификат возможно без личного участия человека, поэтому можно полагать, что предоставление документов при оформлении электронной подписи лица не является надежным и защищенным способом.

Ростелеком, выступающий в качестве оператора Единой базы биометрических данных, на период 2020 года отметил: 11 банковских организаций предоставляли услуги в дистанционном формате на основании биометрических данных; 13,3 тыс. отделений 231 банковских компаний принимают биометрическую информацию, что составляет 95% территорий, где проживает население РФ. Согласно данным ЦБ РФ на период 2022 года, биометрические данные можно предоставить в 13 тыс. отделений 217 банковских компаний. На сегодняшний день применение биометрических данных осуществляется в значительных объемах практически везде.

Другой актуальной проблемой выступает вопрос замены идентификации в цифровом виде на биометрическую идентификацию и формирование цифровой модели граждан. На сегодняшний день уже имеется практика создания подобных баз данных.

Ярким примером послужил случай, произошедший в городе Пермь, где в качестве виновного по ч. 5 ст. 13.11 КоАП РФ была привлечена средняя общеобразовательная школа «Мастерград». Школа использовала видеосистему при входе и выходе из учебного учреждения. Данный случай дошел до разрешения в суде кассационной инстанции, где судом не было установлено весомых аргументов для вынесения решения по существу. Судом не было получено фактических документов (согласий) от законных опекунов и родителей учеников на получение персональных данных и использования видеосистемы. Несмотря на это, администрация школы активно приводила доводы, что согласия были оформлены, однако в судебный процесс данных материалов не было предоставлено [6].

Наиболее сложным случаем в защите биометрических данных физических лиц выступают случаи, когда лица оставляют данные в электронной сети «Интернет», не придавая этому значения и не осознавая, что данный фактор не подлежит контролю. В защиту законных прав и интересов граждан Верховный суд РФ дал разъяснения по вопросу размещения персональных данных в интернете, указав на то, что действия, противоречащие нормам Закона о персональных данных, в частности изложенных п. 1 ч. 1 ст. 6, являются недопустимыми [7]. Персональные данные, размещенные в интернете, являются конфиденциальными и не являются публичными [8].

Интересным случаем в области исследования международного права, является случай, рассматриваемый Верховным судом США. Социальная сеть «Фейсбук» (запрещена на территории РФ) без согласия и информирования пользователей произвел противоправные действия по сбору и дальнейшему хранению биометрических данных, где применили процесс машинного распознавания физических лиц при помощи сканирования фото и видеоматериалов, опубликованных в социальной сети. «Фейсбук»* полагал, что данное действие не привело к значительному вреду пользователей. Данное разбирательство было окончено в 2020 году, вследствие чего «Фейсбук»* был оштрафован на 6млн долларов. Позиция «Фейсбук»* по мнению многих аналитиков и ученых является наиболее безразличной по отношению к пользователям, которые в свою очередь и обратили внимания на то, что их персональные данные не защищены должным образом, при том, что социальная сеть пропагандирует политику безопасного интернета [9, С. 678].

Анализируя преступления в сфере персональных данных, известны нередкие случаи доведения людей до самоубийства, распространение лживых сведений (клевета) в организациях, учебных учреждениях и т.д., вовлечение несовершеннолетних в собирание и продажу персональных данных физических лиц, что влечет за собой нарушение частной жизни граждан; владение чужими данными для пропаганды террористических действий, их подготовки и реализации; сбор, употребление и массовое распространение наркотических, психотропных веществ; вовлечение несовершеннолетних в занятие проституцией; распространение порнографических материалов, в частности с участием несовершеннолетних лиц; пробуждение всеобщей ненависти или вражды. Данный перечень не является исчерпывающим и продолжает расти, в связи с тем, что на настоящий момент отсутствует четкое законодательное регулирование рассматриваемого рода преступлений.

Уголовный кодекс РФ при всем многообразии составов преступления и их наказаний, не кодифицирует действительно актуальную на сегодняшний день проблему оборота персональных данных граждан. Связь с данной проблематикой можно найти в следующих статьях Уголовного закона: ст. 137 УК РФ «Нарушение неприкосновенности частной жизни», ст. 138 УК РФ «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений», ст. 183 УК РФ «Незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну», ст. 272 УК РФ «Неправомерный доступ к компьютерной информации» [10, С. 107].

Обсуждение

Рассматривая процессы развития в области эволюционирования защиты персональных биометрических данных, необходимо обратиться к практике Европейского союза, где в 2004 году был принят закон, который обязывал государства-члены хранить изображения лиц и отпечатки пальцев в паспортах и проездных документах граждан. Вскоре это распространилось на государственные и частные предприятия, которые начали использовать биометрические данные для контроля «толпы». Полагаем, тенденции текущего российского государственно-правового регулирования биометрических данных во многом схожи с зарубежной практикой, в то время как нуждаются в собственном осмыслении, направленном не на контроль и надзор, а правообранную функцию правового регулирования.

Платонова Н.И. в своих трудах отмечает, что официальное понятие биометрических персональных данных, содержащееся в п. 1 ст. 11 Закона № 152-ФЗ включает следующее: сведения, содержащие биологические и физиологические особенности гражданина, к которым относятся биометрические данные, но не затрагивает поведенческую специфику граждан, что является законодательной недоработкой. В то время как правовые источники содержат и другие классификации, к которым относятся несколько видов биометрических данных (промежуточные, физиологические, поведенческие). К промежуточным биометрическим данным относят распознавание речи, а также голоса человека [3, С. 22].

По нашему мнению, является верным то, что законодатель при утверждении приведенного понятия допустил неточности и перечислил как биологические, так и физиологические особенности. Законодатель не причислил поведенческую специфику граждан к биометрическим данным человека.

Рассматривая практический аспект, законодатель столкнулся с проблемами правового регулирования неприкосновенности частной жизни, в связи с устоявшейся правовой позицией доминирования управленческой функции РФ; контроль жизни каждой личности со стороны организаций и предприятий, партийной системы и общества был в приоритете.

Заключение

Несомненно, развитие законодательства и административной практики в условиях масштабной цифровизации не должно ущемлять гарантированные Конституцией Российской Федерации права и свободы человека и гражданина, в частности, «свободное принятие электронных документов не должно трансформироваться в обязательное условие реализации гражданином принадлежащих ему от рождения и гарантированных Конституцией Российской Федерации естественных прав и свобод» [11, С. 492].

Проведенный анализ указывает на то, внесение изменений и корректировка действующего законодательства о персональных данных является наиболее актуальным вопросом. Важно проделать работу по созданию такого механизма, который позволит физическим лицам иметь гарантию защищенности при оформлении документов онлайн и в иных случаях.

Анализируя существующую нормативную базу, разъяснения Верховного суда РФ, судебную практику, считаем необходимым внесение в Уголовный кодекс Российской Федерации изменений в нормативную структуру статьи 137 УК РФ о неприкосновенности частной жизни. Необходимо внести поправки в законодательство, которые будут предоставлять возможность гражданам на получение государственной услуги по реализации права на управление своими персональными и биометрическими данными, в частности запретить их передачу в единые централизованные регистры данных; отказ от внедрения единого регистра населения или обеспечение права граждан на отказ от передачи персональных данных в такой регистр; отказ от внедрения цифровых профилей граждан. Незаконный оборот персональных данных, в том числе биометрических, несет в себе потенциальную угрозу ряду общественных отношений.

Конфликт интересов

Не указан.

Conflict of Interest

None declared.

Рецензия

Сообщество рецензентов Международного научно-исследовательского журнала
DOI: <https://doi.org/10.23670/IRJ.2024.142.109.1>

Review

International Research Journal Reviewers Community
DOI: <https://doi.org/10.23670/IRJ.2024.142.109.1>

Список литературы / References

1. Бачило И.Л. Информационное право РФ / И.Л. Бачило. — 2011. — №18. — С. 522.
2. Лушников А.М. Защита персональных данных работника: сравнительно-правовой комментарий гл. 14 Трудового кодекса РФ / А.М. Лушников // Трудовое право. — 2009. — № 9. — С. 93-101.
3. Платонова Н.И. Современные правовые подходы к пониманию биометрических данных / Н.И. Платонова // Информационное право. — 2018. — № 1. — С. 22-26.
4. Определение Бабушкинского районного суда города Москвы от 24 мая 2019г. по делу М-2536/2019 // Официальный портал судов общей юрисдикции города Москвы. — URL: <https://mos-gorsud.ru/rs/babushkinskij/services/cases/civil/details/> (дата обращения: 18.10.2023).
5. Российская Федерация. Законы. Об электронной подписи: федер. закон: [от 06.04.2011 № 63-ФЗ (посл. ред. от 02.07.2021)] // СПС «Консультант Плюс». — URL: https://www.consultant.ru/document/cons_doc_LAW_112701/ (дата обращения: 03.10.2023).

6. Постановление Седьмого кассационного суда общей юрисдикции от 24 июля 2020г. по делу № 16—2185/2020 // СПС «Консультант Плюс». — URL: <https://www.consultant.ru/cons/cgi/online> (дата обращения: 19.10.2023).
7. Meta* признали экстремистской: что это значит для пользователей и акционеров // Право.ru. — 2022. — URL: <https://pravo.ru/story/240053/> (дата обращения: 25.10.2023).
8. Определение Верховного Суда РФ № 305-КГ17-21291 от 29 января 2018 г. по делу №А40-5250/2017 // СПС «Консультант Плюс». — URL: https://www.consultant.ru/law/podborki/personalnye_dannye_iz_otkrytyh_istochnikov/ (дата обращения: 01.11.2023).
9. Богданов Д.Е. Технодетерминизм в частном праве: влияние биопринтинга на развитие концепции защиты права на цифровой образ / Д.Е. Богданов // Вестник Пермского университета. Юридические науки. — 2020. — № 4. — С. 678-704.
10. Чукреев В.А. Персональные данные, в том числе биометрические данные, как предметы уголовно-правовой охраны / В.А. Чукреев // Вестник Университета имени О.Е. Кутафина. — 2022. — № 3 (91). — С. 107-116.
11. Игонина О.О. Развитие цифровых технологий в период пандемии COVID-19: новые риски и новые возможности / О.О. Игонина // Молодой ученый. — 2021. — № 21 (363). — С. 492-494.

Список литературы на английском языке / References in English

1. Bachilo I.L. Informacionnoe pravo RF [Information law of the Russian Federation] / I.L. Bachilo. — 2011. — №18. — P. 522. [in Russian]
2. Lushnikov A.M. Zashhita personal'nyh dannyh rabotnika: sravnitel'no-pravovoj kommentarij gl. 14 Trudovogo kodeksa RF [Protection of employee's personal data: comparative legal commentary Chapter 14 of the Labor Code of the Russian Federation] / A.M. Lushnikov // Trudovoe pravo [Labor law]. — 2009. — № 9. — P. 93-101. [in Russian]
3. Platonova N.I. Sovremennye pravovye podhody k ponimaniyu biometricheskikh dannyh [Modern legal approaches to understanding biometric data] / N.I. Platonova // Informacionnoe pravo [Information law]. — 2018. — № 1. — P. 22-26. [in Russian]
4. Opredelenie Babushkinskogo rajonnogo suda goroda Moskvy ot 24 maja 2019g. po delu M-2536/2019 [The ruling of the Babushkinsky District Court of Moscow dated May 24, 2019 in the case M-2536/2019] // Oficial'nyj portal sudov obshhej jurisdikcii goroda Moskvy [The official portal of the courts of general jurisdiction of the city of Moscow]. — URL: <https://mos-gorsud.ru/rs/babushkinskij/services/cases/civil/details/> (accessed: 18.10.2023). [in Russian]
5. Rossijskaja Federacija. Zakony. Ob jelektronnoj podpisi [Russian Federation. Laws. About the electronic signature]: Federal Law: [dated 04/06/2011 No. 63-FZ (post-ed. from 07/02/2021)] // SPS Consultant Plus. — URL: https://www.consultant.ru/document/cons_doc_LAW_112701/ (accessed: 03.10.2023). [in Russian]
6. Postanovlenie Sed'mogo kassacionnogo suda obshhej jurisdikcii ot 24 ijulja 2020g. po delu № 16—2185/2020 [Resolution of the Seventh Court of Cassation of General Jurisdiction dated July 24, 2020 in case No. 16-2185/2020] // SPS Consultant Plus. — URL: <https://www.consultant.ru/cons/cgi/online> (accessed: 19.10.2023). [in Russian]
7. Meta* priznali jekstremistskoj: chto jeto znachit dlja pol'zovatelej i akcionerov [Meta* recognized as extremist: what does this mean for users and shareholders] // Pravo.ru. — 2022. — URL: <https://pravo.ru/story/240053/> (accessed: 25.10.2023). [in Russian]
8. Opredelenie Verhovnogo Suda RF № 305-KG17-21291 ot 29 janvarja 2018 g. po delu №А40-5250/2017 [Ruling of the Supreme Court of the Russian Federation No. 305-KG17-21291 dated January 29, 2018 in case No. A40-5250/2017] // SPS Consultant Plus. — URL: https://www.consultant.ru/law/podborki/personalnye_dannye_iz_otkrytyh_istochnikov/ (accessed: 01.11.2023). [in Russian]
9. Bogdanov D.E. Tehnodeterminizm v chastnom prave: vlijanie bioprintinga na razvitie koncepcii zashhity prava na cifrovoj obraz [Technodeterminism in private law: the impact of bioprinting on the development of the concept of protecting the right to a digital image] / D.E. Bogdanov // Vestnik Permskogo universiteta. Juridicheskie nauki [Bulletin of the Perm University. Legal sciences]. — 2020. — № 4. — P. 678-704. [in Russian]
10. Chukreev V.A. Personal'nye dannye, v tom chisle biometricheskie dannye, kak predmety ugolovno-pravovoj ohrany [Personal data, including biometric data, as subjects of criminal law protection] / V.A. Chukreev // Vestnik Universiteta imeni O.E. Kutafina [Bulletin of the O.E. Kutafin University]. — 2022. — № 3 (91). — P. 107-116. [in Russian]
11. Igonina O.O. Razvitie cifrovyh tehnologij v period pandemii COVID-19: novye riski i novye vozmozhnosti [The development of digital technologies during the COVID-19 pandemic: new risks and new opportunities] / O.O. Igonina // Molodoy uchenyj [A young scientist]. — 2021. — № 21 (363). — P. 492-494. [in Russian]