DOI: 10.17803/1994-1471.2022.143.10.183-192

Я. В. Смирнова*

Проблемы обеспечения права на охрану частной жизни при обработке биометрических данных в Европейском Союзе

Аннотация. В статье проводится анализ действующих правовых норм, регламентирующих на уровне Европейского Союза обработку биометрических данных граждан. Особое внимание уделяется изучению перечня условий обработки специальных категорий персональных данных, установленного Общим регламентом ЕС о защите персональных данных (GDPR). В статье отмечаются проблемы преуменьшения в Регламенте GDPR роли согласия субъекта на обработку специальных категорий персональных данных, а также явного преимущества публичного интереса (безопасности общества и государства) перед реализацией индивидом права на неприкосновенность частной жизни. Анализируется практика ЕСПЧ и Суда ЕС по исследуемому вопросу. Автором приводится вывод о коллизиях, возникающих в результате предоставляемого государствам-членам права дополнительно принимать на национальном уровне собственные правила обработки специальных категорий персональных данных. Предлагаются практические меры по совершенствованию правового регулирования обработки биометрических данных в целях установления баланса между частными интересами граждан и публичных интересов общества и государства.

Ключевые слова: европейское право; Европейский Союз; биометрические данные; права человека; право на защиту персональных данных; обработка специальных категорий данных; регламент о защите персональных данных; общественная безопасность; Европейский Суд по правам человека; Суд ЕС.

Для цитирования: *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. — DOI: 10.17803/1994-1471.2022.143.10.183-192.

Ensuring the Right to Privacy in Biometric Data Processing in the European Union

Yanina V. Smirnova, Postgraduate Student, Department of Integration and European Law, Kutafin Moscow State Law University (MSAL)
ul. Sadovaya-Kudrinskaya, d. 9, Moscow, Russia, 125993
yaninasmivi@mail.ru

Abstract. The paper analyzes the current legal norms regulating the processing of biometric data of citizens at the level of the European Union. Particular attention is given to the study of the list of conditions for the processing of

* *Смирнова Янина Викторовна*, аспирант кафедры интеграционного и европейского права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)
Садовая-Кудринская ул., д. 9, г. Москва, Россия, 125993
yaninasmivi@mail.ru

special categories of personal data, established by the EU General Data Protection Regulation (GDPR). The paper notes the problems of downplaying in the GDPR the role of the consent of the subject to the processing of special categories of personal data, as well as the clear advantage of the public interest (security of society and the state) over the individual's right to privacy. The practice of the ECHR and the EU Court of Justice on the issue under study is analyzed. The author draws a conclusion about conflicts that arise as a result of the right granted to Member States to additionally adopt at the national level their own rules for processing special categories of personal data. Practical measures are proposed to improve the legal regulation of the processing of biometric data in order to establish a balance between the private interests of citizens and the public interests of society and the state.
Keywords: European law; European Union; biometric data; human rights; the right to protection of personal data; processing of special categories of data; regulation on the protection of personal data; public safety; European Court of Human Rights; EU court.
Cite as: Smirnova YaV. Problemy obespecheniya prava na okhranu chastnoy zhizni pri obrabotke biometricheskikh dannykh v Evropeyskom Soyuze [Ensuring the Right to Privacy in Biometric Data Processing in the European Union]. *Aktual'nye problemy rossijskogo prava*. 2022;17(10):183-192. DOI: 10.17803/1994-1471.2022.143.10.183-192. (In Russ., abstract in Eng.).

Введение

Правовая охрана частной жизни индивида в условиях прогрессивного развития различных информационных систем обработки и передачи персональной информации является одним из ключевых векторов в сфере охраны прав человека.

Институт защиты персональных данных возник в конце XIX в. как один из элементов появившегося в тот момент права на неприкосновенность частной жизни, когда суды сочли неприемлемыми ряд действий по отношению к личности, которые по своей сути нарушали конфиденциальность[1].

Персональные данные, включая биометрические, содержащиеся в удостоверяющих личность документах, подлежат обработке (хранению) в национальных регистрационных системах, которые, в свою очередь, составляют основу государственного управления.

Однако в ряде стран правомерность использования подобных систем была успешно оспорена на основании принципа конституционной неприкосновенности частной жизни. В 1991 г. Конституционный суд Венгрии постановил, что закон, позволяющий создание многоразового личного идентификационного номера, прямо нарушает конституционное право на неприкосновенность частной жизни[2].

В практике Европейского Суда по правам человека (ЕСПЧ) защита персональных данных рассматривается как часть права на неприкосновенность частной жизни, которое гарантировано статьей 8 Конвенции о защите прав человека и основных свобод[3].

Неприкосновенность частной жизни заключается в реализации права индивида на защиту от неоправданного вторжения, в том числе права на защиту личной информации. Вместе с тем реализация права на неприкосновенность частной жизни может создавать некоторые проблемы при обеспечении безопасности общества. Если человек намеревается совершить какое-либо преступное деяние, например террористический акт, то, вероятно, предоставленное ему законом право на охрану частной жизни открывает перед ним больше возмож-

1 *Warren S. D.*, *Brandeis L. D.* The Right to Privacy // Harvard Law Review. 1890. Vol. 4. No. 5. P. 193–220.

2 *Banisar D.*, *Davies S.* Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments (August 30, 2012) // John Marshall Journal of Computer & Information Law, Vol. 18. No. 1. Fall 1999. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2138799 (дата обращения: 01.02.2022).

3 СЗ РФ. 2001. № 2. Ст. 163.

ностей и инструментов. В этом и заключается основная суть противостояния между правом на неприкосновенность частной жизни и законных интересов и безопасностью общества и государства[4].

Настоящая статья имеет целью анализ правового регулирования обработки биометрических данных и практического влияния действующих правовых норм на возможность реализации права человека на неприкосновенность частной жизни, а также выработку практических предложений по совершенствованию правового регулирования обработки биометрических данных для установления баланса между частными интересами граждан и обеспечением общественной безопасности.

В рамках данного исследования необходимо детально изучить условия обработки биометрических данных, предусмотренные Регламентом Европейского парламента и Совета о защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных и об отмене Директивы 95/46/ЕС (Общий регламент о защите персональных данных / General Data Protection Regulation — GDPR)[5] (далее — Регламент GDPR), и проанализировать судебную практику Европейского Суда по правам человека и Суда Европейского Союза (Суд ЕС), где в качестве основного нарушения при обработке биометрических данных рассматривалось ограничение права на уважение частной жизни.

Регламент GDPR об обработке специальных категорий персональных данных на примере биометрических данных

С принятием 27 апреля 2016 г. Регламента GDPR утратила силу Директива 95/46/ЕС Европейского парламента и Европейского Союза от 24.10.1995 о защите физических лиц при обработке персональных данных и о свободном обращении таких данных[6], в которой одновременно отражались две первостепенные задачи: обеспечение свободного перемещения информации между странами — членами ЕС и обеспечение гарантий защиты основных прав граждан, в том числе право на неприкосновенность личных данных и их защиту от неправомерного использования третьими лицами[7].

В Директиве 95/46/ЕС впервые было закреплено, что под персональными данными понимается любая информация, связанная с физическим лицом, которое может быть идентифицировано прямо или косвенно, в частности посредством ссылки на идентификационный номер или на один или несколько факторов, специфичных для его психологической, ментальной, экономической, культурной, социальной, а также физической идентичности. Под последним прямо подразумеваются биометрические характеристики человека.

Положения Директивы 95/46/ЕС устанавливали обязательства для всех государств-участников по обеспечению обработки таких данных только при условии, если «субъект недвусмысленно выразил на это свое согласие или такая обработка необходима для заключения/испол-

[4] *McMenemy D.* Rights to privacy and freedom of expression in public libraries: squaring the circle. 2016 // URL: https://pureportal.strath.ac.uk/files-asset/54531639/McMenemy_IFLA_2016_rights_to_privacy_and_freedom_of_expression_in_public_libraries.pdf (дата обращения: 01.02.2022).

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) // Official Journal of European Communities, L 119. 04.05.2016. P. 1–88.

[6] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data // Official Journal of the European Communities, L 281. 23.11.1995. P. 31–50.

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

нения контракта; выполнения юридического обязательства, субъектом которого является контролер или она необходима для защиты жизненных интересов субъекта данных». Такая обработка считалась также допустимой, если она была необходима в целях обеспечения законных интересов контролера или третьей стороны, которым раскрыты данные, кроме случаев, когда такие интересы перекрываются интересами фундаментальных прав и свобод субъекта данных.

Со временем, ввиду необходимости предоставления гражданам ЕС большего контроля над собственными персональными данными в условиях технического прогресса, законодательство актуализируется посредством принятия Регламента GDPR, который уже прямо выделяет биометрическую информацию в качестве специальной категории данных, акцентируя внимание на том, что они наиболее уязвимы в современных условиях.

Статья 9 (1) Регламента GDPR устанавливает запрет на обработку таких данных. Тем не менее имеет место ряд исключений из общего правила, которые предлагается подробнее рассмотреть и выяснить, носят ли они неоднозначный характер и не нарушают ли они права человека.

Первым из таких исключений является прямое согласие субъекта на обработку биометрических данных для одной или нескольких обозначенных целей, кроме случаев, когда законодательство ЕС или государства-члена предусматривает, что запрет на обработку не может быть снят субъектом данных (пар. 2 (а) ст. 9 Регламента GDPR).

Под прямым согласием, в соответствии со ст. 4 (11) Регламента GDPR, понимается «добровольное, конкретное, информированное и однозначное волеизъявление, в котором субъект данных с помощью заявления или четкого утвердительного действия дает согласие на обработку своих данных». Если согласие субъекта в форме письменной декларации обладает некой юридической прозрачностью, то в отношении «четкого утвердительного действия» возникает ряд вопросов.

Как нам известно, в мире активно внедряются биометрические технологии распознавания лиц посредством установления систем видеонаблюдения в общественных местах (пешеходные зоны, международные аэропорты, метро, торговые и бизнес-центры), позволяющих идентифицировать личность человека с точностью до 100 %. Будет ли с точки зрения права намеренное использование гражданином, к примеру, метро в качестве основного средства передвижения расцениваться как «четкое утвердительное действие», выражающее прямое согласие на обработку его биометрических данных? На каком основании в этом случае осуществляется сбор биометрических данных граждан? Если статья 7 (2) Регламента GDPR содержит требование к содержанию письменного согласия, то к согласию в форме «четкого утвердительного действия» таких требований не предъявляется. Каким образом контролер данных обязан продемонстрировать, что субъект данных дал согласие на обработку своих уникальных по природе данных (ст. 7 (1) Регламента GDPR)?[8]

Данная неясность и отсутствие в законодательстве закрытого перечня таких действий создает на практике противоречие и противостояние между законодательством в сфере охраны персональных данных и институтом основных прав и свобод человека и гражданина. Закон не должен создавать условия, при которых лицо теряет право на конфиденциальность личной уникальной информации, а должен обеспечивать реализацию права на защиту частной жизни, которое осуществляется непосредственно через информативное согласие

[8] В соответствии со ст. 4 (7) Регламента GDPR контролер — это любое физическое или юридическое лицо, государственный орган, учреждение или другой орган, который самостоятельно или совместно с другими определяет цели и средства обработки персональных данных; контролер или критерии для его определения могут быть установлены законодательством Союза или государства-члена в случаях, когда цели и средства этой обработки определяются законодательством Союза или государства-члена.

или несогласие субъекта на обработку его биометрических данных[9].

Очередное условие, исключающее запрет на обработку биометрических данных, исходит из соображений «существенного публичного интереса», которые «должны быть пропорциональны преследуемой цели, должны соответствовать сути права на защиту персональных данных и предусматривать приемлемые и конкретные меры для защиты фундаментальных прав и интересов субъекта данных» (пар. 2 (g) ст. 9). Однако что именно понимается под «существенным публичным интересом» и чем он отличается от «публичного интереса», о котором упоминается в статье неоднократно, законодатель не поясняет.

Помимо этого, перечень допустимых Регламентом GDPR «преследуемых целей» обработки особой категории данных, снимающих запрет на их обработку, довольно широк. К таким целям относятся:

— цели исполнения обязательств и определенных прав контролера или субъекта данных в сфере трудового права, права социального обеспечения и социальной защиты (п. 2 (b) ст. 9);
— политические, философские, религиозные или профсоюзные цели в рамках лигитимной деятельности фонда, объединения или некоммерческой организации при соблюдении определенных условий, регламентируемых в пар. 2 (d) ст. 9;
— цели осуществления правосудия судами (пар. 2 (f) ст. 9);
— цели профилактической или профессиональной медицины, для оценки трудоспособности работника, для диагностики медицинского состояния, предоставления медицинской или социальной помощи, или лечения, или для управления системами и услугами здравоохранения и социального обеспечения (пар. 2 (h) ст. 9);
— цели защиты от серьезных трансграничных угроз здоровью или для обеспечения высоких стандартов качества и надежности медицинского обслуживания и лекарственных средств или медицинской техники (пар. 2 (i) ст. 9);
— архивные цели в интересах общества; научные, исторические, исследовательские или статистические цели (пар. 2 (j) ст. 9).

В статье подчеркивается, что все указанные цели при такой необходимости обязаны реализовываться строго в соответствии с правом на охрану персональных данных и обеспечивать средства и гарантии защиты фундаментальных прав и интересов субъекта данных. Тем не менее, исходя из анализа положений статьи, невозможно не отметить явное преобладание общественного интереса над правом человека на защиту собственных уникальных по своей природе персональных данных.

Кроме того, формулировка параграфа 2 ст. 9 трактует согласие субъекта на обработку таких персональных данных как одно из оснований для отмены запрета на их обработку, а не как изначально основное и ключевое условие обработки. Из этого следует, что контролер данных имеет право совершать любые операции с данными субъекта при наличии хотя бы одного из вышеперечисленных обстоятельств. Представляется, что в современном правовом обществе, которое признает основные права и свободы человека высшей ценностью, добровольное волеизъявление субъекта данных должно иметь беспрецедентное преимущество над остальными перечисленными в Регламенте GDPR условиями.

Помимо прочего, теряет смысл параграф 1 ст. 9, в целом устанавливающий запрет на обработку чувствительной категории данных, при наличии столь широкого круга исключений из общего правила.

Во избежание такого противоречия в одном документе и впоследствии ограничения права человека на охрану собственной биометрической информации целесообразно было бы изначально установить разрешение на обработку таких персональных данных исключительно при наличии однозначного добровольного согласия субъекта, официально зафиксированного на бу-

[9] *Hall T. S.* The Quantified Self Movement: Legal Challenges and Benefits of Personal Biometric Data Tracking // Akron Intellectual Property Journal. 2014. Vol. 7. Iss. 1. Article 3.

мажном или электронном носителе. В качестве обстоятельств, исключающих необходимость наличия официального согласия субъекта на обработку данных, важно было бы упомянуть цели:

— защиты жизненных интересов субъекта данных, как это установлено в пар. 2 (c) ст. 9 Регламента GDPR;
— предупреждения угрозы национальной или общественной безопасности, транспортной безопасности, противодействия терроризму, осуществления оперативно-разыскной деятельности, здравоохранения;
— раскрытия и предупреждения административных правонарушений и уголовных преступлений правоохранительными органами.

Что касается последней предложенной категории исключений, на практике здесь также наблюдаются правовые противоречия в части обработки чувствительных персональных данных: это, главным образом, заключается в некотором несоответствии норм актов, издаваемых в области осуществления деятельности национальных компетентных органов, основным положениям законодательства об охране прав человека.

Практика ЕСПЧ и Суда ЕС

В фундаментальном деле «С. и Марпер против Соединенного Королевства»[10] 2008 г. ЕСПЧ, ссылаясь на ст. 7 Конвенции о защите физических лиц при автоматизированной обработке персональных данных, заключенной в Страсбурге в 1981 г.[11], подчеркнул, что национальное законодательство государств — участников данной Конвенции обязано предусматривать гарантии, удовлетворяющие требованиям эффективной защиты хранящихся персональных данных от неправомерного использования и злоупотреблений.

Заявители по делу ранее обвинялись в совершении уголовных преступлений, однако впоследствии были оправданы национальным судом. В ходе следственных мероприятий у обвиняемых были сняты образцы отпечатков пальцев, взяты анализы ДНК, а также образцы их клеток. После завершения следствия оба заявителя обратились к полиции с требованием удалить собранные биометрические и биологические материалы из национальной базы данных, в которой подобная информация хранилась бессрочно. Со стороны полиции поступил отказ, обусловленный статьей 64 Акта «О полиции и доказательствах по уголовным делам» 1984 г.[12], которой предусмотрено хранение отпечатков пальцев или образцов ДНК по достижении цели, ради которой они были взяты.

ЕСПЧ поддержал позицию заявителей, отметив, что хранение таких персональных данных по уголовным делам, в которых обвиняемые были оправданы или их уголовное преследование было прекращено, является нарушением ст. 8 Конвенции о защите прав человека и основных свобод. Ссылаясь на решение по делу «Леандер против Швеции»[13], ЕСПЧ отметил, что даже простое хранение информации, относящейся к личной жизни человека, является вмешательством государства в осуществление его прав в нарушение положений ст. 8 Конвенции о защите прав человека и основных свобод. ЕСПЧ подчеркнул, что содержащаяся в отпечатках пальцев информация содержит объективно уникальную информацию о человеке, а в большинстве случаев позволяет максимально точно установить личность индивида. Таким образом, это может напрямую затрагивать право на неприкосновенность частной жизни, а хранение подобной информации без согласия лица, которому она принадлежит, нельзя назвать нейтральным или незначительным.

[10] Applications No. 30562/04 and 30566/04, S. and Marper v. The United Kingdom, ECHR Judgment of 4 December 2008.

[11] СЗ РФ. 2014. № 5. Ст. 419.

[12] Police and Criminal Evidence Act 1984. First Published 1984, Reprinted in the United Kingdom by The Stationery Office Limited. London, 1997.

[13] Application No. 9248/81, Leander v. Sweden, ECHR Judgment of 27 March 1987.

Одновременно ЕСПЧ не отрицает того, что в некоторых случаях вмешательство в право заявителя на неприкосновенность частной жизни может быть признано законным. Но это допустимо лишь при соблюдении некоторых условий, как в деле «Ван дер Вельден против Нидерландов», на которые Суд специально обращает внимание[14].

Аналогичное решение в феврале 2020 г. ЕСПЧ вынес по делу «Гохран против Соединенного Королевства»[15], суть которого заключается в следующем.

Заявитель был задержан полицией Северной Ирландии за вождение в нетрезвом виде, за что позднее был осужден (оштрафован и лишен права управления транспортным средством сроком на 12 месяцев). В день задержания у него были взяты биометрические данные в виде отпечатков пальцев и образец ДНК. Заявитель обратился в Полицейскую службу Северной Ирландии с заявлением об уничтожении или о возврате ему вышеуказанных данных, в чем ему было отказано. При этом, согласно национальному законодательству, подобная информация может храниться неопределенное количество лет с целью более эффективного предотвращения каких-либо противозаконных действий в будущем.

Первоначально спор рассматривался Высоким судом Северной Ирландии, который признал подобное хранение биометрических данных вмешательством в осуществление законных прав заявителя, данных ему статьей 8 Конвенции о защите прав человека и основных свобод, однако пояснил, что такое вмешательство было оправданным и соразмерным.

Позднее по апелляционному заявлению Гохрана дело было рассмотрено Верховным судом Великобритании, который также пришел к выводу, что бессрочное хранение данных в конкретном случае являлось соразмерным. Было подчеркнуто, что решение по делу «С. и Марпер против Соединенного Королевства» касалось только «неосужденных» лиц. Это не означает, что система в Северной Ирландии (и Соединенном Королевстве) в отношении осужденных обязательно является пропорциональной. Тем не менее уровень вмешательства в права заявителя по ст. 8 Конвенции о защите прав человека и основных свобод был низким и подобное вмешательство было оправданным с учетом соблюдения Соединенным Королевством справедливого баланса между конкурирующими государственными и частными интересами. Одновременно был принят во внимание тот факт, что заявитель был только оштрафован и не был заключен в тюрьму, но подчеркнул, что вождение автомобиля с избыточным потреблением алкоголя является серьезным преступлением.

По данному решению ЕСПЧ отметил, что характер совершенного заявителем правонарушения не позволяет усмотреть необходимость бессрочного хранения собранной информации, в то время как аргумент о якобы потенциальном незаконном действии с его стороны в будущем не соответствует стандартам Конвенции о защите прав человека и основных свобод.

ЕСПЧ напомнил, что срок хранения биометрических данных человека остается на усмотрение властей Великобритании. Однако было подчеркнуто, что государство, принимая решение о сроках, должно придерживаться приемлемых и разумных границ в соответствии с принципами демократического общества, а также осуществлять надлежащий контроль за сохранностью данных, принимать меры против разного рода злоупотреблений и гарантировать возможность обжаловать решение о заборе биометрических данных.

Таким образом, суд пришел к выводу, что властям Великобритании «не удалось найти справедливый баланс между конкурирующими государственными и частными интересами», в связи с чем они «перешагнули допустимую свободу усмотрения» порядка сбора и сроков хранения биометрических данных при незначительном правонарушении.

Однако, как показывает судебная практика, не всегда отстаивающие свои законные права

[14] Application No. 29514/05, Van der Velden v. Netherlands, Judgment of 7 December 2006.

[15] Application No. 45245/15, Gaughran v. The United Kingdom, Judgment of 13 February 2020.

и свободы граждане получают желаемую поддержку со стороны органов правосудия.

По делу «Шварц против Бохум» (Германия)[16] в 2013 г. Суд ЕС признал справедливыми и оправданными мероприятия по обработке (забору) биометрических данных, предусмотренные ст. 1 (2) Регламента № 2252/2004 Совета Европейского Союза «О стандартах для средств защиты и биометрических данных в паспортах и проездных документах, выданных государствами — членами ЕС»[17], правомерность проведения которых оспаривалась гражданином Германии Шварцом.

В ходе процедуры получения паспорта заявитель отказался предоставлять отпечатки пальцев, обосновав это тем, что такое требование не имеет соответствующего правового основания и напрямую нарушает право на уважение частной жизни, гарантируемое статьей 7 Хартии Европейского Союза об основных правах от 07.12.2000[18], в результате чего Шварцу было отказано в выдаче паспорта.

Таким образом, на рассмотрение Суда ЕС были представлены вопросы относительно законности и правовой обоснованности принятия Регламента № 2252/2004, а также признания данного Регламента недействительным ввиду наличия положений, нарушающих некоторые основные права ходатайствующих о получении паспорта граждан.

Суд ЕС разъяснил, что обработка, в частности сбор, биометрических данных, предусмотренная статьей 1 (2) Регламента № 2252/2004, в первую очередь является необходимой мерой по предупреждению совершения мошеннических действий в отношении паспортов граждан, ввиду этого цели подобного «вмешательства» в частную жизнь граждан оправданны и обоснованны. Суд подчеркнул, что рассмотрение подобных вопросов относительно законности положений Регламента нецелесообразно, так как его основной и приоритетной целью является предотвращение фальсификации документов, удостоверяющих личность граждан.

Исходя из изложенных соображений Суд ЕС вынес решение об отсутствии оснований для признания недействительными и незаконными положения ст. 1 (2) Регламента № 2252/2004.

Заключение

Подробный анализ правового регулирования обработки биометрических данных, а также обзор судебной практики позволяет автору прийти к следующим выводам.

Во-первых, отмечается установление некорректного, по мнению автора, перечня условий обработки специальных категорий персональных данных в ст. 9 Регламента GDPR и одновременно существенное ущемление таким образом прав человека. Следует учитывать, что в основополагающем документе по защите физических лиц в отношении обработки персональных данных, провозглашающем защиту основных прав и свобод человека основной его целью (ст. 1(2) Регламента GDPR), недопустимо упоминание прямого согласия субъекта на обработку его уникальных данных в качестве исключающего обстоятельства наравне с многочисленными факторами, поддерживающими, главным образом, публичный (общественный) интерес.

Согласие субъекта должно рассматриваться как фундаментальное условие возможности обработки его биометрических данных, а не как одно из 10 оснований для отмены запрета на их обработку.

[16] Judgment of the Court (Fourth Chamber) of 17 October 2013 Michael Schwarz v. Stadt Bochum. Case C-291/12. ECLI:EU:C:2013:670 // URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0291 (дата обращения: 01.02.2022).

[17] Council Regulation (EC) No. 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States // Official Journal of the European Union, L 385. 29.12.2004. P. 1–6.

[18] Charter of Fundamental Rights of the European Union (Strasbourg, December 12, 2007) (2016/C 202/02), Official Journal of the European Union.

Кроме того, Регламент GDPR не устанавливает конкретных требований к форме и содержанию такого волеизъявления, лишь указывает, что оно должно быть «недвусмысленным». Такая формулировка существенно повышает риск тотального неправомерного сбора биометрических данных граждан на практике и, более того, признает такую обработку законной. Как верно отмечает профессор С. Ю. Кашкин, «сужение сферы неприкосновенности частной жизни, вследствие сбора, объединения и анализа огромного массива данных об индивидах тем опаснее, что сбор информации сейчас может осуществляться в том числе в таких сферах и такими способами, которых рядовой человек даже не предполагает»[19].

Во-вторых, предоставленное Регламентом GDPR государствам-членам право принимать на национальном уровне собственные правила обработки в том числе биометрических данных, а также устанавливать условия, при которых такая обработка будет признана правомерной, с одной стороны, реализует обеспечение совместной деятельности Союза и государств-членов в силу ст. 16 (2) Договора о функционировании Европейского Союза[20], с другой — способствует широкому распространению в судебной практике таких дел, как «С. и Марпер против Соединенного Королевства» и «Шварц против Бохум». Это говорит о необходимости унификации норм на уровне законодательства Евросоюза в части вопросов, провоцирующих подобные споры.

Все вышеизложенное позволяет заключить, что защита собственных биологических уникальных данных имеет основополагающее значение для осуществления человеком своего права на уважение частной жизни, гарантированного статьей 8 Конвенции о защите прав человека и основных свобод. Ввиду этого национальное законодательство обязано предусматривать надлежащие гарантии для предотвращения любого такого использования персональных данных исследуемой категории.

БИБЛИОГРАФИЯ

1. *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. — С. 64–90.
2. *Шебанова Н. А.* Охрана персональных данных: опыт Европейского сообщества // Журнал Суда по интеллектуальным правам. — 2019. — № 25. — С. 5–14.
3. *Banisar D., Davies S.* Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments (August 30, 2012) // John Marshall Journal of Computer & Information Law. — 1999. — Vol. XVIII. — No. 1.
4. *Hall T. S.* The Quantified Self Movement: Legal Challenges and Benefits of Personal Biometric Data Tracking // Akron Intellectual Property Journal. — 2014. — Vol. 7. — Iss. 1. — Article 3.
5. *McMenemy D.* Rights to privacy and freedom of expression in public libraries: squaring the circle. — 2016.
6. *Warren S. D.*, *Brandeis L. D.* The Right to Privacy // Harvard Law Review. — 1890. — Vol. 4. — № 5. — P. 193–220.

Материал поступил в редакцию 26 февраля 2022 г.

[19] *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. С. 64–90.

[20] Договор о функционировании Европейского Союза (Рим, 25 марта 1957 г.) (в редакции Лиссабонского договора 2007 г.).

REFERENCES (TRANSLITERATION)

1. Kashkin S. Yu., Pokrovskiy A. V. Iskusstvennyy intellekt, robototekhnika i zashchita prav cheloveka v Evropeyskom Soyuze // Vestnik Universiteta imeni O.E. Kutafina (MGYuA). — 2019. — № 4. — S. 64–90.
2. Shebanova N. A. Okhrana personalnykh dannykh: opyt Evropeyskogo soobshchestva // Zhurnal Suda po intellektualnym pravam. — 2019. — № 25. — S. 5–14.
3. Banisar D., Davies S. Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments (August 30, 2012) // John Marshall Journal of Computer & Information Law. — 1999. — Vol. XVIII. — No. 1.
4. Hall T. S. The Quantified Self Movement: Legal Challenges and Benefits of Personal Biometric Data Tracking // Akron Intellectual Property Journal. — 2014. — Vol. 7. — Iss. 1. — Article 3.
5. McMenemy D. Rights to privacy and freedom of expression in public libraries: squaring the circle. — 2016.
6. Warren S. D., Brandeis L. D. The Right to Privacy // Harvard Law Review. — 1890. — Vol. 4. — № 5. — P. 193–220.