Научная специальность
12.00.10 «Международное право; Европейское право»

УДК 341.1/8
DOI https://doi.org/10.26516/2071-8136.2021.3.89

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ОБОРОТА БИОМЕТРИЧЕСКИХ ДАННЫХ ГРАЖДАН В ЕВРОПЕЙСКОМ СОЮЗЕ

© **Колосов А. В., 2021**
Иркутский государственный университет, г. Иркутск, Россия

Утверждается, что обеспечение безопасности человека и общества является одним из приоритетных и важных направлений деятельности любого правового государства. Сделан вывод о том, что меры, направленные на противодействие преступности, борьба с правонарушениями в информационной сфере невозможны без взаимодействия и сотрудничества между государствами, так как подобные нарушения часто носят трансграничный характер. Изучена деятельность Европейского союза, которая вызывает интерес благодаря уникальной форме сотрудничества в сфере информационного взаимодействия стран-членов и применению новейших технологий идентификации для создания единого европейского пространства безопасности. Рассмотрено правовое регулирование защиты персональных и биометрических данных, проведено сравнение указанных терминов. Выделены признаки, присущие биометрическим данным. Особое внимание уделено анализу Регламента «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС» (General Data Protection Regulation (GDPR)). Было установлено, что новшеством Регламента стало закрепление в европейской практике особых данных конфиденциального характера, концепции биометрических данных и способов их обработки. Проанализирована современная практика Суда Европейского союза в области защиты персональных и биометрических данных граждан. Исследованы современные тенденции развития европейского права в части создания базы биометрических данных – Общего хранилища идентификационных данных (Common Identity Repository (CIR)) и проекта, связанного с ограничением использования искусственного интеллекта в областях, представляющих угрозу для защиты персональных, биометрических данных граждан Европейского союза. Сделан вывод о том, что обработка биометрических данных сопряжена с высокими рисками возникновения нарушений прав отдельных лиц и работа с подобного рода информацией должна соответствовать определенной цели, иметь ограничения по объему обрабатываемых данных и по сроку их хранения для решения конкретных задач.

Ключевые слова: персональные данные, биометрические данные, Общий регламент по защите персональных данных, «чувствительные» данные, Общее хранилище идентификационных данных, искусственный интеллект.

В условиях стремительного расширения информационного пространства, развития современных технологий, появления новых видов персональных данных происходит увеличение количества преступлений и правонарушений, связанных с нарушением прав граждан в информационной сфере.

Большое количество различных видов персональных данных и их постоянный оборот вызывают риск их неправомерного использования. В современном мире невозможно абсолютно гарантировать конфиденциальность и безопасность персональных данных граждан. Все чаще возникают случаи утечки информации в связи с отсутствием четких правил сохранения конфиденциальности и возникновением новых технологий, которые еще не получили достаточного правового регулирования.

Система общественной безопасности в информационной среде, формируемая международным сообществом, способствует созданию новых правовых норм и ужесточению существующих требований к защите прав личности и персональной информации. Выполнение международных обязательств государствами создает необходимые условия для недопущения нарушений субъективных прав и законных интересов граждан.

Обеспечение безопасности человека и общества, противодействие преступным посягательствам является прерогативой и приоритетным направлением деятельности любого правового государства. Однако борьба с правонарушениями в информационной среде невозможна без тесного сотрудничества и взаимодействия государств, так как подобного рода нарушения часто имеют трансграничный

характер и могут затрагивать интересы неограниченного количества граждан.

В связи с этим интересен опыт уникальной региональной международной организации, объединившей большое количество стран, – Европейского союза.

Европейский союз представляет собой форму сотрудничества государств в разнообразных областях, в том числе и в вопросах информационного взаимодействия и применения новейших технологий идентификации для создания единого европейского пространства безопасности. Как обоснованно отмечают специалисты, область защиты данных – это сфера, которая всегда шире одного правового акта [5, с. 257]. Комплексное изучение подобного опыта позволит оценить существующие механизмы правового регулирования оборота персональных данных в информационной среде на территории Европейского союза и использовать подобные положительные знания в практике других стран.

С целью повышения эффективности борьбы с трансграничными преступлениями и правонарушениями Европейский союз с момента своего появления предусмотрел различные формы сотрудничества правоохранительных органов стран – членов Европейского союза, что способствует улучшению взаимодействия, сотрудничества государств и дает возможность оказать эффективную правовую помощь.

Европейский союз разрабатывает различные подходы к обеспечению безопасности граждан в информационной среде. Информационные технологии и появление современных средств обработки и хранения информации чаще всего выступают причиной создания новых норм права и внесения поправок в существующие правовые акты для защиты граждан от возникающих угроз.

В настоящее время количество разнообразных устройств, которые обрабатывают информацию о человеке, растет с небывалой скоростью. Понятие личного пространства человека стало значительно расширяться в связи с развитием современных технологий. Отдельные сферы жизни человека постепенно переходят в онлайн-пространство. Современные телефоны используют отпечатки пальцев и изображения лиц для идентификации пользователя. Системы видеонаблюдения фиксируют и обрабатывают изображения лиц и тел людей для их последующего распознавания. Электронные браслеты анализируют частоту сердцебиений, активность и привычки в течение всего дня. Голосовые помощники обрабатывают голосовые запросы для возможности последующего ответа на них. Новая коронавирусная инфекция также внесла коррективы в повседневную жизнь людей. Государства используют различного рода технические устройства для осуществления контроля за социальным дистанцированием, использованием защитных масок для лица, температурой тела человека.

По справедливому мнению И. Л. Бачило, сегодня нельзя обойти проблему правового режима такого класса информации, как биоинформация: отпечатки пальцев, зрачков глаз человека, его ДНК и другие элементы индивида, широко используемые в практике идентификации субъекта в самых разных областях его жизни и отношений с другими субъектами [1, с. 138].

В силу процесса глобализации подобная информация теряет национальную принадлежность и государства не распространяют на нее свою юрисдикцию, так как в принципе порой невозможно определить собственника информации. Таким образом, такое большое количество персональной информации требует надежной защиты и сохранности, потому что даже при правомерном обороте персональных данных может возникнуть риск неправомерного их использования, что повлечет за собой нарушение неприкосновенности частной жизни лица.

Однако одной из главных проблем в данной области является отсутствие понимания четких критериев относимости той или иной информации к биометрической. Институт биометрических данных сложен в связи с тем, что он является предметом изучения различных наук, представители которых различно определяют данную область и ее содержание.

Например, И. Ф. Фейсханов и Л. Э. Арсланова отмечают, что биометрические персональные данные – это сведения, полученные человеком с рождения и неизменно находящиеся с ним [3, с. 241].

По мнению Г. А. и М. В. Двоеносовых, в основе биометрических данных находится биометрическая информация, под которой понимается биологическая информация, которая в зафиксированном виде приобретает значение социальной, поскольку относится к персональным данным [2, с. 83].

Зарубежные исследователи придерживаются мнения, что биометрические данные не только представляют собой информацию о человеке, но и выступают способом обеспечения уникальной связи данной информации с конкретным лицом и, следовательно, могут служить идентификатором определенного лица [4, с. 302].

Правовое регулирование сферы защиты персональных и биометрических данных сформировалось не сразу. Очень долгое время отсут-

ствовало разграничение между указанными типами данных. Первоначально защита личных данных осуществлялась на национальном уровне. Одним из первых актов в области защиты личной информации стал закон о защите данных, принятый в федеральной земле Гессен в 1970 г[1]. Вскоре, в 1973 г., был принят аналогичный закон в Швеции[2], в 1978 г. во Франции вступил в силу закон «Об обработке данных, файлах данных и индивидуальных свободах»[3]. Таким образом, правовое регулирование данной области общественных отношений прежде всего осуществлялось отдельными странами и носило внутригосударственный характер.

В дальнейшем развитие компьютерных технологий, появление сети Интернет и новых технологических устройств способствовали разработке первых международных актов. Так, в 1981 г. была принята Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, или так называемая Конвенция 108. Данная Конвенция стала первым международным актом по защите данных, имеющим юридически обязательное значение[4].

Существующие национальные правовые акты о защите персональных данных послужили основой для создания региональных международно-правовых документов.

24 октября 1995 г. Европейским парламентом и Советом Европейского союза принимается Директива 95/46/ЕС «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных»[5].

Директивой были заложены принципы, направленные на защиту прав граждан при обработке персональных данных на территории Европейского союза. В документе были предусмотрены создание надзорных органов, технические меры по обеспечению сохранности и конфиденциальности информации. Директива систематизировала нормы в области защиты информации, закрепила понятийный аппарат и послужила толчком для последующего сотрудничества стран в Европейском союзе. В дальнейшем на территории Европейского союза стали появляться и иные акты в области охраны персональных данных в различных сферах, но они зачастую не носили комплексного характера[6].

В 2009 г. происходит кардинальное реформирование системы Европейского союза путем принятия Лиссабонского договора о внесении изменений в Договор о Европейском союзе и Договор об учреждении Европейского сообщества, или так называемый Лиссабонский договор, или Договор о реформе[7]. Данный документ был призван заменить не вступившую в силу Конституцию Европейского союза и внести изменения в основополагающие договоры данной международной организации. Благодаря Лиссабонскому договору Хартия Европейского союза по правам человека становится юридически обязательным документом[8], а новая редакция Договора о функционировании Европейского союза вступает в силу[9]. В целях гармонизации защиты прав граждан Хартия Европейского союза по правам человека и Договор о функционировании Европейского союза закрепили отдельные права граждан по защите персональных данных.

Однако во всех вышеперечисленных документах не была зафиксирована концепция биометрических данных, что обусловливается особенностями развития научно-технического прогресса и отсутствием широкого распространения биометрических технологий.

С 25 мая 2018 г. на территории Европейского союза начал действовать Регламент «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/

[1] Das Datenschutzgesetz des Landes Hessen 7 Oktober 1970/ URL: http://starweb.hessen.de/cache/GVBL/1970/00041.pdf#page=1 (дата обращения: 23.06.2021).

[2] The Data Act of 11 May 1973/ URL: https://www.ilo.org/dyn/natlex/natlex4.detail?p_lang=&p_isn=55767&p_classification=01 (дата обращения: 23.06.2021).

[3] On Data Processing, Data Files and Individual Liberties of 6 January 1978. URL: https://www.ssi.ens.fr/textes/a78-17-text.html (дата обращения: 23.06.2021).

[4] Конвенция о защите физических лиц при автоматизированной обработке персональных данных от 28 янв. 1981 г. URL: https://www.coe.int/ru/web/conventions/full-list/-/conventions/treaty/108 (дата обращения: 23.06.2021).

[5] On the protection of individuals with regard to the processing of personal data and on the free movement of such data: directive 95/46/EC of the European Parliament and of the Council of 24 October 1995. URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046 (дата обращения: 23.06.2021).

[6] On the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA: directive 2016/680 of the European Parliament and of the Council of 27 April 2016. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN (дата обращения 23.06.2021); On the protection of personal data processed in the framework of police and judicial co-operation in criminal matters: framework Decision 2008/977/JHA of 27 November 2008. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008F0977 (дата обращения: 23.06.2021).

[7] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community of 13 December 2007. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12007L%2FTXT (дата обращения: 23.06.2021).

[8] Charter of Fundamental Rights of the European Union of 7 December 2000 // URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT (дата обращения 23.06.2021).

[9] Treaty on the Functioning of the European Union of 25 March 1957. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT (дата обращения: 23.06.2021).

ЕС», или так называемый Общий регламент по защите персональных данных (General Data Protection Regulation (GDPR))[1]. Задача данного Общего регламента заключалась в замене всех существующих ранее актов в области защиты персональных данных единым документом.

Приняв Общий регламент, Европейский союз подтвердил значимость прав и свобод человека и гражданина, связанных с защитой неприкосновенности частной жизни и сохранностью персональных данных лиц. Нормы Общего регламента по защите персональных данных распространяются на территории всех стран – членов Европейского союза, а также на физических и юридических лиц третьих стран, которые занимаются сбором и обработкой персональных данных граждан Европейского союза.

Целью Общего регламента является создание условий для защиты персональных данных и разрешение противоречий, существующих в законодательстве стран – членов Европейского союза, путем установления общих правил.

Данный правовой акт внес ряд изменений в ранее существовавшие нормы о правовом регулировании защиты персональных данных. Документ зафиксировал понятийный аппарат, разграничил категории персональных данных и урегулировал вопросы их обработки. Были прописаны основополагающие принципы, которые применяются во всех сферах обработки персональных данных вне зависимости от вида обработки данных. В соответствии с Общим регламентом обработка персональных данных осуществляется на основании законности, справедливости, при наличии правомерных целей и способов обработки. Также должны соблюдаться правила целостности и конфиденциальности при изучении сведений для снижения возможных рисков нарушения прав и свобод человека и гражданина.

Общий регламент зафиксировал гарантии, в соответствии с которыми персональные данные хранятся не дольше срока, который необходим для достижения целей обработки данных, и при обнаружении неточных персональных данных они будут исправлены или удалены. Таким образом, данный акт призван установить баланс между эффективной защитой персональных данных и необходимостью обработки и использования информации компетентными субъектами.

Новшеством Общего регламента стало закрепление данных конфиденциального характера, таких как информация о сексуальной ориентации, здоровье, генетической и биометрической информации. До принятия данного документа в европейском праве не существовало четкой концепции биометрических данных и способов их обработки.

В соответствии с Общим регламентом по защите персональных данных под биометрическими данными понимаются персональные данные, полученные в результате специальной технической обработки, относящиеся к физическим, физиологическим или поведенческим характеристикам физического лица, которые позволяют произвести или подтверждают уникальную идентификацию этого физического лица, такие как изображения лица или дактилоскопические данные.

Проанализировав данное определение, мы можем установить следующие признаки, присущие биометрическим данным.

Во-первых, биометрические данные – это разновидность персональных данных. Общий регламент по защите персональных данных также содержит понятие персональных данных, под которым понимается любая информация, относящаяся к субъекту данных, т. е. идентифицированному или поддающемуся идентификации физическому лицу, а, в свою очередь, поддающееся идентификации физическое лицо – это лицо, которое можно прямо или косвенно идентифицировать, в частности, посредством ссылки на идентификатор, такой как имя, идентификационный номер, данные о местоположении, онлайновый идентификатор или один или несколько факторов, специфичных для физической, физиологической, генетической, умственной, экономической, культурной или социальной идентичности этого физического лица.

Определение персональных данных трактуется Общим регламентом максимально широко. К персональным данным относят любую информацию, которая характеризует лицо, указывает на конкретного человека и связана с ним. Так, к персональным данным можно отнести фамилию, имя и отчество; место и дату рождения; паспортные данные и т. п.

Биометрические данные – это часть персональных данных, представляющая собой сведения о физиологических особенностях человека, его параметрах, которые позволяют установить личность. К таким данным относят отпечатки пальцев, изображение лица, радужную оболочку глаза и т. п.

В своей совокупности персональные и биометрические данные позволяют составить цельный образ человека и максимально точно его идентифицировать.

[1] 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): Regulation of the European Parliament and of the Council of 27 April 2016. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj (дата обращения: 23.06.2021).

Во-вторых, биометрические данные возможно получить при помощи специальных технических устройств. Биометрические данные представляют собой сведения, которые характеризуют физиологические и поведенческие особенности лица, и для их установления требуется применение специальных технических устройств.

Все подобные устройства работают на основе анализа особенностей человеческого лица и тела. Статические технические устройства, основываясь на физиологических признаках индивида, распознают лица, сетчатку глаз, отпечатки пальцев и т. п. Динамические (поведенческие) технические устройства оценивают поведенческую характеристику людей в процессе повторения лицом различных действий, например походку, голос, жестикуляцию и т. п.

Также специальные технические устройства могут использоваться в сочетании, когда оценивается несколько биометрических характеристик для более точной и комплексной идентификации лица.

В-третьих, биометрические данные относятся к физическому лицу и характеризуют физические, физиологические или поведенческие особенности человека.

Оценка биометрических данных представляет собой измерение различных характеристик человека для установления и проверки его личности. Подобная информация является уникальной, свойственной только конкретному физическому лицу, и характеризует физические, физиологические или поведенческие особенности человека.

Физические особенности человека подвержены изменчивости и характеризуют внешний облик, антропометрические данные и иные особенности лица. Например, к физическим особенностям человека относят возраст, рост, вес, пол и т. д.

Более уникальными и менее подверженными изменчивости являются физиологические особенности человека. Например, радужная оболочка и строение сетчатки глаза, отпечатки пальцев, группа крови, ДНК и т. д.

Поведенческие особенности человека проявляются в динамике и при совершении лицом каких-либо активных действий. Как уже упоминалось, к ним относятся походка, мимика, голос, жестикуляция, почерк и т. д.

В-четвертых, цель сбора биометрических данных заключается в идентификации человека.

Под биометрической идентификацией понимают процесс сравнения данных человека с биометрическими характеристиками для определения сходства, различий и установления истинной личности лица.

Одной из главных задач Регламента является унификация национальных правовых систем. Однако акт также предоставляет возможность государствам-членам принимать дополнительные условия для генетических, биометрических или медицинских данных. В странах Европейского союза были приняты отдельные законы о применении Регламента. Главная идея, которая прослеживается в данных законах, сводится к тому, что биометрические, генетические и медицинские данные могут быть подвергнуты обработке, но при условии соблюдения прав субъектов данных отношений, гарантий и мер безопасности, направленных на сохранность подобного рода информации[1].

Многие государства стали рассматривать биометрические данные как «чувствительный» вид персональных данных (sensitive data). Все биометрические данные имеют высокую степень уникальности и неповторимости, и такие устойчивые характеристики данных позволяют практически безошибочно идентифицировать конкретное лицо. В связи с этим анализ подобных данных должен производиться в ограниченных случаях с особой тщательностью и осторожностью и по общему правилу должен быть запрещен без наличия явно выраженного согласия со стороны исследуемого лица.

Сохранность персональных и биометрических данных должна быть гарантирована и наличием возможности для их защиты. На уровне Европейского союза функционирует Суд Европейского союза (European Court of Justice), представляющий собой институт судебной власти данной региональной организации. Особенностью данного Суда является то, что он не только правоприменительный орган, но правосоздающий. Благодаря деятельности Суда формируется прецедентное, или так называемое третичное, право Европейского союза, которое актуально для всех стран-членов и национальных судебных органов. Принимаемые Судом прецедентные решения призваны упорядочить и гармонизировать возникающие общественные отношения на территории Европейского союза для их единообразного понимания.

[1] Bundesdatenschutzgesetz, BDSG. 25 Mai 2018. URL: https://www.gesetze-im-internet.de/ bdsg_2018/index.html (дата обращения: 23.06.2021); Provisions for the Adaptation of the National Legislation to the Provisions of the General Data Protection Regulation 2016/679: decreto Legislativo 10 agosto 2018, n. 101. URL: https://www.gazzettaufficiale.it/eli/ id/2018/09/04/18G00129/sg (дата обращения: 23.06.2021).

Суд неоднократно отмечал, что защита персональных данных играет очень важную роль в реализации права на уважение частной жизни[1].

На практике возникают случаи, когда граждане Европейского союза пытаются защитить свое право в области сохранности своих персональных и биометрических данных. Интересен пример гражданина Германии, которому было отказано в возможности получения заграничного паспорта, так как он не согласился сдавать отпечатки своих пальцев[2]. В соответствии с Регламентом Совета Европейского союза 2252/2004 от 13 декабря 2004 г. о стандартах для средств защиты и биометрических данных в паспортах и проездных документах, выданных государствами – членами Европейского союза, документы для въезда и выезда с территории государств-участников должны иметь цифровые фото и отпечатки пальцев владельцев. Однако, по мнению данного гражданина, наличие его отпечатков пальцев представляет собой угрозу частной жизни и нарушает его право на защиту персональных данных. Суд Европейского союза постановил, что сбор отпечатков пальцев является обоснованной и законной мерой, необходимой для защиты общественных интересов и ограничения нелегального въезда на территорию Европейского союза.

Сбор индивидуальных данных граждан через мобильные устройства, личной информации от интернет-провайдеров, использование специальных приложений для геолокации с целью установления местонахождения лица стали одними из главных проблем современности в области защиты персональных данных граждан от злоупотреблений со стороны государств. В решении от 6 октября 2020 г. Суд Европейского союза постановил, что вмешательство государств в сферу фундаментальных прав, связанных с конфиденциальными данными лиц, должно осуществляться лишь при угрозе национальной безопасности, не должно носить массовый характер, а сбор информации должен быть ограничен определенным временем, целью сбора и осуществляться под надзором судебных и административных органов государства. Данное правило также распространяется на правоохранительные органы и спецслужбы государства[3].

Практика Суда подчеркивает верховенство европейского права и для обеспечения безопасности граждан и их персональных данных вводит общие правила, связанные с ограничением использования информации для защиты от возможных злоупотреблений со стороны государств и их органов.

Подобный подход приобретает все большую актуальность в связи с появлением новых информационных баз. В апреле 2019 г. Европейский парламент Европейского союза одобрил создание одной из крупнейших в мире баз биометрических данных – Общего хранилища идентификационных данных (Common Identity Repository (CIR)). Данная база объединит Шенгенскую информационную систему (Schengen Information System), Европейскую дактилоскопию (Eurodac), Визовую информационную систему (Visa Information System (VIS)). Кроме того, будут включены и три новые системы: Европейская система регистрации уголовных дел граждан третьих стран (European Criminal Records System for Third Country Nationals (ECRIS-TCN)), Система въезда/выезда (Entry/Exit System (EES)) и Европейская система информации и авторизации путешествий (European Travel Information and Authorisation System (ETIAS))[4].

Общее хранилище идентификационных данных будет содержать персональные и биометрические данные, необходимые для пограничных и правоохранительных органов с целью упрощения их работы и поиска необходимых лиц в объединенной системе, а не в разрозненных информационных базах.

В этой связи интересен проект от 21 апреля 2021 г., предлагаемый Европейской комиссией Европейского союза, связанный с ограничением использования искусственного интеллекта в областях, представляющих угрозу для защиты персональных, биометрических данных граждан Европейского союза[5]. В соответствии с документом, ограничения предусмотрены в зависимости от степени риска.

Неприемлемый риск (Unacceptable risk) – это области, где использование искусственного интеллекта будет запрещено в связи с угрозой безопасности и потенциальной возможностью нарушения прав людей. Например, это приложения, влияющие на поведение людей, и системы, позволяющие правительствам оценивать

[1] Decision of the Court in joined cases C-293/12 and C-594/12 Digital Rights Ireland of 8 April 2014. Para. 48. URL: https://curia.europa.eu/juris/liste.jsf?num=C-293/12 (дата обращения: 23.06.2021).

[2] Decision of the Court Judgment of the Court (Fourth Chamber) of 17 October 2013. URL: https://curia.europa.eu/juris/liste.jsf?num=C-291/12 (дата обращения: 23.06.2021).

[3] Decision of the Court in joined cases Case C-623/17 of 6 October 2020. URL: https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-10/cp200123en.pdf (дата обращения: 23.06.2021).

[4] Interoperability between EU border and security information systems: press release of 16 April 2019. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2018/628267/EPRS_BRI(2018)628267_EN.pdf (дата обращения: 23.06.2021).

[5] Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence: press release of 21 April 2021. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1682 (дата обращения: 23.06.2021).

социальные показатели граждан и формировать социальный рейтинг.

К областям высокого риска (High-risk) отнесены критические инфраструктуры (например, транспорт), которые могут поставить под угрозу жизнь и здоровье граждан; компоненты безопасности продуктов (например, применение искусственного интеллекта в роботизированной хирургии); государственные услуги (например, кредитная оценка, лишающая граждан возможности получить кредит); отправление правосудия (например, применение закона к конкретному набору фактов) и иные сферы.

Незначительный риск (Limited risk) возможен при использовании голосовых роботов и чат-ботов. Их применение будет возможно, если пользователь будет знать, что контактирует с искусственным интеллектом, а не человеком.

Системы с минимальным риском (Minimal risk) не представляют угрозы для безопасности граждан и не предполагают регулирования. Например, это видеоигры с поддержкой искусственного интеллекта или спам-фильтры.

Особое внимание уделяется технологиям, связанным с оценкой биометрии и распознаванием лиц. Они будут всесторонне анализироваться перед их использованием и сопровождаться подробной информацией о нюансах их применения для снижения возможных рисков.

Предлагается внести исключения, относящиеся к применению правоохранительными органами технологий по распознаванию лиц в общественных местах с целью поиска детей, преследования преступников и предотвращения террористических актов.

В целях осуществления контроля и подготовки рекомендаций для стран-членов в отношении новых внедряемых правил планируется создать Европейский совет по искусственному интеллекту (European Artificial Intelligence Board), объединяющий представителей стран – членов Европейского союза. В свою очередь, государства должны будут создать национальные органы для оценки рисков в области технологий с искусственным интеллектом, предусмотреть их сертификацию и инспектирование.

В данный момент документ находится на стадии рассмотрения, и для его принятия потребуется одобрение европейских институтов, а также время для создания необходимых дополнительных документов и органов.

Новые правила, предложенные Европейской комиссией, обусловлены актуальностью общественных процессов, протекающих на территории Европейского союза, развитием научно-технического прогресса и появлением новых технологий, требующих тщательного правового регулирования. Однако настоящим правилам не хватает конкретики, так как из предложенного проекта не ясно, каким образом будут оцениваться потенциальные риски в области нарушения прав человека, какие ограничительные меры будут использоваться по отношению к новым технологиям. Также могут возникнуть определенные сложности с сертификацией новых технологий на территории Европейского союза, их удорожанием, что повлечет увеличение срока для ввода в эксплуатацию новых разработок, а это, в свою очередь, может поставить в неравное положение создателей технологий с искусственным интеллектом в Европейском союзе и специалистов в этой сфере деятельности из других стран, где используются более мягкие способы регулирования данной сферы.

Таким образом, в настоящее время правовое регулирование сферы персональных и биометрических данных активно формируется и развивается путем принятия различных правовых актов как на уровне Европейского союза, так и на уровне стран-членов, устанавливающих единые правила по работе с персональными данными и информацией граждан.

Обработка биометрических данных сопряжена с высокими рисками возникновения нарушений прав отдельных лиц. В связи с этим работа с подобного рода информацией должна соответствовать определенной цели, иметь ограничения по объему обрабатываемых данных и по сроку их хранения для решения конкретных задач. Также требуется создание отдельного правового акта по защите физических лиц при обработке биометрических данных на уровне Европейского союза с целью единообразного регулирования подобных общественных отношений, складывающихся на территории государств-участников и защиты прав граждан.

СПИСОК ЛИТЕРАТУРЫ

1. Бачило И. Л. Информационное право : учебник для магистров. 3-е изд., перераб. и доп. М. : Юрайт, 2013. 576 с.

2. Двоеносова Г. А., Двоеносова М. В. Биометрия как наука, метод и способ документирования // Управление персоналом. 2009. № 11. С. 82–86.

3. Фейсханов И. Ф., Арсланова Л. Э. Некоторые аспекты защиты биометрических персональных данных в информационных системах : сб. докладов XIV Междунар. конф. Екатеринбург. 2020. С. 241–243.

4. Krausová A., Hazan H., Matejka J. Biometric Data Vulnerabilities: Privacy Implications // The lawyer quarterly. 2018. № 3. P. 295–305.

5. Koops B.-J. The Trouble with European Data Protection Law // International Data Privacy Law. 2014. P. 250–261.

REFERENCES

1. Bachilo I.L. *Informacionnoe parvo: uchebnik dlya magistrov*. [Information law: textbook for masters]. Moscow, Yurait Publ., 2013, 576 p. (in Russian)

2. Dvoenosova G.A. Biometriya kak nauka metod i sposob dokumentirovaniya [Biometrics as a science, method and method of documentation]. *Upravlenie personalom* [Personnel management], 2009, vol. 11, pp. 82-86. (in Russian)

3. Feishanov I.F. Nekotorie aspekti zaschiti biometricheskih personalnih dannih v informacionnih sistemah [Some aspects of the protection of biometric personal data in information systems]. *Sbornik dokladov XIV Mejdunarodnoi konferencii*. [Collection of reports of the XIV International Conference. Ekaterinburg], 2020, pp. 241-243. (in Russian)

4. Krausová A., Hazan H., Matejka J. Biometric Data Vulnerabilities: Privacy Implications. The lawyer quarterly. 2018, no. 3, pp. 295-305. (in English)

5. Koops B.-J. The Trouble with European Data Protection Law. International Data Privacy Law, 2014, pp. 250-261. (in English)

Legal Regulation of the Turnover of Biometric Data of Citizens in the European Union

© Kolosov A. V., 2021

Ensuring the security of a person and society is one of the priority and important areas of activity of any legal state. Measures aimed at countering crime and combating offenses in the information sphere are impossible without interaction and cooperation between states, since such violations are of a cross-border nature. The article examines the activities of the European Union, which is of interest due to the unique form of cooperation in the field of information interaction of the member states and the use of the latest identification technologies to create the European security space. The legal regulation of the protection of personal and biometric data is considered, the comparison of these terms is carried out. The features inherent in biometric data are highlighted. Special attention is paid to the analysis of the Regulation «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 (GDPR)). It was found that the innovation of the Regulation was the consolidation of special confidential data, the concept of biometric data and methods of their processing in European practice. The modern practice of the Court of Justice of the European Union in the field of protection of personal and biometric data of citizens is analyzed. The article examines the current trends in the development of European law in terms of creating a biometric database - Common Identity Repository (CIR)) and a project related to limiting the use of artificial intelligence in areas that pose a threat to the protection of personal, biometric data of citizens of the European Union. It is concluded that the processing of biometric data is associated with high risks of violations of the rights of individuals, and work with this kind of information should meet a certain goal, have restrictions on the volume of processed data and on the duration of their storage for solving specific tasks.

Keywords: personal data, biometric data, General Data Protection Regulation, sensitive data, Common Identity Repository, artificial intelligence.