Федеральное государственное автономное образовательное учреждение высшего образования «Московский государственный юридический университет имени О.Е. Кутафина (МГЮА)»

На правах рукописи

Завацкая Янина Викторовна

Регулирование использования биометрических данных в праве Европейского Союза

5.1.5. Международно-правовые науки (юридические науки)

Диссертация на соискание ученой степени
кандидата юридических наук

Научный руководитель:
доктор юридических наук, профессор
Калиниченко Пауль Алексеевич

Москва — 2025

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ 3

ГЛАВА 1. ИСПОЛЬЗОВАНИЕ БИОМЕТРИЧЕСКИХ ДАННЫХ В ПРАВЕ ЕВРОПЕЙСКОГО СОЮЗА: ИСТОРИЧЕСКИЙ И ТЕОРЕТИЧЕСКИЙ АСПЕКТЫ 20

§ 1.1. Формирование и развитие правового регулирования использования биометрических данных в Европейском Союзе 20

§ 1.2. Биометрические данные в системе защиты персональных данных Европейского Союза 43

ГЛАВА 2. ИСТОЧНИКИ РЕГУЛИРОВАНИЯ ИСПОЛЬЗОВАНИЯ БИОМЕТРИЧЕСКИХ ДАННЫХ В ПРАВЕ ЕВРОПЕЙСКОГО СОЮЗА 68

§ 2.1. Источники права Европейского Союза как основа регулирования использования биометрических данных 68

§ 2.2. Регулирование использования биометрических данных в национальном законодательстве государств — членов ЕС 85

§ 2.3. Международно-правовые основы регулирования использования биометрических данных в Европейском Союзе 94

ГЛАВА 3. СОВРЕМЕННЫЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ПРАВОВОЙ ОХРАНЫ БИОМЕТРИЧЕСКИХ ДАННЫХ: ОПЫТ ЕВРОПЕЙСКОГО СОЮЗА 116

§ 3.1. Использование биометрических данных в целях обеспечения частной, общественной и государственной безопасности в Европейском Союзе 116

§ 3.2. Охрана биометрических данных в Европейском Союзе в контексте обеспечения прав человека 155

ЗАКЛЮЧЕНИЕ 179

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 183

ВВЕДЕНИЕ

Актуальность темы исследования. Прогрессивное развитие биометрических технологий приводит к масштабному их внедрению во все сферы жизнедеятельности общества. Биометрические системы внедряются в банковском секторе, бизнесе, социальной сфере, сфере пограничного контроля, а также используются для обеспечения безопасности государства и граждан. Популярность биометрических данных как средства технологической индивидуализации человека обусловлена высокой эффективностью. Биометрические данные, такие как отпечатки пальцев или радужная оболочка глаза, представляют собой уникальные и надежные способы идентификации личности, что делает их использование востребованным для обеспечения защиты личной информации и безопасности на всех уровнях.

Вопросы использования биометрических данных в целях обеспечения безопасности являются предметом обсуждения многих организаций и объединений международного уровня. В преддверии саммита БРИКС (22–24 октября 2024 г.) Президент РФ В. В. Путин в выступлении упомянул о необходимости создания в перспективе единой цифровой инфраструктуры БРИКС и подчеркнул, что «здесь, конечно, важно определить согласованные подходы бизнеса, общественности, профильных органов власти по использованию биометрии, обеспечению информационной безопасности»[1].

Информационная безопасность в контексте биометрии характеризуется привычными операциями с биометрическими данными, которые позволяют упростить процессы аутентификации и авторизации, сокращая время и усилия, необходимые для доступа к различным устройствам и сервисам или проверок на пограничном контроле. Однако использование таких средств индивидуализации способно влиять на реализацию основных прав и свобод человека.

[1] Выступление Президента Российской Федерации В. В. Путина на пленарном заседании Делового форума БРИКС 18 октября 2024 г. [Электронный ресурс] // URL: http://kremlin.ru/events/president/news/75347 (дата обращения 18.10.2024).

В рамках предупреждения распространения COVID-19 в 2020 г. силы европейских стран были брошены на обеспечение соблюдения гражданами государств-членов карантинных мероприятий и отслеживание их передвижения посредством биометрических систем. Кроме того, отметим прекращение консульствами некоторых государств — членов ЕС (Дания, Италия) приема заграничных паспортов старого образца (без электронного носителя биометрической информации) и отказ Чехии с 2024 г. во въезде гражданам Российской Федерации на свою территорию без биометрического паспорта, расцененный Министерством иностранных дел РФ как одна из очередных антироссийских дискриминационных мер[2]. Правомерность указанных инициатив государств — членов ЕС ставится под вопрос в контексте возможного нарушения прав человека и дискриминации.

Европейский Союз (ЕС) — интеграционное объединение, которое основывается на общих принципах уважения человеческого достоинства, свободы, демократии, недискриминации и равенства полов, справедливости и солидарности[3]. В ЕС разработаны и действуют нормы по защите персональных данных, в том числе Регламент (ЕС) от 27 апреля 2016 г. 2016/679 о защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных, отменяющий Директиву от 24 октября 1995 г. 95/46/ЕС (далее — Регламент 2016/679, Регламент о защите данных)[4], который установил общие стандарты обработки биометрических данных.

Кроме того, на использование биометрических данных в ЕС оказывают влияние акты ЕС, регулирующие иные смежные общественные отношения, например Регламент (ЕС) от 13 июня 2024 г. 2024/1689, устанавливающий единые правила в области искусственного интеллекта (далее — Регламент об ИИ)[5], а также

---

[2] Брифинг официального представителя МИД России М. В. Захаровой. Москва, 21 августа 2024 г.

[3] Кашкин С. Ю., Калиниченко П. А., Четвериков А. О. Право Европейского союза : учебник для вузов / под ред. С. Ю. Кашкина. 5-е изд., перераб. и доп. М. : Юрайт, 2024. С. 86.

[4] 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) // OJ. 4.5.2016. L 119. P. 1–88.

[5] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No. 300/2008, (EU) No. 167/2013, (EU)

международные стандарты безопасности и защиты данных и нормы национального законодательства государств — членов ЕС, которые они вправе самостоятельно принимать в части установления особого правового регулирования обработки биометрических данных.

Несмотря на наличие в правовых актах ЕС специальных норм о персональных данных и в меньшей степени о биометрических данных, на практике в регулировании использования биометрических данных существуют новые вызовы и проблемы. Современные инновационные достижения в геномных исследованиях[6], разработке и применении технологий искусственного интеллекта, развитии цифровой среды и платформенных решений[7] порождают новые парадигмы регулирования данной сферы. Как отмечает профессор А. В. Корнев, цифровые технологии серьезным образом меняют сферу права в целом и юридическую деятельность в частности, вызывая новые проблемы и риски[8].

«Изменяется и характер социальности, — подчеркивает профессор В. Н. Синюков, — в него постепенно входят на правах субъектов и новых нетипичных объектов явления, по старой юридической классификации имеющие неживой, не субъектный и не объектный характер, — инженерия генома, биотехнологии, Интернет, искусственный интеллект»[9].

Отсюда возникла необходимость комплексного рассмотрения вопросов, связанных с регулированием биометрических данных в праве ЕС.

Степень разработанности темы исследования. Правовое регулирование биометрических данных в силу набранной значимости и актуальности является одним из популярных направлений как в зарубежной, так и в отечественной науке. За последние 10 лет по данной теме опубликовано немалое количество

No. 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (text with EEA relevance) // OJ. 12.7.2024. L 2024/1689.

[6] См. подробнее: Дубов А. Б., Калиниченко П. А. Правовые парадигмы регулирования исследований и разработок в области человеческого генома и их практического использования в России и за рубежом. Часть I // Вестник Университета имени О.Е. Кутафина (МГЮА). 2021. № 7. С. 61–69.

[7] Кашкин С. Ю., Алтухов А. В. В поисках концепции правового регулирования искусственного интеллекта: платформенные правовые модели // Вестник Университета имени О.Е. Кутафина (МГЮА). 2020. № 4. С. 26–40.

[8] Корнев А. В. Юридическая деятельность в цифровую эпоху: понятие, содержание, формы // Актуальные проблемы российского права. 2021. Т. 16. № 6. С. 28.

[9] Синюков В. Н. Цифровое право и проблемы этапной трансформации российской правовой системы // Lex Russica. 2019. № 9 (154). С. 9–18.

специальных исследований. Однако эти исследования посвящены отдельным аспектам регулирования биометрических данных и не представляют собой полный системный анализ регулирования данной сферы в ЕС.

В современной отечественной науке общим вопросам определения и регулирования оборота биометрических данных в ЕС посвящена работа А.В. Колосова. Анализ основ правового регулирования использования удостоверяющих личность документов с биометрическими данными в ЕС составляет один из разделов объемного исследования профессора А.Г. Волеводза, посвященного международной и отечественной практике применения таких документов и проблемах его регулирования. Правовой режим, особенности правового регулирования в государствах-членах ЕС и проблемы охраны биометрических данных рассматриваются в разных публикациях М.С. Кривогина. Вопросы охраны прав человека при использовании биометрических данных также освещены в специальном исследовании В.В. Архипова и В.Б. Наумова. Биометрические данные в контексте персональных данных и вопрос об их соотношении с генетической информацией являются предметом исследований А.В. Минбалеева и И.М. Рассолова.

Среди зарубежных трудов отметим труды К. Джассеран (C. Jasserand), Е. Киндт (E. Kindt) и Е. Мордини (E. Mordini), подробно анализирующие правовую природу, сущность, правовой режим биометрических данных.

Зачастую современными специалистами в области информационной безопасности и защиты данных биометрические данные рассматриваются поверхностно с точки зрения регулирования специальной категории данных, такой же как генетические данные или информация о здоровье. Фундаментальных научных трудов, раскрывающих особенности использования именно биометрических данных, как в отечественной, так и в зарубежной литературе чрезвычайно мало. Авторы главным образом рассматривают биометрические данные в общем контексте с персональными данными[10] либо исследуют

[10] См., например: Шадрин С. А. Правовое регулирование защиты персональных данных в Европейском союзе: генезис и перспективы развития : автореф. дис. ... канд. юрид. наук. Казань, 2019.

технические аспекты использования биометрической информации[11], не уделяя внимания вопросам понятийно-категориального аппарата биометрических данных, основным его характеристикам, особенностям правовой природы данного вида конфиденциальной информации.

Гораздо меньше внимания в научной литературе уделено вопросам охраны биометрических данных в ЕС в контексте обеспечения прав человека и проблемам использования биометрических данных в целях обеспечения безопасности, которые позволяют сформировать полноценную картину применения биометрических данных на практике.

При всем многообразии исследований проблем использования и защиты персональных данных в ЕС очевидно отсутствие в современной юридической науке комплексного сравнительно-правового анализа регулирования использования биометрических данных, который представлен в настоящей работе.

Объектом настоящего исследования выступает совокупность общественных отношений, возникающих в связи с использованием биометрических данных в ЕС — как на уровне интеграционного объединения, так и на уровне государств — членов ЕС и их граждан.

Предмет настоящего исследования составляют положения правовых актов ЕС, в том числе учредительных договоров, а также институтов ЕС, национальное законодательство государств — членов ЕС, материалы судебной практики и иные источники права, определяющие статус биометрических данных и правила их использования, а также международно-правовые документы в области безопасности и защиты прав и основных свобод человека. Предмет исследования также образуют доктринальные источники и научные подходы, отражающие сущность биометрических данных и практические правовые проблемы их использования.

Цель и задачи исследования. Цель диссертационной работы — выявление исторических и современных особенностей регулирования использования

[11] Галяшина Е. И. Теоретические и прикладные основы судебной фоноскопической экспертизы : дис. … докт. юрид. наук. Воронеж, 2002.

биометрических данных в праве ЕС и возникающих в рамках этого регулирования практических проблем, а также формулирование соответствующих рекомендаций для России и интеграционных объединений с ее участием по принятию правовых мер в рамках совершенствования международного сотрудничества в данной области на основе опыта ЕС.

Данная цель обусловливает постановку и решение следующих **задач**:

1) изучение истории формирования и развития правового регулирования использования биометрических данных в ЕС, установление предпосылок развития правового регулирования в данной области;

2) исследование определения понятия «биометрические данные» в отечественной и зарубежной доктрине и источниках права ЕС, определение содержания исследуемой категории, а также установление места биометрических данных в системе персональных данных ЕС;

3) изучение источников права ЕС как основы регулирования использования биометрических данных (источники первичного права, вторичного права, прецедентного права), а также анализ национального законодательства государств-членов и международно-правовых источников в этой части и практики Европейского суда по правам человека (далее — ЕСПЧ);

4) анализ компетенций ЕС в сфере регулирования биометрических данных;

5) определение современных проблем регулирования биометрических данных в праве ЕС в контексте обеспечения прав человека и безопасности;

6) анализ современного состояния сотрудничества России и ЕС по вопросам миграции, визовой политики, взаимодействия правоохранительных органов и в иных сферах посредством обмена биометрическими данными граждан, выработка предложений по совершенствованию такого сотрудничества.

Теоретическую основу исследования составляют прежде всего труды представителей отечественной правовой науки в области международного права, европейского и интеграционного права, теории права, конституционного, информационного права и др., среди которых А. Х Абашидзе, С. С. Алексеев,

Л. П. Ануфриева, К. А. Бекяшев, П. Н. Бирюков, А. В. Бутрина, М. Ю. Велижанина, И. А. Вельдер, А. Г. Волеводз, Е.Е. Гуляева, А. В. Исполинов, П. А Калиниченко, С. Ю. Кашкин, Е. В. Киселева, А. В. Корнев, О. Е. Кутафин, И. И. Лукашук, Е. К. Матевосова, И. В. Микурова, А. В. Минбалеев, А. П. Мовчан, Н. А. Молчанов, М. В. Некотенева, Е. Ю. Покаместова, И. М. Рассолов, В. Н. Синюков, Н. А. Соколова, Э. В. Талапина, О. В. Танимов, Г. И. Тункин, С. В. Черниченко, А. О. Четвериков, С. Г. Чубукова, С. А. Шадрин, Л. М. Энтин, М. Л. Энтин, Ю. М. Юмашев.

Яркими представителями зарубежной юридической науки в области персональных данных, в том числе биометрических данных выступили К. Абботт (K. Abbott), К. Джассеран (C. Jasserand) и Е. Киндт (E. Kindt), а также Д. Бастард (J. Bustard), А. Мариан (A. Marian) и Т. Холл (T. Hall). Как можно заметить, несмотря на неоспоримую актуальность проблемы охраны биометрических данных, число зарубежных специалистов и работ, освещающих исследуемую автором категорию персональных данных, незначительно. В рамках анализа вопросов о соблюдении прав ребенка в сфере миграционного контроля с применением биометрических данных автор обращался к правовым исследованиям М. Ридль (M. Riedl) в этой области. При исследовании роли источников мягкого права в регулировании использования биометрических данных автор обращался к работам Л. Сенден (L. Senden), Д. Снидал (D. Snidal), К. Эббот (K. Abbot) и Д. Шелтона (D. Shelton).

Методологическую основу исследования составили общенаучные методы познания, а также специальные способы и приемы, применяемые в юридических науках: диалектический, исторический методы, метод логической дедукции и индукции, системный подход, сравнительный (сравнительно-правовой), формально-юридический методы и др.

Диалектический метод применялся автором при установлении степени влияния источников международного права и национального законодательства государств — членов ЕС на регулирование использования биометрических данных. Сравнительно-правовой метод был задействован при сопоставлении норм

права ЕС и актов «мягкого права» и формулировании выводов о роли этих источников в формировании режима использования биометрических данных.

Нормативная и эмпирическая база исследования.

Нормативную основу исследования составили в первую очередь положения действующих учредительных документов ЕС (Договор о Европейском Союзе 1992 г. (далее — ДЕС), Договор о функционировании Европейского Союза 1957 г. в редакции Лиссабонского договора 2007 г. (далее — ДФЕС)), Хартии Европейского Союза об основных правах 2000 г., регламентов, директив и других нормативных актов, изданных институтами ЕС, судебной практики ЕС, а также международных договоров. Большое значение для исследования рассматриваемой темы имела практика Суда ЕС.

Важное место в определении тенденций и перспектив правового регулирования биометрических данных заняло изучение рекомендательных актов «мягкого права» как институтов ЕС, так и международных организаций.

В ходе исследования был проанализирован научный и практический материал, затрагивающий различные аспекты использования биометрических данных в ЕС. Нормативную основу диссертации составили более 60 нормативных актов ЕС правового и рекомендательного характера, а также решения Суда ЕС.

Научная новизна исследования. Новизна диссертационной работы обусловлена прежде всего ее предметом, целью и задачами. Она является первым в отечественной науке всесторонним исследованием регулирования использования биометрических данных в праве ЕС.

Настоящая диссертация выступает первым полным и комплексным сравнительно-правовым исследованием, которое специально посвящено выработке практических предложений, направленных на совершенствование правовых основ регулирования рассматриваемых правоотношений, на основе глубокого изучения теоретических, нормативных и практических материалов. В настоящем исследовании впервые в отечественной науке выведены особенности эволюции правового регулирования биометрических данных в ЕС, рассмотрены все уровни правового регулирования использования биометрических данных на

международном уровне и уровне ЕС, а также намечены пути дальнейшего совершенствования законодательства ЕС в данной сфере.

Автором введен в научный оборот новый теоретический материал, представляющий интерес как для науки европейского права, так и для других юридических наук, прежде всего международного и конституционного права.

На основе проведенного исследования автор **выносит на защиту следующие положения**.

1. Формирование правового регулирования биометрических данных на уровне ЕС параллельно развивается в двух направлениях:

— сфера безопасности;

— права человека и персональные данные, к нему относящиеся.

Такой подход обусловлен тем, что биометрические данные рассматриваются нами, с одной стороны, как инструмент защиты человека и общества (с точки зрения международных стандартов безопасности и соответствующих актов ЕС в этой сфере), с другой — как объект правовой защиты, направленной на минимизацию рисков нарушения прав человека (с точки зрения международных и региональных актов о правах человека и персональных данных).

С появлением новых стандартов в области безопасности возникают новые правовые категории и правоотношения, которые оказывают влияние на права человека и сферу защиты персональных данных. Таким образом, указанные сферы находятся в тесной взаимосвязи, а правовые нормы их регулирования дополняют друг друга, учитывая современные проблемы обеспечения частной, общественной и национальной безопасности, а также защиты прав человека и персональных данных.

2. Правовое регулирование биометрических данных в ЕС как категории персональных данных прошло три основных этапа, каждый из которых характеризуется постепенным ростом значимости внедрения биометрических данных в жизнь общества и необходимостью создания надежной правовой защиты их субъектов.

I этап: конец 1990-х — начало 2000-х гг. — этап интеграции первых международных стандартов в области безопасности и противодействия терроризму, в сфере прав человека и персональных данных в законодательстве ЕС. На данном этапе в законодательстве ЕС впервые употребляются такие термины, как «биометрия», «биометрические характеристики» или «идентификаторы». «Биометрических данных» как отдельной категории персональных данных еще не существует, вместо этого понятия чаще используются «отпечатки пальцев» или «изображение лица». Законодательство о персональных данных в этот период впервые отмечает прогресс в сфере информационных технологий, которые стали существенно упрощать обработку и обмен данными, и устанавливает соответствующие принципы обработки и защиты. Акты ЕС в области безопасности, в свою очередь, регулируют использование биометрических данных скорее с точки зрения технических аспектов, нежели как категории персональных данных, требующей особой правовой защиты.

II этап: 2007–2016 гг. — этап выделения биометрических данных в системе персональных данных и зарождения специального правового регулирования. Именно в 2007 г. на уровне ЕС была предпринята первая попытка дать определение биометрических данных как отдельной правовой категории.

На этот же этап приходятся изменения в учредительных договорах ЕС, связанные с вступлением в силу Лиссабонского договора, которые в последующем служат ориентиром при принятии актов как в области персональных данных, так и в области безопасности, а также закрепляют право каждого на защиту персональных данных и устанавливают соответствующие правила защиты в ЕС. Косвенно на данном этапе уже шла речь о необходимости предусматривать особые правила защиты таких данных, например в сферах судебного и полицейского сотрудничества, а также национальной безопасности.

В этот период формируются понятие и перечень биометрических данных, определяется их место в качестве категории данных, раскрывающей информацию о физическом лице, формулируются требования подлинности и надежности, а также необходимость соблюдения в отношении биометрических данных

требований об обеспечении безопасности персональных данных. В визовом законодательстве происходят обновления, создаются новые информационные системы для обмена данными в сфере пограничного контроля.

III этап: 2016 г. — настоящее время — современный период регулирования (специальное регулирование биометрических данных). Важнейшую роль на данном этапе сыграло принятие Регламента о защите данных, в соответствии с которым биометрические данные относятся к специальной категории персональных данных наряду с генетическими данными и данными о здоровье. Отдельной статьей предусмотрены условия обработки специальных категорий персональных данных. Все государства — члены ЕС приводят национальное законодательство в соответствие с требованиями Регламента, предусматривают правила обработки биометрических данных в различных отраслевых правовых актах.

Данный этап отмечается также разработкой и принятием в 2024 г. Регламента об ИИ, значительная часть которого посвящена применению биометрических систем и обращению с биометрическими данными. В сфере пограничного контроля и визового режима, полицейского и судебного сотрудничества продолжают разрабатываться и актуализироваться правила взаимодействия информационных систем по безопасному обмену данными.

На современном этапе сфера безопасности стремительно расширяется и уже не ограничивается только нормами в области противодействия терроризму, пограничного контроля или судебного и полицейского сотрудничества. Теперь безопасность — это безопасный доступ к помещениям, устройствам, банковским и прочим услугам с использованием биометрических данных граждан.

3. Регламент о защите данных содержит следующее определение биометрических данных: «Биометрические данные — это персональные данные, полученные в результате специальной технической обработки, относящиеся к физическим, физиологическим или поведенческим характеристикам физического лица, которые позволяют или подтверждают уникальную идентификацию этого физического лица, такие как изображения лица или дактилоскопические данные».

Данное определение является размытым. Современное определение биометрических данных в праве ЕС, по нашему мнению, должно исходить из реальных особенностей исследуемой категории данных.

Во-первых, биометрические данные — это персональные данные, в основе которых лежат уникальные и неотчуждаемые биологические характеристики индивида, представляющие собой исключительно эталонный образец биоматериала физического лица или изображения биологически уникального свойства человека, полученного посредством специальной технической обработки.

Определение биометрических данных должно исключать отнесение к ним физиологических, поведенческих, эмоциональных и других динамических характеристик, которые не являются постоянными и уникальными, а следственно, не позволяют провести высокоточную и однозначную идентификацию личности.

Во-вторых, биометрические данные считаются таковыми только при условии, если такие данные в процессе их сбора прошли специальную техническую обработку, способную их считать, записать и сохранить в том виде, в котором они представлены физическим лицом. Без такой обработки отпечатки пальцев считались бы просто дактилоскопическими данными, а изображение лица — обыкновенной фотографией.

В-третьих, определение биометрических данных должно содержать закрытый перечень таких данных, который может обновляться по мере необходимости в связи с новыми техническими возможностями биометрических систем.

4. Источники первичного и вторичного права ЕС обобщенно затрагивают использование биометрических данных, в основном регулируя общие принципы защиты биометрических данных и отдельные вопросы их получения и обработки. Однако значительной проблемой регулирования использования биометрических данных в праве ЕС является сегментарный характер существующих норм, которые формируются не в специальном законодательстве, а в отдельных актах, регламентирующих иные сферы (удостоверяющие личность документы, полицейское и судебное сотрудничество, соблюдение требований визового и

миграционного законодательства, защита информации в сфере регулирования искусственного интеллекта).

Центральными актами в иерархии источников права ЕС, предусматривающих регулирование биометрических данных, являются регламенты о защите данных и об ИИ. Регламент о защите данных выступает своего рода ориентиром для остальных актов ЕС, которые в меньшей или большей степени содержат правила использования биометрических данных. Основанный на нем Регламент об ИИ более детально подходит к вопросам регулирования именно биометрических систем, а не биометрических данных. Кроме того, такое правовое регулирование не представляется полным и всесторонним, принимающим во внимание все сферы, в которых биометрические данные могут применяться.

5. Международные нормы универсального и регионального характера содержат базовые принципы и гарантии, которые служат основой формирования нормативных актов ЕС, предусматривающих правовое регулирование защиты прав человека вообще и персональных данных в частности. Однако анализ источников международного права, прямо или косвенно предусматривающих регулирование биометрических данных, показывает, что регулирование на данном уровне представляется дискретным и комплексного специального характера не имеет.

Анализ норм международного «мягкого права» говорит также о сегментарности регулирования использования биометрических данных: на международном уровне сегодня нет специального источника, который бы содержал необходимое правовое регулирование данной сферы. Обеспечить защиту биометрических данных от посягательств по всему миру, регулировать стандарты трансграничного обмена информацией и технические требования к сбору и обработке биометрических данных национальное право не способно. Это приводит к необходимости создания единой международной системы защиты персональных данных — универсальной конвенции об использовании биометрических данных, которая создала бы единый правовой понятийный аппарат и всеобщие правила регулирования биометрических данных и стала бы ориентиром как для ЕС, так и для других интеграционных объединений и государств, включая Евразийский

экономический союз (ЕАЭС) и Россию.

6. Правовое регулирование биометрических данных в области безопасности реализуется через совместную компетенцию ЕС с государствами-членами в сфере пространства свободы, безопасности и правосудия, закрепленной подпунктом «j» п. 2 ст. 4 и разделом V ДФЕС.

Основной блок правового регулирования в этой области чаще всего составляют акты ЕС о создании и функционировании специализированных систем обмена и хранения данных между судебными и правоохранительными органами, а также в сфере пограничного контроля и визового режима. Особое место в таких актах отводится биометрическим данным как единственному на сегодняшний день методу проведения высокоточной идентификации лиц. Например, «Прюмские достижения», «Дублинская система» и обновленная Европейская дактилоскопическая система (European Dactyloscopy System (EURODAC)) (далее — Евродак), которая на сегодняшний день стала биометрической, представляют собой комплекс правовых решений, являющихся одним из главных инструментов такого регулирования в рамках реализации судебного сотрудничества по уголовным делам и полицейского сотрудничества, охватываемого главами 2, 4 и 5 разд. V ДФЕС.

7. Действующее правовое регулирование биометрических данных не всегда коррелирует с общими принципами уважения и защиты прав человека, провозглашенными Уставом ООН, которые закреплены в международных и региональных договорах в области прав человека и хартиях. Использование современных биометрических систем на основе технологий искусственного интеллекта порождает ряд проблем, которые приводят к нарушению таких прав, как право искать убежище; свобода передвижения и проживания в государствах — членах ЕС; право на неприкосновенность частной жизни; равенство и недискриминация; свобода выражения мнений, собраний, ассоциаций; права ребенка и т.д.

Нарушения перечисленных прав в большинстве являются следствием следующих факторов.

Во-первых, в Регламенте о защите данных установлен общий запрет на обработку биометрических данных. Однако в закрытом перечне случаев данный запрет не применяется. Такие случаи характеризуются в основном необходимостью защиты интересов других лиц или защиты от серьезных трансграничных угроз здоровью, целями важного публичного интереса, осуществления правосудия и т.д. При этом согласие субъекта персональных не является необходимым условием обработки биометрических данных.

Кроме того, зачастую субъекты лишены возможности выразить отказ в предоставлении и обработке их биометрических данных, что обусловлено строгими требованиями некоторых актов ЕС или государств-членов в сфере безопасности, например о включении биометрических данных в удостоверяющие личность документы или в полицейское досье. В противном случае гражданину ЕС или гражданам третьих стран будет просто отказано в выдаче запрашиваемого документа.

Изложенное позволяет обозначить следующие проблемы влияния правового регулирования биометрических данных на права человека:

— проблему преобладания интересов общественности и безопасности над интересами и правами субъекта данных;

— проблему согласия на обработку персональных данных и возможности отказа.

Во-вторых, государства — члены ЕС вправе вводить дополнительные условия или ограничения в отношении обработки биометрических данных. Данное обстоятельство, на наш взгляд, наделяет правовое регулирование этой области неоднородностью и приводит к отсутствию на территории ЕС унифицированного подхода к использованию биометрических данных. Это влечет повышение количества споров в прецедентной практике Суда ЕС и ЕСПЧ относительно правомерности действий над биометрическими данными граждан в государствах — членах ЕС и соответствия норм национального законодательства государств-членов правовым актам ЕС в сфере персональных данных.

8. За долгие годы сложившегося сотрудничества России и ЕС в

правоохранительной деятельности и в сфере безопасности, в том числе в рамках визового диалога, иммиграционной политики и взаимодействия России с Европолом, между сторонами не заключено ни одного соглашения об использовании персональных данных общего характера, и в частности соглашения об обмене биометрическими данными. Полагаем, что в дальнейшем инициирование диалога со стороны России относительно возможности подготовки проекта и заключения подобного соглашения станет важным шагом в борьбе с преступностью и защите персональных данных.

На данном этапе представляется целесообразным заключение отдельных соглашений по обмену персональными / биометрическими данными между Россией и дружественными странами, входящими в состав международных организаций и интеграционных объединений, таких как Евразийский экономический союз (ЕАЭС), Организация Договора о коллективной безопасности (ОДКБ), Шанхайская организация сотрудничества (ШОС) и т.д.

Теоретическая значимость диссертационного исследования заключается в том, что благодаря проведенному анализу нормативного материала и доктринальных источников автор пришел к выводам о понятии, месте, сущности и особенностях регулирования биометрических данных. Полученные знания и результаты исследования могут использоваться при преподавании учебных дисциплин (модулей) в рамках освоения специальных курсов обучающимися по направлениям подготовки «Юриспруденция» уровней бакалавриата и магистратуры.

Практическая значимость работы определяется в первую очередь тем, что отдельные выводы, изложенные в ней, могут быть использованы в ходе межгосударственных переговоров по повышению эффективности международного сотрудничества по вопросам использования и защиты персональных данных. Положения настоящего исследования могут быть востребованы при разработке законодательных инициатив по устранению пробелов законодательства, регулирующего использование и защиту биометрических данных человека, как в ЕС, так и в Российской Федерации.

Настоящее исследование имеет важное практическое значение для пути России к совершенствованию собственной миграционной политики посредством введения мер, предусматривающих сбор биометрических данных иностранных граждан, осуществляющих въезд на территорию страны. Результаты исследования отражают реальную важность использования биометрических данных во взаимодействии России и ЕС при сборе биометрических данных граждан России для получения визы в страны Шенгенской зоны, а также в рамках организации сотрудничества правоохранительных органов в целях обеспечения общественной безопасности.

Степень достоверности и апробация результатов. Основные выводы и положения исследования основаны на всестороннем анализе достаточной теоретико-методологической базы. Теоретическая и нормативная основы исследования, изложенные в диссертационной работе, свидетельствуют о корректности и согласованности представленных положений.

Апробация результатов исследования выразилась в обсуждении различных аспектов темы диссертации на научно-практических конференциях, проводимых в Университете имени О.Е. Кутафина (МГЮА), а также в публикациях по исследуемой теме. По проблематике диссертации опубликовано четыре работы, в том числе три научных статьи — в изданиях, входящих в перечень Высшей аттестационной комиссии Министерства науки и высшего образования РФ.

Структура диссертационного исследования обусловлена его целями и задачами и включает введение, три главы, объединяющие семь параграфов, заключение и список использованных источников.

ГЛАВА 1. ИСПОЛЬЗОВАНИЕ БИОМЕТРИЧЕСКИХ ДАННЫХ В ПРАВЕ ЕВРОПЕЙСКОГО СОЮЗА: ИСТОРИЧЕСКИЙ И ТЕОРЕТИЧЕСКИЙ АСПЕКТЫ

§ 1.1. Формирование и развитие правового регулирования использования биометрических данных в Европейском Союзе

Сегодня биометрические данные граждан повсеместно используются в совершенно разных сферах жизни человека. Общественная безопасность, противодействие терроризму, миграционный контроль, банковский сектор, здравоохранение, охрана помещений – все эти сферы поддерживаются путем оснащения биометрическими системами идентификации. Совершая заграничную поездку с паспортом нового поколения или оплачивая покупку в супермаркете с применением функции «Face ID» на смартфоне, человек дает согласие на обработку биометрических данных, что стало привычным действием и неотъемлемой частью повседневной жизни. Вместе с тем такие данные являются уникальными по своей природе и составляют специальную категорию «чувствительных» персональных данных, что обусловливает необходимость их особой правовой защиты[12].

Исследование вопроса о формировании и развитии правового регулирования использования биометрических данных невозможно без краткого анализа становления самой биометрии и биометрической идентификации. Понятия «биометрия» и «биометрические данные» с исторической точки зрения неразрывно связаны[13].

В научной литературе термин «биометрия» рассматривается в трех аспектах. Биометрия как характеристика[14] подразумевает измеримые биологические (анатомические и физиологические) или поведенческие черты человека, которые могут быть использованы для автоматического распознавания. Биометрия как

---

[12] Кривогин М. С. Особенности правового регулирования биометрических персональных данных. С. 80.

[13] Newbold R. Newbold's Biometric Dictionary for Military and Industry. 2nd ed. NY : Authorhouse, 2008.

[14] Под характеристиками в данном случае понимаются собственно биометрические данные, полученные при помощи биометрических технологий.

процесс представляет собой автоматизированные методы распознавания личности на основе измеримых биологических (анатомических и физиологических) и поведенческих характеристик[15]. Наконец, «биометрия — это наука об идентификации или верификации личности по физиологическим или поведенческим отличительным характеристикам»[16] или «научная дисциплина, изучающая способы измерения различных параметров человека с целью установления сходства (различий) между людьми и выделения одного конкретного человека из множества других людей»[17].

Термин «биометрические данные» имеет более прикладное значение и представляет собой некий «биометрический образец, биометрический признак или биометрическое свойство»[18], под которыми сегодня понимаются измеряемые физические характеристики индивида или его персональные поведенческие черты, имеющие достаточную стабильность на прогнозируемый период возможных измерений и существенно отличающиеся от аналогичных параметров множества других людей[19].

Таким образом, в определенном контексте «биометрия» и «биометрические данные» могут считаться синонимами.

Некоторые ученые при исследовании вопроса о зарождении и эволюции правового регулирования использования биометрических данных делают акцент на отсутствии на протяжении долгого времени разграничения между биометрическими данными и персональными данными других видов[20], мотивируя это тем, что регулирование исследуемой категории данных берет начало в 1970-е гг., когда защита личных данных имела комплексный характер и осуществлялась только на национальном уровне[21]. Ими констатируется, что биометрические

---

[15] Jefferson R. B. Biometrics: Privacy, Progress and Government. New York : Nova Science Publishers, Inc., 2010.

[16] Болл Р. М., Коннел Дж. Х., Панканти Ш., Ратха Н. К., Сеньор Э. У. Руководство по биометрии. М. : Техносфера, 2007.

[17] Иванов А. И. Биометрическая идентификация личности по динамике подсознательных движений. Пенза : Изд-во Пенз. гос. ун-та, 2000.

[18] Иванов А. И. Указ. соч.

[19] Рассолов И. М., Чубукова С. Г., Микурова И. В. Биометрия в контексте персональных данных и генетической информации: правовые проблемы // Lex russica. 2019. № 1. С. 110.

[20] См. подробнее: Колосов А. В. Правовое регулирование оборота биометрических данных граждан в Европейском союзе // Сибирский юридический вестник. 2021. № 3 (94). С. 89–96.

[21] Колосов А. В. Указ. соч.

данные до принятия правовых норм, разграничивающих категории персональных данных, подпадали под общее правовое регулирование личных данных, с чем нельзя не согласиться.

Действительно, одним из первых актов в области защиты личной информации, который был принят на территории стран ЕС, стал Закон о защите данных 1970 г. федеральной земли Западной Германии Гессен[22]. Документ носил локальный характер и действовал только на территории данной земли. Затем в 1973 г. был принят аналогичный закон в Швеции[23], в 1978 г. вступил в силу Закон «Об обработке данных, файлах данных и индивидуальных свободах», принятый во Франции[24].

Этот же подход лег в основу разработки первых международных актов в области защиты данных, а именно Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных (Конвенции 108)[25]. Более того, он же отразился и в нормативных актах ЕС, в частности в Директиве от 24 октября 1995 г. 95/46/ЕС (далее — Директива 95/46/ЕС)[26], действовавшей до 2018 г., и сменившем ее Регламенте о защите данных.

Относительно становления правового регулирования использования биометрических данных существуют различные точки зрения. Одни авторы говорят о том, что данная категория получила развитие в XX в. в рамках прикладных наук[27]. Другие исследователи говорят о более раннем внимании законодателя к внедрению биометрических технологий и нескольких этапах эволюции рассматриваемого понятия.

Сторонники первого подхода рассматривают биометрические данные как результат технологического прогресса, как инструмент автоматизации процессов и

---

[22] Das Datenschutzgesetz des Landes Hessen vom 7. Oktober 1970.

[23] The Data Act of 11 May 1973.

[24] Act 78-17 on Data Processing, Data Files and Individual Liberties of 6 January 1978 (Data Protection Act) // BGBl. 1978. No. 565.

[25] Конвенция о защите физических лиц при автоматизированной обработке персональных данных (заключена в Страсбурге 28 января 1981 г.) // СЗ РФ. 2014. № 5. Ст. 419.

[26] 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 // OJ. 23.11.1995. L 281. P. 31–50.

[27] Галяшина Е. И. Теоретические и прикладные основы судебной фоноскопической экспертизы : автореф. дис. ... докт. юрид. наук. Воронеж, 2002. С. 8.

систем идентификации, который появился в XX в. с развитием новых технологий и сделал возможным использование персональных данных в различных направлениях юриспруденции[28]. Согласно данной концепции, правовое регулирование применения биометрических технологий началось в 1970-е гг., когда таковые стали использоваться в криминалистике для формирования доказательственной базы и поимки преступников. Данная концепция представляется оправданной в контексте вышеприведенных примеров правового регулирования персональных данных и использования биометрии для идентификации личности.

Другие авторы говорят о нескольких этапах развития правового регулирования биометрических данных. По мнению Е. Г. Барковской, первый период берет начало с древних времен и продолжается до 1990-х гг., когда в качестве одного из способов получения информации для идентификации человека использовался метод описания признаков его внешности (в частности, данных о цвете коже, форме лица, размере отдельных частей лица и особых приметах) в судебных материалах, на основе которых осуществлялся розыск преступников[29].

Второй этап, по мнению автора, ознаменован первым применением научного подхода в исследовании и фиксации биометрии. Так, в этот период начал использоваться бертильонаж — система идентификации преступника по численным данным антропометрических параметров и их совокупным пропорциям[30], а третий этап начинается с середины и заканчивается в конце XX в. и связан с развитием новых технологий и разработкой новейших методик, с помощью которых стало возможным осуществить автоматизацию системы идентификации на основе обработки звукового сигнала при помощи компьютерных систем[31]. В ходе четвертого этапа, который начался в 2000-х гг. и продолжается до сих пор, осуществляется повсеместное внедрение

---

[28] Галяшина Е. И. Теоретические и прикладные основы судебной фоноскопической экспертизы : автореф. С. 8.

[29] Барковская Е. Г. Исторические предпосылки и практические потребности интеграции биометрического и криминалистического знания // Философия права. 2010. № 6. С. 28.

[30] Набиев Р. Ф., Горяев Э. Э. Бертильонаж: славное прошлое и возможные перспективы // Ученые записки Казанского юридического института МВД России. 2019. Т. 4. № 2 (8). С. 78.

[31] Галяшина Е. И. Теоретические и прикладные основы судебной фоноскопической экспертизы : автореф.

биометрических технологий в системы глобальной защиты человечества от угрозы мирового терроризма. На данном этапе разрабатываются всё новые методы идентификации человека по различным его динамическим и поведенческим признакам: походке, жестикуляции, мимике, артикуляции речевого аппарата, динамике воспроизведения подписи, динамике работы на клавиатуре (клавиатурный почерк) и др.[32]

Данная теория о длительной эволюции биометрической идентификации находит поддержку и в зарубежной научной литературе. Так, ученые М. Смит и С. Миллер аналогично приходят к выводу, что первое известное применение формы биометрической идентификации имело место в Древнем Египте, затем получило развитие в достижениях Ф. Гальтона и Э. Генри[33] и стало центральным инструментом идентификации в уголовном расследовании в 1980-х гг.[34] По мнению исследователей, последним этапом эволюции использования биометрических технологий является период с середины 2000-х гг. по сегодняшнее время, когда идентификация по отпечаткам пальцев широко используется вне правоохранительных органов и интегрируется в сферу пограничного контроля[35].

Концепции, предусматривающие развитие биометрических данных с древних времен, несомненно, учитывают все важные этапы эволюции использования биометрии, однако, если исследовать именно правовое регулирование данного института, то можно сделать вывод, что становление правового регулирования данных в ЕС осуществляется именно в XX в., с законодательным закреплением рассматриваемой категории. Вышеприведенные периодизации развития биометрической идентификации представляются достаточно обширными и охватывающими разные общественные процессы. Поэтому первые два этапа неоспоримо могут рассматриваться как исторические предпосылки развития биометрии и появления такой категории, как

---

[32] Барковская Е. Г. Указ. соч. С. 28–31.

[33] Ashbourn J. Biometrics: Advanced Identity Verification: The Complete Guide. London : Springer-Verlag, 2000. P. 1–6.

[34] Smith M., Miller S. Op. cit. P. 167–175.

[35] Ashbourn J. Op. cit. P. 1–6.

биометрические данные, но не как самостоятельные этапы развития института биометрических данных. Безусловно, дактилоскопия легла в основу биометрической идентификации личности, вместе с тем биометрическая идентификация предполагает особую техническую обработку данных с использованием специальных средств автоматизации, кроме того, перечень таких данных уже не ограничивается одними отпечатками пальцев.

Таким образом, биометрические технологии, в частности дактилоскопические, применяются в криминалистике и деятельности правоохранительных органов начиная с XIX в., а в XX в. благодаря техническому прогрессу появилась возможность формализовать алгоритмы распознавания человека по его внешним данным или особенностям поведения и применять для этого автоматизированные системы.

Если можно считать убедительным, что начало формированию и развитию правового регулирования использования биометрических данных в ЕС положено в XX в., то ответ на вопрос о том, что стало поводом для регулирования биометрической идентификации, не является столь очевидным.

Некоторые ученые считают отправной точкой резкого развития биометрической идентификации трагедию, произошедшую в США 11 сентября 2001 г., а именно серию террористических актов в башнях-близнецах Всемирного торгового центра в Манхэттене Нью-Йорка[36]. Впоследствии эти события оказали глубокое влияние на то, как ЕС в дальнейшем сформировал политику в области миграции и свободного передвижения людей на своей территории. Непосредственное внимание было также сосредоточено на предполагаемой слабости внешних границ ЕС и необходимости предупреждения террористических актов в зоне свободной границы ЕС.

Как отмечает А. В. Бутрина, биометрические системы обеспечения безопасности ранее использовались только для защиты военных секретов и самой

[36] Baldaccini A. Counter-Terrorism and the EU Strategy for Border Security: Framing Suspects with Biometric Documents and Databases // European Journal of Migration & Law. 2008. Vol. 10 (1). P. 31–49 ; Вельдер И. А. Система правовой защиты персональных данных в Европейском Союзе : дис. ... канд. юрид. наук. Казань, 2006. С. 131.

важной коммерческой информации. Ну а после потрясшего весь мир террористического акта ситуация резко изменилась. Сначала биометрическими системами доступа оборудовали аэропорты, крупные торговые центры и другие места скопления народа. Повышенный спрос спровоцировал исследования в этой области, что, в свою очередь, привело к появлению новых устройств и технологий[37].

События 11 сентября 2001 г. вызвали серьезную обеспокоенность по поводу защиты проездных документов и потребовали выработки рекомендаций относительно того, что можно сделать для повышения их защищенности от мошенничества или злоупотребления.

С учетом того что персональные данные, в том числе и биометрия, стали объектом пристального контроля именно с развитием системы защиты внешних границ ЕС и получили регулирование в начале 2000-х гг., в период формирования шенгенского права, оправдан подход, согласно которому выделение биометрической информации в законодательстве в сфере защиты персональных данных (в странах ЕС) началась именно с терактов 2001 г.[38]

Впрочем, нельзя не отметить, что до 2001 г. колоссальная работа в данной области была проведена в рамках таких международных организаций, как Международная организация гражданской авиации (далее — ИКАО) и Совет Европы.

Работа в рамках Совета Европы осуществлялась в направлении защиты прав физических лиц при развитии технических систем обработки их данных. В 1968 г. Парламентская ассамблея Совета Европы обратилась к Комитету министров с Рекомендацией 509[39], с просьбой рассмотреть вопрос о том, предоставляют ли Европейская конвенция по правам человека 1950 г. (далее — ЕКПЧ)[40] и внутреннее

---

[37] Бутрина А. В. Биометрическая идентификация личности // Актуальные проблемы авиации и космонавтики. 2012. № 8. С. 389.

[38] Кривогин М. С. Предпосылки формирования специальной правовой защиты биометрических персональных данных // Общество: политика, экономика, право. 2016. № 8. С. 99.

[39] Council of Europe. Recommendation 509 (1968) on Human Rights and Modern Scientific and Technological Developments, adopted by the Assembly on 31st January 1968 (16th Sitting) [Электронный ресурс] // URL: https://pace.coe.int/en/files/14546/html (дата обращения: 10.04.2024).

[40] Конвенция о защите прав человека и основных свобод от 4 ноября 1950 г. // СЗ РФ. 2001. № 2. Ст. 163.

право государств-членов достаточную защиту права на частную жизнь в связи с развитием современной науки и технологии. Исследования, проведенные по указанию Комитета министров Совета Европы в качестве ответа на данную Рекомендацию, показали, что национальное законодательство в странах не обеспечивает достаточной защиты частной жизни людей и других прав и интересов физических лиц в отношении автоматизированных банков данных. Исходя из этих выводов, Комитет министров Совета Европы принял в 1973 и 1974 гг. две резолюции о защите данных. В первой Резолюции (73) 22[41] устанавливаются принципы защиты данных в частном секторе, а во второй Резолюции (74) 29[42] — для общественного сектора. Вскоре, однако, стало очевидно, что ввиду различной трактовки концепции «приватность» в разных странах экстерриториальная защита персональных данных невозможна без общих принципов защиты данных, которые позволили бы гармонизировать национальные законы стран-участниц. Парламентская ассамблея Совета Европы, принимая во внимание эту тенденцию, рекомендовала Комитету министров Совета Европы в Рекомендации 890 (1980)[43] изучить возможность включения в ЕКПЧ положения о защите личных данных.

После четырех лет переговоров страны — члены Совета Европы в 1981 г. приняли Конвенцию 108. В первоначальной редакции Конвенция 108 разъясняла функции и обязанности участников цифровой среды, уделяла особое внимание защите человеческого достоинства и личной автономии при обработке персональных данных. Конвенция 108 запрещала обработку чувствительной информации, к которой были отнесены сведения о расовой принадлежности, здоровье, политических и религиозных взглядах, если национальное право не обеспечивает надлежащих гарантий защиты этой информации. На тот момент

[41] Committee of Ministers of the Council of Europe. Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector, adopted by the Committee of Ministers on 26 September 1973 at the 224th meeting of the Ministers' Deputies [Электронный ресурс] // URL: https://pace.coe.int/en/files/14546/html (дата обращения: 10.04.2024).

[42] Committee of Ministers of the Council of Europe. Resolution (74) 29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector, adopted by the Committee of Ministers on 20 September 1974 at the 236th meeting of the Ministers' Deputies [Электронный ресурс] // URL: https://pace.coe.int/en/files/14546/html (дата обращения: 10.04.2024).

[43] Recommendation 890 (1980) on the protection of personal data, Parliamentary Assembly of the Council of Europe, Documents 4472 and 4484 [Электронный ресурс] // URL: https://pace.coe.int/en/files/14546/html (дата обращения: 10.04.2024).

биометрические данные в перечень чувствительных категорий персональных данных не входили.

Работа ИКАО в направлении формирования правил об использовании биометрических данных, как и в Совете Европы, началась аналогично в 1968 г. В отличие от Совета Европы ИКАО начала разрабатывать технические требования (спецификации) к внедрению машиносчитываемых паспортов, которые формировались на основе биометрических данных.

В 1980 г. в первой редакции уже был опубликован международный Стандарт интеграции биометрической идентификационной информации в проездные документы под названием «Документ Doc 9303 “Паспорт с машиносчитываемыми характеристиками”» (далее — Doc 9303)[44]. Согласно Doc 9303 биометрические характеристики человека рассматривались в качестве данных, хранящихся на машиносчитываемом паспорте: «К документам, удостоверяющим личность, относится электронный паспорт, представляющий собой машиносчитываемый паспорт (МСП), содержащий чип бесконтактной интегральной схемы, на котором хранятся данные со страницы данных МСП, биометрические характеристики владельца паспорта и элемент защиты данных с помощью шифровальной технологии PKI. Термин “электронный паспорт” обозначает только глобально интероперабельные паспорта, обеспечивающие биометрическую идентификацию»[45].

В Doc 9303 впервые были сформулированы виды физиологических систем биометрической идентификации, используемых в удостоверяющих личность документах: система распознавания черт лица; система распознавания отпечатка пальца; система распознавания радужной оболочки глаза.

Система распознавания черт лица была заявлена в качестве обязательной к использованию, а две остальные — в качестве факультативных.

---

[44] ICAO Document 9303. Specifications are published in three separate parts for each type of machine- readable travel document: part 1 for passports, part 2 for visas, and part 3 for official travel documents (cards).

[45] Документ ИКАО Doc 9303. Машиносчитываемые проездные документы. Часть 1: Машиносчитываемые паспорта. Том 1: Паспорта с машиносчитываемыми данными, хранящимися в формате оптического распознавания знаков. Том 2: Спецификация на электронные паспорта со средствами биометрической идентификации. Изд. 6-е. Монреаль : ИКАО, 2006.

В 1984 г. ИКАО была образована Техническая консультативная группа по машиносчитываемым проездным документам (TAG/MRTD), которая обеспечивала доработку и обновление Doc 9303. В результате работы, проведенной в 1998–2001 гг., Техническая консультативная группа по машиносчитываемым проездным документам пришла к выводу о возможности использования для удостоверения личности биометрических данных, сохраняемых в электронном виде, выбрала и рекомендовала лицо в качестве основной биометрической характеристики, а бесконтактную интегральную схему — в качестве технологии хранения данных.

Таким образом, в документах ИКАО биометрические данные стали предметом внимания как характеристики, которые выступили основой для новых проездных документов и нового способа контроля за передвижением лиц.

Следовательно, развитие правового регулирования использования биометрических данных на международном уровне осуществлялось в двух направлениях: 1) использование биометрических данных для формирования новых документов контроля; 2) защита прав личности при автоматизированной обработке персональных данных.

С учетом того, что все без исключения государства — члены ЕС являются участниками как Совета Европы, так и ИКАО, они должны были выполнять принятые организациями правила.

Выполнение Конвенции 108 было обеспечено принятием 24 октября 1995 г. Европейским парламентом и Советом Европейского Союза Директивы 95/46/ЕС, которая предусматривала гарантии защиты физических лиц при обработке персональных данных и закрепила общие принципы свободного обращения и использования таковых. В Директиве 95/46/ЕС не было упоминания о биометрических данных, однако ее положения распространялись на все персональные данные в различных сферах экономической и социальной жизни: Директива 95/46/ЕС определила, что принципы обработки и защиты принимаются в том числе ввиду прогресса в сфере информационных технологий, которые стали существенно упрощать обработку и обмен такими данными.

Как и все государства — члены ИКАО, страны ЕС должны были начать

выдачу машиносчитываемых паспортов согласно ч. 1 Doc 9303 не позднее 2010 г.[46] В сентябре 2003 г. Европейская комиссия подготовила два проекта Правил, предусматривающих введение к 2005 г. двух наборов биометрических данных (отпечатков пальцев и оцифрованных фотографий) в визах и документах на вид на жительство для граждан третьих стран[47]. Как в отношении виз, так и в отношении документов на вид на жительство были приняты также поправки к Правилам, направленные на повышение уровня безопасности этих документов на основе технических требований, установленных ИКАО[48].

В июне 2003 г. Европейский совет в Салониках предложил Европейской комиссии подготовить предложения по «согласованному подходу» в ЕС к биометрическим идентификаторам, что должно было привести к «согласованным решениям в отношении документов граждан третьих стран, паспортов граждан ЕС и информационных систем»[49]. Помимо требования о включении оцифрованной фотографии и отпечатков пальцев в визы и документы на вид на жительство, Комиссией было предусмотрено, что биометрические данные должны храниться на чипах бесконтактной интегральной схемы визовой наклейки, а также наклейки документов на вид на жительство, прилагаемой к паспорту. Так как на тот момент это было технически невозможно из-за проблем с несовместимостью между несколькими чипами в паспорте, предложения были отозваны и вновь представлены в отношении документов на вид на жительство с биометрическими данными в 2006 г.[50] В качестве альтернативного решения было предложено, чтобы использование наклеек для оформления документов на вид на жительство было постепенно прекращено и такие документы выдавались в дальнейшем только в формате карточек. В отношении виз было принято решение, что биометрический

---

[46] Волеводз А. Г. Удостоверяющие личность документы с биометрическими персональными данными. С. 87–117.

[47] COM (2003) 558 final, 24 September 2003. См. также: Coleman N. From Gulf War to Gulf War — Years of Security Concern in Immigration and Asylum Policies at European Level // Terrorism and the Foreigner: A decade of tension around the rule of law in Europe / A. Baldaccini, E. Guild (eds). P. 72–75 ; Peers S. EU Justice and Home Affairs Law. 2nd ed. Oxford University Press, 2006. P. 232–234.

[48] Council Regulation (EC) No. 334/2002 of 18 February 2002 amending Regulation (EC) No. 1683/95 laying down a uniform format for visas // OJ. 2002. L 53/7 ; Council Regulation (EC) No. 1030/2002 of 13 June 2002 laying down a uniform format for residence permits for third-country nationals // OJ. 2002. L 157/1.

[49] Presidency Conclusions, Thessaloniki European Council, 19–20 June 2003, para. 11.

[50] COM (2006) 110 final, 10 March 2006.

чип в них внедряться не будет, а непосредственно биометрические идентификаторы будут храниться только в Визовой информационной системе[51] (Visa Information System, VIS)[52]. Цель информационной системы — воспрепятствовать подделкам виз и тем самым незаконному въезду в шенгенское пространство граждан третьих стран. Составной частью подобных данных являются и биометрические индикаторы — фотография гражданина третьей страны и отпечатки пальцев[53].

Таким образом, технические элементы безопасности, содержащиеся в документах на вид на жительство и визах, были приведены в соответствие с элементами безопасности в паспортах. В 2004 г. был принят Регламент Совета (ЕС) 2252/2004 о стандартных элементах надежности и биометрических данных в паспортах и проездных документах, выданных государствами-членами (далее — Регламент 2252/2004)[54].

Регламент 2252/2004 предусматривал, чтобы паспорта с чипами для распознавания лиц и проездные документы начали выдаваться государствами-членами к августу 2006 г., а цифровые отпечатки пальцев были интегрированы в документы уже к декабрю 2007 г.[55]

Минимальные стандарты безопасности паспортов и других проездных документов, выдаваемых в государствах-членах (приложение к Регламенту), предусматривали, что такие документы должны содержать чипы бесконтактной интегральной схемы, на которых хранятся непосредственно биометрические характеристики владельца паспорта (фотография и отпечатки пальцев).

Регламентом 2252/2004 также было установлено, что включение биометрических данных в цифровой форме в эти документы должно

---

[51] Правовая основа VIS представлена в виде Решения Совета 2004/512/EC (Council Decision 2004/512/EC, 2004) и Регламента Совета и Парламента 767/2008 (Regulation (EC) No. 767/2008, 2008).

[52] Ibid., p. 3 referring to a Strategic Committee on 21–22 June 2005 in Luxembourg where this decision was taken.

[53] Четвериков А. О. Правовой режим пересечения людьми внутренних и внешних границ государств — членов Европейского Союза.

[54] 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 // OJ. 2004. L 385/1.

[55] Прецедентным случаем неисполнения обязательства, предусмотренного Регламентом 2252/2004, стало дело № C-139/13 «European Commission v. Kingdom of Belgium» (Judgment of the Court (Ninth Chamber) of 13 February 2014 — European Commission v. Kingdom of Belgium (Case C-139/13) // OJ. 29.3.2014. C 93. P. 18–19).

осуществляться только для обеспечения их подлинности и использования для удостоверения личности их владельцев в случаях, предусмотренных законодательством государств-членов.

Позднее Регламентом (ЕС) от 28 мая 2009 г. 444/2009 (далее — Регламент 444/2009)[56] были внесены изменения в Регламент 2252/2004, в частности, была предусмотрена необходимость соблюдения в отношении биометрических данных требований об обеспечении безопасности персональных данных, предусмотренных Конвенцией 108. Были уточнены требования к обеспечению безопасности изготовления электронных паспортов компетентными органами государств-членов и установлено, что в чипы бесконтактной интегральной схемы должны вводиться оцифрованные страница с данными электронного паспорта, фотография владельца и отпечатки только двух пальцев.

Таким образом, принятые международными организациями правила по внедрению биометрических данных в документы, удостоверяющие личность, появились задолго до террористических актов 2001 г., и именно они стали толчком к формированию правовой основы выдачи биометрических паспортов и проездных документов в ЕС, главным образом на базе регламентов 2252/2004 и 444/2009.

Большое значение в формировании правового регулирования биометрических данных в ЕС также имеют категория «пространство свободы, безопасности и правосудия», которая появляется в учредительных документах ЕС лишь с подписанием в 1997 г. и вступлением в силу 1 мая 1999 г. Амстердамского договора, и «Шенгенские достижения», в которых находит отражение данная концепция.

Понятие «Шенгенские достижения» охватывает две основные группы «шенгенских источников»:

— первичные акты, заключенные в форме международных договоров, а именно: Соглашение «О постепенной отмене проверок на общих границах»,

[56] Regulation (EC) No. 444/2009 of the European Parliament and of the Council of 28 May 2009 amending Council Regulation (EC) No. 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States // OJ. 6.6.2009. L 142. P. 1–4.

подписанное 14 июня 1985 г., и Конвенция «О применении Шенгенского соглашения от 14 июня 1985 г. о постепенной отмене проверок на общих границах», подписанная 19 июня 1990 г. (Шенгенские соглашения), которые на тот момент еще не являлись источниками права Европейских сообществ и ЕС;

— базирующиеся на Шенгенских соглашениях все вторичные шенгенские акты.

Как отмечает профессор А. О. Четвериков, именно в Шенгенских соглашениях были первоначально сформулированы большинство направлений политики и деятельности, которые после Амстердамского договора образуют содержание компетенции ЕС в рамках пространства свободы, безопасности и правосудия. Так, в полной мере «шенгенскими» по происхождению являются политика в отношении пересечения людьми внутренних и внешних границ государств-членов, визовая, иммиграционная политика, политика по вопросам предоставления убежища (гл. 2 «Политика в отношении пограничного контроля, предоставления убежища и иммиграции» разд. V «Пространство свободы, безопасности и правосудия» части третьей ДФЕС). В значительной степени «шенгенское» происхождение имеют и мероприятия Союза по развитию и регулированию сотрудничества государств-членов в уголовно-правовой сфере на уровне полицейских и судебных органов (разд. III «Полиция и безопасность» Шенгенской конвенции; современная правовая основа: гл. 4 «Судебное сотрудничество по уголовным делам» и гл. 5 «Полицейское сотрудничество» разд. V части третьей ДФЕС)[57].

Все перечисленные направления и мероприятия на том этапе только создавали предпосылки для дальнейшего применения биометрических данных, затем предусматривали их постепенное внедрение посредством создания специализированных информационных систем (таких, как VIS и Шенгенская информационная система (Schengen Information System, SIS)[58]), а сегодня являются

[57] Четвериков А. О. Правовое регулирование либерализации трансграничных отношений : опыт Европейского Союза : дис. ... докт. юрид. наук. М., 2010.

[58] Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the

полноценной областью их применения в рамках реализации совместной компетенции ЕС с государствами-членами в сфере пространства свободы, безопасности и правосудия, закрепленной подпунктом «j» п. 2 ст. 4 ДФЕС.

До террористических актов 2001 г. в ЕС не существовало единой информационной базы, предполагающей возможность обмена информацией между государствами-членами. Именно после терактов на чрезвычайном заседании Совета ЕС 20 сентября 2001 г. было решено, что процедура выдачи виз должна быть ужесточена и что в ближайшее время на рассмотрение необходимо представить предложения по созданию единой базы для обмена информацией о визах, выданных государствами-членами[59].

Реализация плана по созданию единых баз данных началась через три года с созданием VIS, которая предназначалась для сбора и хранения отпечатков пальцев и иных биометрических данных граждан третьих стран, обращающихся за краткосрочными визами.

Решение Совета о создании VIS датируется 8 июня 2004 г.[60] В том же году Комиссия предложила принять закон, определяющий функции VIS и условия обмена данными между государствами-членами по заявлениям на получение краткосрочных виз, в том числе фотографиями и отпечатками пальцев. Соглашение по данному закону было достигнуто на заседании Совета по вопросам юстиции и внутренних дел в 2007 г.[61], а годом ранее решением Европейской комиссии от 22 сентября 2006 г. об установлении технических спецификаций стандартов в отношении биометрических идентификаторов для VIS был разработан перечень биометрических данных, указываемых в визах, и порядок получения виз и вида на жительство для неграждан ЕС[62].

Кроме того, для обмена оперативной информацией, дактилоскопическими и

Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No. 1987/2006 // OJ. 07.12.2018. L 312. P. 14–55.

[59] Extraordinary Council meeting of 20 September 2001, Doc. 12019/01 (Presse 327), para. 26.

[60] Council Decision 2004/512/EC establishing the Visa Information System (VIS) // OJ. 2004. L 213/5.

[61] Doc. 10267/07 (Presse 125) [Электронный ресурс] // URL: https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/visa-information-system_en (дата обращения: 20.03.2024).

[62] Commission Decision of 22 September 2006 2006/648/EC laying down the technical specifications on the standards for biometric features related to the development of the Visa Information System (notified under document number C (2006) 3699) //OJ. 27.9.2006. L 267. P. 41–43.

генетическими данными в отношении лиц, представляющих потенциальную опасность, 27 мая 2005 г. между Бельгией, Германией, Испанией, Францией, Люксембургом, Нидерландами и Австрией была подписана Конвенция о расширении трансграничного сотрудничества для борьбы с терроризмом, трансграничной преступностью и нелегальной миграцией, которая называется по месту подписания «Прюмская конвенция» или «Шенген III»[63]. Конвенция должна была решить проблему полицейского сотрудничества в странах шенгенского пространства. Прюмская конвенция предусмотрела организацию обмена оперативной информацией, дактилоскопическими и генетическими данными относительно лиц, представляющих потенциальную опасность, и создание баз данных такой информации. Несмотря на то что не все государства — участники Конвенции были готовы сразу начать обмен геномной информацией[64], Прюмская конвенция заложила основу для формирования единой ДНК-базы.

Принятые меры нашли отражение и в Кодексе Сообщества о визах (Визовый кодекс)[65], установленном Регламентом (ЕС) от 13 июля 2009 г. 810/2009, который отменил ранее действовавшие в ЕС нормы о единой (шенгенской) визе[66].

Общими правилами подачи ходатайства теперь предусмотрены представление заявителем фотографии в соответствии с установленными международными техническими стандартами и дактилоскопирование его отпечатков пальцев (ст. 10 Визового кодекса).

Статья 13 «Биометрические элементы идентификации» Визового кодекса, регламентирует получение консульствами государств-членов у ходатайствующего лица биометрических идентификаторов, включая фотографию и десять отпечатков

---

[63] Convention between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands and the Republic of Austria on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration [Электронный ресурс] // URL: http://www.statewatch.org/media/documents/news/2005/aug/Prum-Convention.pdf (дата обращения: 01.03.2024).

[64] См.: Никитина И. Э., Нетрусова Т. И., Никитина А. Ю. Значение Прюмского договора в деле обеспечения обмена криминалистической информацией по уголовным делам в государствах — членах Европейского Союза // Научный портал МВД России. 2014. № 4 (28). С. 133.

[65] Regulation (EC) No. 810/2009 of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas (Visa Code) // OJ. 15.9.2009. L 243. P. 1–58.

[66] The Schengen acquis — Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders // OJ. 22.09.2000. L 239. P. 0019–0062.

пальцев, при соблюдении гарантий, предусмотренных ЕКПЧ, Хартией ЕС об основных правах[67] и Конвенцией Организации Объединенных Наций о правах ребенка[68]. Хранилищем таких данных стали такие национальные базы данных, как уже упомянутые VIS и SIS.

Новые требования к содержанию биометрических данных граждан в визовых документах также нашли отражение в положениях Регламента (ЕС) от 23 апреля 2009 г. 390/2009 о внесении изменений в общие консульские инструкции по оформлению виз для дипломатических представительств и консульских учреждений в связи с введением биометрических данных, в том числе положения об организации приема и обработки визовых заявлений[69]. Указанные нормы признают интеграцию биометрических идентификаторов в VIS важным шагом на пути к более надежной связи между владельцем визы и паспортом во избежание использования фальшивых идентификаторов и повторяют требования, изложенные в Визовом кодексе.

Вышеперечисленные меры по приведению законодательства в соответствие с требованиями обеспечения национальной безопасности путем внедрения биометрических систем идентификации, принятые мировым и европейским сообществом, носили больше технический характер. Закрепленные в законодательстве правила касались процедурных вопросов пересечения границы, формирования биометрических характеристик и создания единой базы данных таковых и представляются вынужденной оперативной мерой реагирования на разрастающийся по всему Земному шару терроризм.

Несмотря на фактическое использование биометрических данных, до 2007 г. данное понятие официально не было закреплено ни в рассмотренных международных документах, ни в законодательстве ЕС. Лишь в 2007 г., спустя шесть лет после террористических актов в США, на уровне ЕС рабочей группой по

---

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

[68] Конвенция о правах ребенка (одобрена Генеральной Ассамблеей ООН 20 ноября 1989 г.) (вступила в силу для СССР 15 сентября 1990 г.) // Сборник международных договоров СССР. 1993. Вып. XLVI.

[69] Regulation (EC) No. 390/2009 of the European Parliament and of the Council of 23 April 2009 amending the Common Consular Instructions on visas for diplomatic missions and consular posts in relation to the introduction of biometrics including provisions on the organisation of the reception and processing of visa applications // OJ. 28.5.2009. L 131. P. 1–10.

вопросам защиты физических лиц при обработке персональных данных «Article 29 Working Party» (A29WP)[70] правовое регулирование биометрических данных стало прорабатываться детально, в частности, именно в тот момент впервые было дано правовое определение категории биометрических данных[71]. Это говорит о том, что с момента использования до закрепления биометрических данных в правовых актах Союза понадобилось время для осознания уникальности и потенциала данной категории персональных данных.

В 2009 г. система ЕС претерпевает колоссальное реформирование после вступления в силу Лиссабонского договора[72]. Изменения главным образом коснулись трех международных документов, которые в настоящее время составляют основу права ЕС:

— ДЕС[73], подписанного 7 февраля 1992 г. и вступившего в силу 1 ноября 1993 г. в редакции Маастрихтского договора, действующего в настоящее время в редакции Лиссабонского договора;

— ДФЕС[74], подписанного 25 марта 1957 г. в редакции Римского договора, также действующего в редакции Лиссабонского договора;

— Хартии Европейского Союза об основных правах[75], одобренной 7 декабря 2000 г. в городе Ницце.

Последняя получила юридическую силу только с 2009 г. и стала первичным источником права ЕС благодаря Лиссабонскому договору.

Последовавшие изменения нашли отражение в современной статье 16 ДФЕС, закрепляющей право каждого на защиту персональных данных и устанавливающей соответствующие правила защиты Европейским парламентом и Советом, а также в

---

[70] Article 29 Working Party — рабочая группа по защите физических лиц при обработке персональных данных, учрежденная статьей 29 Директивы Европейского парламента и Совета Европейского Союза 95/46/ЕС от 24 октября 1995 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных. 25 мая 2018 г. была заменена Европейским советом по защите данных (European Data Protection Board (EDPB)) в соответствии с Регламентом 2016/679.

[71] A29WP. Opinion 4/2007 on the concept of personal data (20 June 2007). 01248/07/EN WP 136.

[72] 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: 23.03.2024).

[73] Treaty on European Union // OJ. 07.06.2016. C 202. P. 1–388.

[74] Treaty on the Functioning of the European Union // OJ. 07.06.2016. C 202. P. 1–388.

[75] Charter of Fundamental Rights of the European Union // OJ. 07.06.2016. C 202. P. 389–405.

корреспондирующей ей Декларации 20, в которой обращается внимание на необходимость предусматривать случаи, когда такие правила затрагивают вопросы национальной безопасности.

Декларации являются приложением к Заключительному акту Межправительственной конференции 2007 г. и представляют собой официальные заявления государств-членов в отношении некоторых статей учредительных документов Союза и различных сфер регулирования. Среди них отметим и Декларацию 21, которая предусматривает требование об установлении особых правил о защите персональных данных и их свободном перемещении для сфер судебного и полицейского сотрудничества.

В соответствии со ст. 39 ДЕС, аналогично ст. 16 ДФЕС, Европейский Совет также наделен полномочием по принятию решения, устанавливающего правила о защите физических лиц в отношении обработки персональных данных государствами-членами при осуществлении деятельности и о свободном перемещении таких данных.

В статье 8 Хартии ЕС об основных правах закреплено, что каждому человеку гарантируются право на защиту относящихся к нему персональных данных, право на получение доступа к собранным в отношении него данным и право на устранение в них ошибок. Помимо этого, данная статья предусматривает основания обработки персональных данных. Однако во всех вышеперечисленных документах биометрические данные концептуально не закреплялись. Впрочем, поскольку биометрические данные в это время уже находились под пристальным вниманием законодателя, представляется верным, что отсутствие прямого указания на таковые в учредительных документах в редакции Лиссабонского договора можно считать выражением воли законодателя рассматривать биометрические данные в качестве составной части персональных данных.

Разработка специального правового регулирования в отношении использования биометрических данных стала возможной только с принятием в 2016 г. Регламента о защите данных и вступлением его в силу в 2018 г. В соответствии со ст. 9 Регламента биометрические данные относятся к специальным

категориям персональных данных наряду с генетическими данными и данными о здоровье, поэтому для их обработки предусмотрены особые условия, закрепленные этим же Регламентом.

Кроме этого, в последние годы новым и прорывным направлением в законодательстве ЕС стало правовое регулирование систем искусственного интеллекта, которые составляют техническую основу использования биометрических данных посредством различных биометрических систем. Более конкретные положения относительно использования биометрических систем и биометрических данных содержатся в Регламенте об ИИ. Как и любой другой акт ЕС, содержащий правила использования биометрических данных в какой-либо сфере, Регламент об ИИ опирается на Регламент о защите данных как основной акт о персональных данных ЕС и призывает к его соблюдению при регулировании общественных отношений с использованием систем искусственного интеллекта.

С учетом всего изложенного можно прийти к следующим выводам.

В науке сложилось мнение, что биометрические данные имеют историю, уходящую корнями в древние времена, когда для идентификации личности человека использовались методы фиксирования и учета физических и поведенческих характеристик. Кроме того, принято считать, что биометрические данные обязаны своей природой дактилоскопическим данным и временам, когда впервые было доказано, что отпечатки пальцев человека являются уникальными и неповторяющимися.

Несомненно, дактилоскопические данные, а именно отпечатки пальцев, стали отправной точкой для создания и развития биометрических систем, в то же время биометрические данные сегодня охватывают гораздо более широкий круг физических характеристик и даже поведенческих черт благодаря прорывным технологиям в данной области и в соответствии с действующим законодательством.

Особенно отметим: биометрические данные становятся биометрическими только в результате специальной технической обработки, которая широко применяется лишь в последние десятилетия.

Принимая во внимание реальную сущность биометрических данных, можно сделать вывод, что указанные периоды послужили лишь далекой исторической предпосылкой их создания, а непосредственно само правовое регулирование использования биометрических данных в ЕС параллельно развивается в двух основных направлениях: безопасность и права человека. Соответственно, становление регулирования биометрических данных будет характеризоваться принятием различных правовых актов в указанных областях, находящихся непосредственно во взаимодействии и взаимодополнении, на разных этапах.

Таким образом, предлагается следующая периодизация.

I этап: конец 1990-х — начало 2000-х гг. — этап интеграции первых международных стандартов в области безопасности, прав человека и персональных данных в законодательстве ЕС. На данном этапе в законодательстве ЕС впервые употребляются такие термины, как «биометрия», «биометрические характеристики» или «идентификаторы». «Биометрических данных» как отдельной категории персональных данных еще не существует, вместо этого понятия чаще используются «отпечатки пальцев» или «изображение лица». Этот этап характеризуется в том числе:

— принятием Директивы 95/46/ЕС в рамках имплементации ЕКПЧ и Конвенции 108;

— принятием Регламента 2252/2004 в рамках внедрения Doc 9303;

— развитием визового законодательства (акты о создании VIS и SIS, подписание Прюмской конвенции и т.д.).

Законодательство о персональных данных в этот период впервые отмечает прогресс в сфере информационных технологий, которые стали существенно упрощать обработку и обмен данными, и устанавливает соответствующие принципы обработки и защиты. А акты ЕС в области безопасности Акты ЕС в области безопасности регулируют использование биометрических данных скорее с точки зрения технических аспектов, нежели как категории персональных данных, требующей особой правовой защиты.

II этап: 2007–2016 гг. — этап выделения биометрических данных в системе персональных данных и зарождения специального правового регулирования. Именно в 2007 г., как уже было отмечено, в Заключении Рабочей группы 4/2007 о концепции персональных данных было впервые дано определение биометрических данных.

На этот же этап приходятся изменения в учредительных договорах ЕС, связанные с вступлением в силу Лиссабонского договора, которые служат основой принятия актов как в области персональных данных, так и в области безопасности, а также закрепляют право каждого на защиту персональных данных и устанавливают соответствующие правила защиты в ЕС. Косвенно на данном этапе уже шла речь о необходимости предусматривать особые правила защиты таких данных, например в сферах судебного и полицейского сотрудничества, а также в вопросах национальной безопасности, на что было обращено внимание в упомянутых декларациях к Заключительному акту Межправительственной конференции 2007 г.

В этот период выработаны понятие и перечень биометрических данных, определено их место в качестве категории данных, раскрывающей информацию о физическом лице, сформулированы требования подлинности и надежности, а также необходимость соблюдения в отношении биометрических данных требований об обеспечении безопасности персональных данных. В визовом законодательстве на данном этапе происходят обновления в виде принятия регламентов (ЕС) 810/2009 и 390/2009, создаются информационные системы для обмена данными в сфере пограничного контроля.

III этап: 2016 г. — настоящее время — современный период регулирования (специальное регулирование биометрических данных).

Важнейшую роль на данном этапе сыграло принятие Регламента 216/679, в соответствии с которым биометрические данные относятся к специальной категории персональных данных наряду с генетическими данными и данными о здоровье. Отдельной статьей предусмотрены условия обработки специальных категорий персональных данных. Все государства — члены ЕС приводят

национальное законодательство в соответствие с требованиями Регламента о защите данных, предусматривают правила обработки биометрических данных в различных отраслевых правовых актах.

Данный этап ознаменован также разработкой и принятием Регламента об ИИ, значительная часть которого посвящена вопросам применения биометрических систем и обращению с биометрическими данными.

В сфере пограничного контроля и визового режима, полицейского и судебного сотрудничества продолжают разрабатываться правила взаимодействия информационных систем по безопасному обмену данными.

В настоящее время по-прежнему не существует отдельных правовых актов, посвященных регулированию конкретно биометрических данных. Вместе с тем нормы, регулирующие их использование, пронизывают многие сферы в современном законодательстве ЕС, которые предложено будет рассмотреть далее в диссертационном исследовании.

Таким образом, современному устоявшемуся правовому пониманию биометрических данных как специальной категории данных с особым законодательным регулированием предшествуют вышеперечисленные этапы формирования правовой базы в этой области.

Принятие первых правовых актов, предусматривающих внедрение биометрических характеристик в проездные документы и документы, удостоверяющие личность, имело целью прежде всего установление технических стандартов и инструкций и не предусматривало изначально специального правового регулирования в области защиты такой категории данных. Однако по итогам исследования принятия следующих актов и внесения изменений в действовавшие на тот момент можно установить логику европейского законодателя, которая заключается в постепенном переходе от технических стандартов к стандартам защиты персональных данных, а от регулирования персональных данных — к биометрии как специальной категории[76].

[76] Семенова Я. В. Формирование правового регулирования использования биометрических данных в Европейском Союзе // Евразийский юридический журнал. 2022. № 8. С. 68.

§ 1.2. Биометрические данные в системе защиты персональных данных Европейского Союза

В юридической науке вопрос о перечне характеристик, которые могут составлять биометрическую информацию, остается дискуссионным, а значит, и единого подхода к определению понятия «биометрические данные» с закрытым перечнем таких характеристик в настоящий момент не существует, что, по нашему мнению, представляет собой первопричину возникающих на практике проблем правового регулирования использования биометрических данных.

Такого же мнения придерживается А. В. Колосов, который отмечает, что одной из главных проблем в рассматриваемой области является именно «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 неоднозначно определяют данную область и ее содержание»[77].

Соответственно, необходимо установить перечень характеристик, подпадающих под категорию биометрических данных согласно существующим научным подходам, а также положениям актов ЕС. Важно исследовать роль и место биометрических данных в системе персональных данных, их ключевые признаки, позволяющие отнести данные физического лица именно к категории биометрических данных.

Действительно, проанализировав различные точки зрения, можно прийти к выводу, что природа биометрических данных не так однозначна. Например, И. Ф. Фейсханов и Л. Э. Арсланова отмечают, что биометрические персональные данные — это сведения, полученные человеком с рождения и неизменно находящиеся с ним[78].

---

[77] Колосов А. В. Указ. соч. С. 90.

[78] Фейсханов И. Ф., Арсланова Л. Э. Некоторые аспекты защиты биометрических персональных данных в информационных системах // Российские регионы в фокусе перемен : сб. докладов XIV Междунар. конф. 2020. Екатеринбург, 2020. С. 241.

М. А. Магаммедов также утверждает, что «биометрические данные заложены в человека самой природой — закодированная информация, которую люди научились считывать при помощи сканера, сенсора и других устройств. Это: радужная оболочка глаза, отпечаток пальца, код ДНК, лицо, слепок голоса, строение вен и прочее»[79].

По мнению Г. А. и М. В. Двоеносовых, в основе биометрических данных лежит биологическая информация, приобретающая в зафиксированном виде значение социальной, поскольку она относится к персональным данным[80].

В. Е. Степенко и А. Д. Богдановская к биометрическим данным относят всякую информацию, с помощью которой по внешним признакам возможно отличить одного человека от другого, и придерживаются следующего определения: «биометрические данные — это сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность»[81]. Соответственно, биометрические данные делятся на определяющие биологические особенности человека и определяющие физиологические особенности человека. При этом к биологическим биометрическим данным В. Е. Степенко и А. Д. Богдановская относят биологические сведения о молекулярном строении ДНК и группе крови. Отмечается, что ДНК каждого человека уникальна и неповторима. И именно ДНК закладывает в нас тот или иной вид нашей биометрии, который практически никогда не повторится в другом человеке.

Физиологические биометрические данные разделяют еще на два типа: статические (анатомические) и динамические (поведенческие) биометрические характеристики человека. Статические характеристики — все то, что дано человеку от рождения и не изменяется со временем (например, геометрия лица и рук,

---

[79] Магаммедов М. А. Биометрические данные и банки // Цифровая парадигма развития общества: взгляд из будущего : сборник научных трудов по итогам студенческой научно-практической конференции, Саратов, 26 апреля 2019 года / редколлегия: Н. С. Яшин [и др.]. Саратов : Саратовский социально-экономический институт РЭУ имени Г. В. Плеханова, 2019. С. 151.

[80] Двоеносова Г. А., Двоеносова М. В. Биометрия как наука, метод и способ документирования // Управление персоналом. 2009. № 11. С. 83.

[81] Степенко В. Е., Богдановская А. Д. Биометрические персональные данные // Евразийский Союз Ученых. 2020. № 4-10 (73). С. 16.

рисунок сетчатки глаза, отпечатки пальцев). К динамическим биометрическим характеристикам относятся почерк, голосовая артикуляция, манипуляции на клавиатуре, т.е. все то, что типично и уникально для конкретного человека, но в большей или меньшей степени изменяется с течением его жизни.

М. С. Кривогин, ссылаясь на Э. Мордини[82], отмечает, что биометрические технологии используются для идентификации субъектов по таким физиологическим, биологическим и поведенческим характеристикам, как геометрия лица, отпечатки пальцев, ДНК, манера ходьбы[83].

По существу предложенные отечественными исследователями определения объединяет следующее:

— в них отсутствует исчерпывающий перечень характеристик, которые могут быть названы биометрическими данными;

— в основном проводится разграничение биометрической информации на биологические и физические, физиологические и поведенческие черты человека;

— ДНК человека отнесена к биометрическим данным.

Одной из первых и главных правовых проблем представляется отсутствие ясности по поводу того, что в каждом конкретном случае понимается под биологическими, физическими, физиологическими и поведенческими чертами, ведь каждая дефиниция относит к той или иной группе биометрических данных различные характеристики человека. Отсюда вытекают и сложности с установлением закрытого перечня таких характеристик, а также неопределенность с отнесением к биометрическим данным ДНК.

Разделение биометрических данных некоторые ученые считают нецелесообразным[84]: физиология выступает составной частью биологии, а потому некорректно разграничивать биологическую и физиологическую информацию. Так, по замечанию Н. И. Платоновой, биология является системой наук, изучающих живых существ и их взаимодействие с объектами живой и неживой

---

[82] Mordini E. Second Generation Biometrics: The Ethical, Legal and Social Context. N.Y., 2012. P. 130.

[83] Кривогин М. С. Особенности правового регулирования биометрических персональных данных. С. 81.

[84] Попкова А. Р. Правовой режим использования биометрических персональных данных при удаленной идентификации физических лиц банками // Молодой ученый. 2020. № 1 (291). С. 183.

природы, а одной из наук, входящей в эту систему, выступает физиология. Таким образом, «биологические особенности человека» являются более широким понятием, охватывающим «физиологические особенности человека». Кроме того, названный автор поднимает вопрос отнесения к биометрическим данным сведений о татуировках, пирсинге, шрамах и т.д. и полагает, что они сами по себе не могут представлять собой биологические характеристики человека. Не утихают споры и касательно отнесения фото— и видеоизображений человека к биометрическим данным[85].

К. Жассеран разграничивает понятия «биометрические данные» и «биометрические характеристики»; вместе с тем биометрические характеристики, из которых извлекаются биометрические данные, являются физическими / физиологическими или поведенческими чертами. Подобные признаки (такие как лицо, отпечатки пальцев, голос или походка) демонстрируют некоторые отличительные особенности (так называемые паттерны), которые можно измерить и сопоставить в целях распознавания человека[86]. Одновременно с этим названный автор указывает, что разница между физиологическими и физическими характеристиками не совсем ясна, так как многие эксперты выделяют только два типа характеристик: физические и поведенческие или физиологические и поведенческие.

К. Жассеран также справедливо отмечено, что «биометрические характеристики сами по себе не считаются биометрическими данными. Только персональные данные, полученные “в результате их обработки”, квалифицируются как биометрические данные. Таким образом, не лицо человека, а изображения его лица (фотографии) будут квалифицированы как биометрические данные. Аналогично не кончик пальца, а изображение отпечатка пальца будет классифицировано как биометрические данные». Названный автор приходит к такому логичному выводу, поскольку «биометрические данные», согласно

---

[85] Платонова Н. И. Современный подход к пониманию персональных данных // Право и современные государства. 2017. № 5. С. 14.

[86] Jasserand C. Legal Nature of Biometric Data: From «Generic» Personal Data to Sensitive Data // European Data Protection Law Review. 2016. Vol. 2. Issue 3. P. 297–311.

юридическому определению Регламента о защите данных, это прежде всего персональные данные. Чтобы быть защищенными в соответствии с правилами защиты данных, персональные данные должны быть по крайней мере частью системы регистрации или обрабатываться автоматизированными средствами. Таким образом, сами биометрические характеристики не подлежат обработке, а можно обрабатывать только данные, полученные на основе этих характеристик.

Исследователи Кембриджского университета через определение технологии биометрической аутентификации разделяют биометрические данные на физические и поведенческие характеристики[87].

Профессор Лейденского университета в Нидерландах Е. Киндт проводит аналогичную классификацию биометрических характеристик, выделяя среди них физические / физиологические (отпечатки пальцев и рисунок лица) и поведенческие (походку)[88].

М. Гонсалвес и М. Гамейро ограничиваются при определении биометрических данных физиологическими характеристиками и относят к ним черты лица, отпечатки пальцев, радужную оболочку глаза, а также ДНК[89].

Вместе с тем вопрос о том, может ли быть отнесена генетическая информация и ДНК к биометрическим характеристикам, остается в доктрине спорным. Особую важность данный вопрос приобретает с формированием информационного общества как социального явления[90], следствием чего стало развитие геномных исследований, в том числе с использованием тканей и органов человека, его генетического материала. Это порождает две группы отношений: а) отношения, охватывающие область генной инженерии человека в широком смысле, включая сферы исследования и практического использования (тесно связанные отношения), внедрения геномных и постгеномных технологий в потребительский рынок; б)

---

[87] Biometric Security / J. Hu, D. Chek Ling Ngo, A. Beng Jin Teoh (eds). Newcastle upon Tyne, England : Cambridge Scholars Publishing, 2015. P. 3.

[88] Kindt E. Privacy and Data Protection Issues of Biometric Applications: A Comparative Analysis. Springer, 2013. P. 23–32.

[89] Gonçalves M. E., Gameiro M. I. Does the Centrality of Values in the Lisbon Treaty Promise More Than It Can Actually Offer? EU Biometrics Policy as a Case Study // European Law Journal. 2014. Vol. 20 (1). P. 21–33.

[90] Калиниченко П. А. Глобальное и региональное регулирование исследований и разработок в области человеческого генома и их практического использования. С. 20.

отношения, связанные с геномной информацией, ее сбором (получением), хранением, обработкой, анализом и распространением[91]. Как было указано, к физиологическим составляющим биометрических данных относят ДНК.

ДНК (дезоксирибонуклеиновая кислота) — носитель генетической информации о человеке, записанной в виде последовательности нуклеотидов с помощью генетического кода. ДНК каждого живого существа уникальна и является своеобразным индивидуальным «отпечатком», позволяющим идентифицировать человека[92]. Совокупность ДНК человека представляет его геном.

Только за последние два десятка лет в европейской науке и законодательстве предпринято несколько попыток дать развернутые юридические определения генетическим данным, которые учитывают различные характеристики исследуемого объекта[93]. Так, Совет Европы выделил две стороны генетических данных, которые необходимо учитывать:

— данные любого рода, касающиеся наследственных характеристик индивидуума, которые составляют наследие группы лиц, связанных с ним;

— любые данные, относящиеся к обмену любой генетической информацией (генами), касающейся отдельного лица или генетической линии в отношении любого аспекта здоровья или заболевания, независимо от того, является это идентифицирующим признаком или нет[94].

В соответствии с указанными определениями, с одной стороны, генетические данные человека могут быть отражены в таких биометрических характеристиках, как отпечатки пальцев, и стать предметом идентификации; с другой стороны, эта идентификация уже не будет считаться уникальной, ведь подобные данные являются источником информации не только о своем носителе, но и о родственных и наследственных связях идентифицируемого лица.

---

[91] Калиниченко П. А. Глобальное и региональное регулирование исследований и разработок в области человеческого генома и их практического использования. С. 20.

[92] Рассолов И. М., Чубукова С. Г., Микурова И. В. Биометрия в контексте персональных данных и генетической информации. С. 114.

[93] Рассолов И. М., Чубукова С. Г., Микурова И. В. Правовое регулирование использования генетической информации в Евросоюзе // Аграрное и земельное право. 2019. № 7 (175). С. 120.

[94] Рекомендация от 13 февраля 1997 г. R (97) 5 о защите медицинских данных (Recommendation No. R (97) 5 on the Protection of Medical Data. Feb. 13, 1997).

К аналогичному выводу приходит И. М. Рассолов, заключая, что «неправильно относить генетическую информацию только к персональным данным конкретного лица. Такая информация в значительной мере относится и к неограниченному кругу лиц — родственников, предков и потомков. С молекулой ДНК, помимо ее индивидуальности, связано и другое основополагающее свойство — наследственность и способ передачи наследственной информации[95]. И молекула ДНК является носителем информации не только о конкретном индивидууме, но и о его родителях и родственниках. Из этого следует, что, давая согласие на обработку своей генетической информации, субъект персональных данных также разрешает доступ к генетической информации своих родственников, что с точки зрения законодательства о персональных данных требует получения их согласия[96]. Следовательно, такая информация не является строго индивидуальной, а относится к неограниченному кругу лиц. Поэтому представляется целесообразной позиция авторов о том, что генетическая информация представляет собой самостоятельный вид конфиденциальной информации, сбор, хранение, использование и распространение которой возможны только в соответствии с положениями законодательства и не определяются лишь согласием субъекта»[97].

А. В. Минбалеев в контексте геномной информации утверждает, что она «является специальной разновидностью персональных данных, и на нее не должны распространяться правила о биометрических персональных данных или режима иного вида персональных данных, если это прямо не будет предусмотрено законодательством о генетической информации»[98].

Американские специалисты Б. П. Сперри, М. Эллис и Р. Р. Шарп отмечают существующую среди экспертов в области генетических данных обеспокоенность ввиду того, что ДНК создает проблему конфиденциальности данных, отличную от

---

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

[96] Рассолов И. М., Чубукова С. Г., Микурова И. В. Анализ возможного применения к регулированию отношений по поводу генетической информации институтов персональных данных, личной тайны, врачебной тайны // Lex russica. 2020. Т. 73. № 4. С. 147.

[97] Рассолов И. М., Чубукова С. Г., Микурова И. В. Биометрия в контексте персональных данных и генетической информации. С. 114.

[98] Минбалеев А. В. Защита прав субъектов генетической информации в правовом государстве в условиях развития информационного общества // Правовое государство: теория и практика. 2020. № 2 (60). С. 64.

тех, которые возникают при сборе других биометрических данных, поскольку она может содержать сведения обо всей генетической структуре человека, включая пол, расу, здоровье, историю болезней и предрасположенность к заболеваниям[99]. Другие критики, такие как американский юрист и бывший директор департамента по Ближнему Востоку и Северной Африке одной из ведущих правозащитных международных неправительственных организаций «Хьюман Райтс Вотч» (Human Rights Watch) С. Л. Уитсон, полагают, что обработка дактилоскопических данных, содержащих ДНК, приводит к «массовым нарушением прав человека» из-за круга собираемой частной медицинской информации и возможности ее неправомерного использования[100].

Обозначенные проблемы теории правового регулирования биометрических данных так или иначе оказывают влияние на практическое восприятие указанной категории персональных данных, его правового статуса, содержания и впоследствии на обращение с такими данными.

В связи с этим исследование поставленных вопросов предполагает анализ не только существующих в научной юридической литературе подходов, но и международных правовых актов, актов ЕС и национального законодательства государств-членов.

Как упоминалось выше, только в начале 2000-х гг. на уровне ЕС была вынесена на обсуждение необходимость определения понятия «биометрические данные». Первые документы и доклады по этой теме свидетельствуют о нерешительности в определении их точного статуса и понятия.

В 2003 г. Рабочей группой был издан документ, в котором предусматривалось рассмотрение правил защиты данных при применении биометрических систем[101]. На обсуждение был поставлен вопрос о распространении действия существовавшей на тот момент Директивы 95/46/ЕС, которая устанавливала общие правила защиты и обращения с персональными

[99] Sperry B. P., Allyse M., Sharp R. R. Genetic Fingerprints and National Security // American Journal of Bioethics. 2017. Vol. 17 (5). P. 1–3.

[100] Whitson S. Kuwait: New counterterror law sets mandatory DNA testing. Human Rights Watch, 2015.

[101] A29WP. Working Document on Biometrics (2003) WP 80.

данными, на биометрические данные. Однако выводы о характере биометрических данных на тот момент казались неясными: с одной стороны, было признано, что биометрические данные по своей природе являются именно личными данными, поскольку они всегда относятся к индивиду, которого «обычно можно идентифицировать»[102]; с другой стороны, предполагалось, что биометрические данные не всегда выступают в качестве личных данных человека. Как отметила Е. Киндт, Рабочая группа не предлагала тогда каких-либо четких критериев для разграничения случаев, когда биометрические данные являются личными данными, и случаев, когда они таковыми не являются[103].

Определение понятия «биометрические данные» было сформулировано спустя долгое время в ходе дискуссий в отношении биометрической идентификации и технологий. Рабочая группа исследовала состояние биометрических данных с точки зрения защиты данных еще до появления соответствующей дефиниции. Только в 2007 г. Рабочая группа дала определение этой категории в Заключении 4/2007 о концепции персональных данных[104]. Согласно указанному Заключению, биометрические данные определялись как «биологические свойства, физиологические характеристики, живые черты или повторяющиеся действия, являющиеся уникальными для конкретного индивида и поддающиеся измерению, даже если используемые на практике для их технического измерения закономерности включают определенную степень вероятности». В том же Заключении утверждалось, что биометрические данные имеют двоякую природу: они одновременно являются частью информации о человеке и представляют собой уникальную связь между этим человеком и его биометрическими характеристиками[105]. Интересно отметить, что определение биометрических данных, первоначально содержащееся в предложениях по пакету реформ в области защиты данных, также не было связано с персональными

---

[102] A29WP. Working Document on Biometrics (2003) WP 80.

[103] Kindt E. J. Having Yes, Using No? About the New Legal Regime for Biometric Data // Computer Law & Security Review. 2018. Vol. 34. No. 3. P. 523–538.

[104] A29WP. Opinion 4/2007 on the concept of personal data (20 June 2007). 01248/07/EN WP 136.

[105] Waldmann Agarwal M. A., Fleisher A. Biometric Information — A Brave New World of Regulatory Compliance. Morrison Foerster, 2017.

данными.

При анализе отчетов и заключений Рабочей группы К. Жассеран приходит к выводу, что биометрические данные рассматривались в качестве как технического, так и юридического понятия, потому что сам этот термин отражает техническое преобразование биометрических характеристик в форматы, которые могут быть использованы для биометрического распознавания[106]. Вместе с тем техническая составляющая не требует привязки к конкретному человеку, в то время как в контексте защиты данных такая связь имеет решающее значение для определения того, являются ли технические биометрические данные персональными данными.

Как было отмечено выше, до принятия Регламента 2016/679 и признания утратившей силу Директивы 95/46/ЕС не существовало четкого положения о концепции биометрических данных и специальных норм, регулирующих обработку биометрических данных в документах ЕС по защите данных.

С принятием Регламента о защите данных биометрические данные отнесены в ЕС к специальным категориям персональных данных наряду с данными, раскрывающими расовое или этническое происхождение, политические взгляды, религиозные или философские убеждения, членство в профессиональном союзе, а также генетическими данными и данными, касающимися здоровья, половой жизни или сексуальной ориентации физического лица[107].

Пункт 51 Преамбулы Регламента о защите данных поясняет, что специальные категории персональных данных — это «персональные данные, которые по своей природе особенно чувствительны к фундаментальным правам и свободам и заслуживают особой защиты, поскольку контекст их обработки может создать значительные риски для фундаментальных прав и свобод».

В отношении биометрических данных здесь же отдельно подчеркивается, что обработка фотографий не должна систематически считаться обработкой особых категорий персональных данных, так как они охватываются определением понятия «биометрические данные», только когда обрабатываются посредством

[106] Jasserand C. Op. cit. P. 297–311.
[107] General Data Protection Regulation. Article 9.

специальных технических средств, позволяющих осуществить уникальную идентификацию или аутентификацию физического лица. Такие персональные данные не должны обрабатываться, за исключением случаев, предусмотренных Регламентом о защите данных, когда подобная обработка разрешена.

Обратим внимание на то, что пункт 51 Преамбулы определяет биометрические данные как «особенно чувствительные». Термин «sensitive data» встречается довольно часто и в публикациях зарубежных ученых, когда речь идет о выделении биометрических данных в отдельную категорию. Их «чувствительность» является и предметом исследований российских ученых-юристов.

Е. Киндт отмечает, что пункт 1 ст. 9 Регламента о защите данных не рассматривает всю обработку биометрических данных как «чувствительную». В списке «чувствительных данных» упоминаются только биометрические данные, обрабатываемые с целью однозначной идентификации физического лица.

Вопрос о том, могут ли биометрические данные считаться «чувствительными», впервые был рассмотрен в 2012–2013 гг. в Совете Европы Комитетом по биоэтике в рамках работы по совершенствованию регулирования защиты прав человека в области биомедицины и в связи с применением достижений биологии и медицины[108].

В Заключении, принятом на первом заседании в 2012 г. по повестке пересмотра положений Конвенции 108 Совета Европы[109], Комитет пришел к выводу, что «чувствительными» такие данные будут считаться только при определенном использовании, в связи с тем, что «во многих случаях то, что следует называть биометрическим, — это не исходные данные, а, скорее, конкретные технические операции по обработке, применяемые к этим данным и полученным данным».

---

[108] Комитет был создан как консультативный орган, способствующий обеспечению деятельности Руководящего комитета Совета Европы по биоэтике в рамках изучения правовых проблем, возникающих в связи с развитием биомедицинской сферы. См.: The terms of reference of their mission for 2012–2013, Committee on Bioethics (DH-BIO) Terms of Reference, DH- BIO/INFO (2012) 2. P. 4.

[109] Committee on Bioethics, Opinion on the document of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD) entitled «Modernisation of Convention 108: new proposals», DH-BIO (2012) 12 final, Restricted, 21.6.2012. P. 6.

К. Жассеран аналогично констатирует, что в отличие от других типов персональных данных, перечисленных в качестве специальных категорий («чувствительных»), биометрические данные не рассматриваются как «чувствительные» по своей природе, а становятся таковыми в процессе и результате их использования (обработки).

Впрочем, в течение многих лет вовсе ставилась под вопрос способность биометрических данных раскрывать конфиденциальные сведения, что сеяло сомнения в научном сообществе относительно их «чувствительности».

Вместе с тем результаты нескольких проведенных научных исследований отпечатков пальцев доказали, что биометрические данные могут раскрывать этот тип «чувствительной информации» (например, отпечатки пальцев содержат сведения о происхождении (этнической принадлежности) человека)[110].

Н. Лю полагает, что биометрические данные становятся «чувствительными» только в случае, если их обработка осуществляется с целью получения «чувствительной» информации, такой как сведения о здоровье или генетическая информация и т.д.[111] Соответственно, именно контекст использования биометрических данных обуславливает применение режима конфиденциальных данных. В то же время названный автор утверждает, что «статус биометрических данных должен основываться не на конфиденциальных данных, которые они могут раскрыть, а на их собственных характеристиках». По ее мнению, поскольку биометрические данные могут использоваться в качестве «относительно уникальных и универсальных ключевых данных» для получения остальных видов конфиденциальной информации о человеке, их следует рассматривать как “чувствительные” персональные данные в целом»[112].

П. Куинн в связи с толкованием п. 1 ст. 9 Регламента о защите данных замечает, что для биометрических данных предусматривается определение в

---

[110] Fournier N. A., Ross A. H. Sex, Ancestral, and Pattern Type Variation of Fingerprint Minutiae: Forensic Perspective on Anthropological Dermatoglyphics // American Journal of Physical Anthropology. 2015. Vol. 160 (4). P. 625–632.

[111] Liu N. Y. Bio-Privacy: Privacy Regulations and the Challenge of Biometrics. N.Y., 2012. P. 151.

[112] Liu N. Y. Op. cit. P. 151.

качестве «чувствительных данных», основанное на целях, а не на контексте. Для всех других категорий конфиденциальных данных, упомянутых в указанной статье, Регламент использует термины «данные, раскрывающие…» или «данные, касающиеся…». По мнению названного автора, это определение в значительной степени носит контекстуальный характер и не играет большой роли в намерениях потенциальных контролеров данных. Соответственно, биометрические данные являются исключением с точки зрения защиты конфиденциальных данных в соответствии с Регламентом о защите данных. Цель этого, по-видимому, состоит в том, чтобы исключить автоматическое рассмотрение таких данных, как фотографии и визуальные изображения, в качестве конфиденциальных данных[113].

Интересно отметить, что некоторые российские ученые, напротив, признают, что «чувствительность» биометрических персональных данных обуславливается их собственными свойствами, а не целью использования и обработки[114].

Объясняется это тем, что, во-первых, биометрические характеристики являются уникальными и универсальными: например, ДНК, отпечатки пальцев, геометрия лица (в большинстве случаев) присущи исключительно одному человеку, что позволяет осуществить идентификацию физического лица и существенно ограничивать право на неприкосновенность частной жизни; во-вторых, подобная информация, а также содержащие ее материальные носители становятся доступны для сбора и анализа другим лицам в процессе повседневной активности субъекта, независимо от его воли, что дает возможность производить накопление и обработку таких сведений скрытно, без уведомления субъекта; в-третьих, в отличие от других персональных данных, например фамилии, имени, которые присваиваются другими субъектами или государством и могут быть в дальнейшем изменены, биометрические характеристики являются практически неизменяемыми, что может привести к негативным последствиям в случае неправомерного их использования третьими лицами.

---

[113] Quinn P. The Difficulty of Defining Sensitive Data — The Concept of Sensitive Data in the EU Data Protection Framework // German Law Journal. 2021. No. 22 (8). P. 1583–1612.

[114] Подробнее см.: Кривогин М. С. Особенности правового регулирования биометрических персональных данных. С. 80–89.

Приведенные обстоятельства позволяют М. С. Кривогину рассматривать биометрические персональные данные в качестве «чувствительной» информации, обработка которой должна, по его мнению, регулироваться специальными нормами.

В соответствии с п. 14 ст. 4 Регламента о защите данных биометрические данные — это «персональные данные, полученные в результате специальной технической обработки, которые касаются физических, физиологических или поведенческих черт физического лица, а также позволяют произвести или подтверждают однозначную идентификацию этого физического лица, (например, изображение лица или дактилоскопические данные)». Все акты ЕС, которые содержат нормы, регулирующие обработку биометрических данных или же просто их упоминание, руководствуются, как правило, определением Регламента о защите данных (например, Регламент об ИИ), в связи с чем оно может считаться эталонным, а следовательно, центральным в нашем исследовании.

Исходя из указанного определения, биометрические данные являются прежде всего персональными данными. Это, в свою очередь, означает, что, прежде чем юридически квалифицироваться как «биометрические», такой тип данных должен соответствовать критериям, применимым к общей категории персональных данных.

Помимо этого, соответствующие данные будут считаться биометрическими только при наличии трех условий:

— они получены в результате специальной технической обработки;

— они относятся к физическим, физиологическим или поведенческим чертам физического лица;

— они позволяют произвести или подтверждают однозначную идентификацию этого физического лица.

Кроме того, позднее обратим внимание на закрытый перечень примеров таких данных в определении, а именно изображение лица и дактилоскопические данные.

Рассмотрим каждое из названных условий подробнее.

Во-первых, закрепленное в Регламенте о защите данных определение не предусматривает пояснения, что следует понимать под «специальной технической обработкой», за исключением того, что целью такой обработки должна быть однозначная идентификация лица.

Как отмечает Е. Киндт[115], указание «в результате специальной технической обработки» обязано своим происхождением формулировке, предложенной Комитетом по биоэтике в вышеупомянутом Заключении 2012 г.

В названном Заключении Комитет представил замечания по модернизации Конвенции 108 и концепциям, предложенным Комиссией ЕС относительно определений генетических и биометрических данных, и резюмировал, что «биометрические данные — это не исходные данные, а, скорее, конкретные технические операции по обработке, применяемые к этим данным и полученным данным»[116]. Таким образом, многие данные, классифицируемые как биометрические (фотографии, аудио— или видеозаписи), будут являться «обычными» персональными данными, которые в большинстве случаев будут подвержены обычной обработке (обмену, архивированию, публикации), т.е. данные становятся биометрическими только при биометрической обработке исходных характеристик.

В связи с этим остается открытым вопрос, в какой конкретно момент технической обработки собранные данные становятся биометрическими, и будет ли считаться, например, изображение отпечатков пальцев «обычными» данными.

К. Жассеран в своем исследовании[117] перечисляет технические этапы биометрического распознавания, ссылаясь на стандарт Международной организации по стандартизации ISO/IEC 2382-37[118]. На первом этапе предполагается занесение биометрических характеристик в биометрическую систему. Биометрические характеристики «снимаются» в виде изображения, а полученный формат называется биометрическим образцом. На втором этапе

---

[115] Kindt E. J. Having Yes, Using No? P. 523–538.
[116] Bioethics Committee, DH-BIO (2012) 12 final. P. 6.
[117] Jasserand C. Op. cit. P. 297–311.
[118] ISO/IEC 2382-37 (n 24), Term 37.03.21.

осуществляется извлечение образца, кодирование (преобразование в метки и числа посредством алгоритма). На третьем этапе происходит сравнение биометрического образца с ранее записанным шаблоном. При этом особенно отмечается необходимость разграничения понятий «биометрический образец» и «необработанные биометрические данные». «Необработанными биометрическими данными» в данном случае будут считаться сами биометрические характеристики (радужная оболочка глаза, кончик пальца), в то время как «биометрический образец» — это изображение биометрической характеристики. Термин «необработанные данные» следует использовать только как синоним термина «биометрические характеристики»[119].

Таким образом, биометрические характеристики приобретают статус биометрических данных в момент начала их трансформирования, т.е. на первом этапе технической обработки.

Во-вторых, необходимо пояснить, что понимается под «однозначной идентификацией». К. Жассеран утверждает, что идентификация в данном случае имеет очень узкое и конкретное значение. Она относится к процессу установления личности человека путем сравнения биометрического образца с ранее сохраненными биометрическими шаблонами, существующими в различных базах данных[120]. Это и есть сопоставление «один ко многим»[121]. Идентичность в контексте биометрии не требует установления гражданской или юридической идентичности человека, но определяет, что образец и ранее записанный шаблон происходят от одного и того же лица. Идентичность устанавливается, когда обнаружено совпадение между биометрической характеристикой и биометрическим шаблоном.

Одновременно с этим следует ли понимать такую идентификацию как установление порога идентификации, которому должны соответствовать биометрические данные? На указанном этапе абсолютная уникальность

---

[119] Jasserand C. Op. cit. P. 297–311.
[120] ISO/IEC 2382-37 (n 24), Term 37.08.03.
[121] A29 WP, Opinion 3/2012 (n 8) 5.

биометрических данных не доказана ввиду того, что биометрическое распознавание личности базируется на измерениях и вероятностях сходства. Зачастую результаты сравнения биометрических данных подвергаются ошибкам, что приводит впоследствии к ложной идентификации. По этой причине утверждать, что «однозначная» (уникальная) идентификация является «высшей степенью идентификации»[122] в контексте биометрических данных, будет некорректно.

В-третьих, самым дискуссионным и открытым остается вопрос о содержании физических, физиологических и поведенческих черт физического лица.

В контексте Регламента о защите данных А. В. Колосов раскрывает содержание физических, физиологических и поведенческих характеристик следующим образом[123].

Физические особенности человека квалифицируются как подверженные изменчивости и характеризующие внешний облик антропометрические данные и иные особенности лица (например, возраст, рост, вес, пол и т.д.).

Более уникальными и менее подверженными изменениям 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. К ним относятся походка, мимика, голос, жестикуляция, почерк и т.д.

При анализе определения биометрических персональных данных в Регламенте о защите данных Н. И. Платонова предлагает аналогичный подход к классификации, который, по ее мнению, является наиболее проработанным и отвечающим современному уровню развития науки[124]:

---

[122] См.: Kotschy W. Article 2, Directive 95/46/EC // Concise of European IT law / A. Büllesbach, S. J. H. Gijrath, Y. Poullet, J. E. J. Prins (eds). Kluwer Law International, 2010. P. 35.

[123] Колосов А. В. Указ. соч. С. 93.

[124] Платонова Н. И. Указ. соч. С. 15.

1) сведения о физиологических особенностях человека, обладающие высокой степенью устойчивости (геномная, дактилоскопическая информация, группа крови, строение сетчатки глаза, ушной раковины, геометрия руки и т.д.);

2) физические параметры человека, которые имеют меньшую идентификационную значимость ввиду меньшей уникальности, устойчивости и более высокой степени изменчивости. Речь идет о признаках внешнего облика человека, его антропометрических данных (росте, весе, возрасте, татуировках, пирсинге, шрамах и т.д.);

3) поведенческие особенности человека, проявляющиеся в динамике и характерные для подсознательных движений (походка, жестикуляция, мимика, артикуляция, речь, голос и т.д.).

В предложенных российскими исследователями классификациях бросается в глаза разнообразие информации, которая, как заявлено, является уникальной и свойственной только конкретному физическому лицу. В то же время констатируется, что перечисленные виды характеристик обладают разной степенью уникальности, в чем мы видим существенное противоречие, поскольку, например, рост, вес или возраст не представляют собой индивидуальную и неповторимую информацию.

Рассуждая о физических, физиологических и поведенческих особенностях человека, Е. Киндт приходит к выводу, что сами по себе эти черты являются «простыми» или «обычными» персональными данными и не могут считаться биометрическими по определению п. 14 ст. 4 Регламента о защите данных[125]. Следовательно, сбор и хранение таких «обычных» персональных данных, даже если они относятся к уникальным характеристикам человека, подпадает под общее правовое регулирование персональных данных. Это требует наличия общего правового основания в соответствии со ст. 6 Регламента о защите данных для законности обработки, общих информационных обязательств и т.д. Однако биометрические данные фактически позволяют однозначно идентифицировать

[125] Kindt E. J. Having Yes, Using No? P. 523–538.

лицо или подтвердить личность, и, чтобы стать полезными, они должны технически подвергаться обработке. Поэтому нельзя согласиться с тем, что такие данные не должны считаться биометрическими данными.

Впрочем, говоря о поведенческих чертах, нельзя отрицать, что они чаще всего могут быть подвержены фальсификации. Некоторые ученые полагают, что поведение является эффективным способом распознавания людей, как и их физические характеристики. Американские ученые Р. Челлаппа и П. Турага указывают, что преимущество этого подхода состоит в том, что наблюдение за субъектом может продолжаться длительное время без перерыва или вмешательства в его деятельность[126]. В качестве идентифицирующего признака названные авторы рассматривают походку человека, движение его головы, силуэт, жесты, отмечая, что такого рода сведения содержат больше информации, чем просто трехмерная структура лица человека. Кроме того, психофизические исследования обнаружили доказательства того, что при наличии информации как о структуре, так и о динамике люди склонны больше полагаться на динамику в случаях, например, плохих условий освещения, ограниченного пространства и т.д.[127] Однако представляется верным, что, например, походка или осанка могут умышленно меняться преступником во избежание задержания правоохранительными органами при помощи биометрических технологий распознавания лиц и систем видеонаблюдения. Таким образом, поведенческие черты не могут быть названы уникальными и неповторимыми и использоваться для однозначной идентификации лица.

Говоря о закреплении статуса биометрических данных на уровне национального законодательства государств — членов ЕС, отметим, что до принятия Регламента о защите данных 2016 г. они были вправе самостоятельно принимать решение в части отнесения биометрических данных к специальным («чувствительным») категориям персональных данных и установления особого

---

[126] Chellappa R., Turaga P. Advances in Video-Based Biometrics // Advances in Computers. 2011. Vol. 83. P. 183–203.

[127] Белая О. В., Кицай Ю. А. Биометрические данные как средство идентификации и аутентификации человека: российский и международный опыт // Право и практика. 2020. № 1. С. 87.

правового регулирования их обработки. Например, Франция считалась одним из первых и наиболее продвинутых государств-членов в части принятия мер по минимизации рисков в области защиты персональных данных, возникающих в связи с развитием биометрических систем[128]. Еще в 2012 г. при рассмотрении проекта Закона о защите идентичности[129] Конституционный Совет Франции определил, что сбор, обработка, хранение, использование и передача биометрических данных должны в любом случае быть обоснованы необходимостью защиты публичного интереса, и их осуществление должно быть адекватным и пропорциональным такой цели[130].

С вступлением в силу в 2018 г. Регламента о защите данных для государств — членов ЕС теперь установлено единое определение категории «биометрические данные» и предусмотрено их особое место в системе персональных данных в качестве «чувствительных» данных. Одновременно с этим в соответствии со ст. 9(4) Регламента о защите данных государства-члены могут сохранять или вводить дополнительные условия, в том числе ограничения в отношении обработки биометрических данных, генетических данных или данных, касающихся здоровья, что стало отражаться в их национальном законодательстве.

В Испании биометрические данные ранее не были отнесены к «чувствительной» категории персональных данных, поэтому внедрение здесь Регламента о защите данных предполагало изменение концепции в области защиты биометрических данных, в связи с чем Управление по защите информации Испании (Spanish Data Protection Authority, DPA) сразу выпустило несколько отчетов и руководств, касающихся биометрической аутентификации и идентификации в различных секторах (например, в сфере борьбы с отмыванием денег)[131].

Несмотря на унификацию определения и содержания понятия

---

[128] Gayrel C. The principle of proportionality applied to biometrics in France: Review of ten years of CNIL's deliberations // Computer Law & Security Review. 2016. No. 32(3). P. 450–461.

[129] Loi n° 2012-410 du 27 mars 2012 relative à la protection de l'identité // JORF. N° 0075 du 28 mars 2012. P. 5604, texte n° 2.

[130] Conseil Constitutionnel, Décision nº 2012-652 DC of 22 March 2012, nº 8. ECLI:FR:CC:2012:2012.652.DC.

[131] López-Lapuente L. Spain // The Privacy, Data Protection and Cybersecurity Law Review. London : Law Business Research Ltd., 2022. P. 372–386.

«биометрические данные» на уровне актов ЕС и национального законодательства государств-членов, в настоящее время, на наш взгляд, проблема практического применения норм в рассматриваемой области остается актуальной.

Прежде всего это связано, как отмечалось, с нечеткими формулировками, используемыми в Регламенте о защите данных при определении биометрических данных. Отсутствует правовое разъяснение, что понимается под физическими, физиологическими и поведенческими чертами. Приведенные в качестве примера изображение лица и дактилоскопические данные не образуют исчерпывающий перечень характеристик, которые могут быть преобразованы в биометрические данные.

Дело в том, что в различных областях науки существуют различные толкования интересующих нас характеристик.

Ввиду того, что человек — существо биосоциальное, при определении биометрических данных было бы логично руководствоваться понятиями, официально признанными и используемыми именно в области биологических наук. Кроме этого, целесообразно пересмотреть возможность отнесения к биометрическим данным предложенных в ныне действующих нормах европейского права признаков физического лица, которые по своей природе не являются биологически уникальными и, помимо прочего, менее остальных признаков устойчивы к фальсификации[132]. Речь идет преимущественно о поведенческих признаках, которые могут меняться субъектом в связи с различными обстоятельствами. Поэтому представляется верным, что поведенческие черты не могут быть названы уникальными и неповторимыми и использоваться для однозначной идентификации лица.

Отсутствие в правовых источниках четкого единого подхода к определению исчерпывающего перечня характеристик, подпадающих под категорию биометрических данных, может привести впоследствии к несоблюдению условий их обработки и нарушению права на неприкосновенность частной жизни.

---

[132] Смирнова Я. В. Особенности содержания понятия «биометрические данные» в праве Европейского Союза // Вестник Университета имени О.Е. Кутафина (МГЮА). 2021. № 7. С. 166.

Не решен в Регламенте о защите данных и вопрос о том, относится ли ДНК к физиологическим или генетическим данным. Согласно п. 13 ст. 4 Регламента «генетические данные» выделены в отдельную категорию и представляют собой разновидность персональных данных, относящихся к наследственным или приобретенным генетическим характеристикам физического лица, которые дают уникальную информацию о физиологии или здоровье этого физического лица, а также являются в том числе результатом анализа его биологического образца[133]. На основании п. 34 Преамбулы Регламента генетические данные следует рассматривать как персональные данные в отношении унаследованных или приобретенных генетических характеристик физического лица, которые являются результатом анализа его биологического образца, в частности исследования хромосомной, дезоксирибонуклеиновой кислоты (ДНК) или рибонуклеиновой кислоты (РНК), либо анализа иного элемента, позволяющего получить соответствующую информацию.

Согласно п. 1 ст. 9 Регламента о защите данных обработка генетических данных наряду с биометрическими запрещена. Уточнений о том, является ли генетическая информация наряду с иными физиологическими характеристиками человека составной частью биометрических данных, нет.

Ясность в этот вопрос вносит национальное законодательство государств — членов ЕС. Так, ст. 706-54 Уголовно-процессуального кодекса Франции предусматривает, что генетические отпечатки пальцев, сохраненные в Национальном автоматизированном файле генетических отпечатков пальцев (далее — FNAEG)[134], производятся только из «некодирующих» сегментов ДНК, которые предусмотрены только для идентификации человека, а единственная цель, которую преследует эта обработка, — получить «генетическую подпись» человека, а не информацию о его физиологических, морфологических, наследственных

[133] General Data Protection Regulation. P. 13.

[134] Цит. по: Рассолов И. М., Чубукова С. Г., Микурова И. В. Биометрия в контексте персональных данных и генетической информации. С. 115.

характеристиках[135]. Целью же анализа «кодирующих» последовательностей является получение информации о здоровье соответствующего лица[136]. Следовательно, если ДНК используется для анализа физиологической информации о человеке, то такая информация относится к генетической. Если ДНК необходима только для идентификации, то подобные данные относятся к биометрии. Однако в Регламенте о защите данных соответствующие пояснения о том, какие именно сегменты ДНК собираются как биометрические данные, отсутствуют, что также представляется упущением в законодательстве ЕС.

Исследования зарубежных ученых-юристов и формулировка п. 14 ст. 4 Регламента о защите данных обращают внимание на то, что сами по себе характеристики человека не являются биометрическими данными. Они приобретают такой статус только посредством прохождения этапов специальной технической обработки; вместе с тем эти данные используются для подтверждения «однозначной» (уникальной) идентификации физического лица. Указанный критерий является ключевым в юридическом понимании биометрических данных, так как он содержит ссылку на цели их использования. Это означает, что характеристикам человека, чтобы стать биометрическими данными, недостаточно пройти специальную техническую обработку — они должны подлежать такой обработке только в целях проведения биометрической идентификации или подтверждения личности. На это указывают в определении биометрических данных уточнения «позволяют провести» и «подтверждают», где «позволяют провести» относится к установлению личности человека (непосредственно биометрической идентификации), а «подтверждают» — к проверке личности.

Что касается режима «чувствительных» биометрических данных, представляется верным, что он обусловлен тем, что биометрические данные человека, помимо собственных уникальных характеристик, которые, по нашему мнению, заключаются в основанных на точных измерениях индивидуальных

---

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

[136] Рассолов И. М., Чубукова С. Г., Микурова И. В. Биометрия в контексте персональных данных и генетической информации. С. 115.

показателях, несут в себе конфиденциальную информацию, относящуюся к иным специальным категориям персональных данных, например информацию о здоровье, генетическую информацию или информацию о происхождении лица. Кроме этого, полагаем, что утверждение относительно того, что биометрические данные становятся «чувствительными» только в случае, если их обработка производится непосредственно с намерением получения конфиденциальной «чувствительной» информации, будет являться ошибочным, поскольку обнаружение таких сведений может стать следствием обработки, проведенной в целях проведения элементарной идентификации физического лица и в иных целях, предусмотренных условиями обработки специальных категорий данных.

Таким образом, анализ работ отечественных и зарубежных ученых, а также источников права ЕС и законодательства государств-членов позволяет констатировать, что «биометрические данные» — это прежде всего персональные данные, которые отвечают трем критериям:

— они получены в результате специальной технической обработки;

— они относятся к физическим, физиологическим или поведенческим чертам физического лица;

— они позволяют произвести или подтверждают однозначную идентификацию этого физического лица.

Вместе с тем, на наш взгляд, перечисленные критерии не являются достаточными. Определение, закрепленное в Регламенте о защите данных, только вызывает неясность относительно содержания биометрических данных и дает повод для дискуссий на сей счет в правовой науке о персональных данных.

В связи с этим считаем целесообразным предложить основные идеи и требования, которые рекомендуется учесть при утверждении официального правового определения биометрических данных в ближайшей перспективе в законодательстве ЕС о персональных данных:

1) биометрические данные — это персональные данные, в основе которых лежат уникальные и неотчуждаемые биологические характеристики индивида;

2) такие характеристики должны представлять собой исключительно эталонный образец биоматериала физического лица или изображения биологически уникального свойства человека, полученного посредством специальной технической обработки;

3) определение биометрических данных должно исключать отнесение к ним поведенческих и физиологических характеристик по двум причинам:

— во-первых, поведенческие характеристики не являются постоянными и уникальными, а следовательно, не позволяют провести высокоточную и однозначную идентификацию личности физического лица;

— во-вторых, не существует однозначного понимания того, какие характеристики человека являются физиологическими, что делает определение биометрических данных размытым;

4) биометрические данные считаются таковыми только при условии, если они в процессе их сбора прошли специальную техническую обработку, позволяющую их считать, записать и сохранить в том виде, в котором они представлены физическим лицом. Указанное требование обусловлено нашим знанием о том, что биометрическими данными можно было бы назвать и обыкновенные отпечатки пальцев, предоставленные на бланке дактилоскопических карт, просто на основании наличия корней «био» и «метр» в таком юридическом термине в сфере персональных данных, как «биометрические данные». Однако наше правовое исследование идет в ногу со временем и принимает во внимание, что в XXI в. — веке высоких технологий — подобные данные хранятся не в архивных папках на бумажных носителях, а в международных и национальных базах данных, которые оптимизируют процесс обмена данными в целях обеспечения безопасности;

5) определение биометрических данных должно содержать строго закрытый перечень таких данных, который может поступательно обновляться в связи с новыми техническими достижениями биометрических систем.

ГЛАВА 2. ИСТОЧНИКИ РЕГУЛИРОВАНИЯ ИСПОЛЬЗОВАНИЯ БИОМЕТРИЧЕСКИХ ДАННЫХ В ПРАВЕ ЕВРОПЕЙСКОГО СОЮЗА

§ 2.1. Источники права Европейского Союза как основа регулирования использования биометрических данных

При исследовании любых правоотношений и правовых явлений в пределах ЕС прежде всего необходимо изучить источники права ЕС. Такой подход обеспечивает полную и всестороннюю оценку современного состояния правового регулирования исследуемых отношений.

Система источников права ЕС имеет специфику и включает в себя три категории: источники первичного права; источники вторичного права; источники прецедентного права.

К первым относятся учредительные договоры с многочисленными приложениями и декларациями, а также соглашения и акты, изменяющие и/или дополняющие учредительные документы, составляющие международно-правовую базу ЕС[137], а именно:

— уже упомянутые ДЕС, ДФЕС и Хартия ЕС об основных правах. Договоры имеют одинаковую юридическую силу в соответствии со ст. 1 ДЕС и ст. 1 ДФЕС. Хартия приравнена по юридической силе к указанным договорам на основании ст. 6 ДЕС;

— Амстердамский договор 1997 г., Ниццкий договор 2001 г., Лиссабонский договор 2007 г.;

— договоры о присоединении новых государств-членов, и т.д.

К источникам вторичного права относятся акты, издаваемые институтами Союза, а также все другие акты, принимаемые на основе учредительных договоров[138]; их формы и содержание достаточно разнообразны. Особое место в системе источников вторичного права занимают нормативные договоры, а именно

---

[137] Юмашев Ю. М. Региональная интеграция и международные отношения // Московский журнал международного права. 2006. № 1. С. 75.

[138] Юмашев Ю. М. Указ. соч.

международные соглашения ЕС с третьими странами, а также правовые акты, регулирующие исследуемые отношения. Далее указанные источники будут рассмотрены более подробно в плоскости регулирования биометрических данных.

Наконец, прецедент является отдельной категорий источников права ЕС наряду с источниками первичного и вторичного права. Однако прецедентное право всегда дополняет и развивает положения учредительных договоров и не может отменять их, вместе с тем нормы вторичного права могут как дополняться прецедентами, так и отменяться по решениям судов ЕС.

Предлагаем проанализировать роль каждой категории источников права ЕС в организации правового регулирования использования биометрических данных.

А. Источники первичного права

ДЕС закрепляет юридический факт учреждения ЕС, содержит основные принципы ЕС, положения об институтах Союза, о внешнеполитической деятельности Союза и специальные положения об общей внешней политике и политике безопасности[139]. Применительно к использованию биометрических данных положения ДЕС закрепляют основные принципы[140], которые в том числе влияют на определение общего режима обращения персональных данных в ЕС.

ДФЕС определяются сфера ведения и компетенция Союза, характеризуются общие направления политики ЕС, систематизируются положения, определяющие пространство свободы, безопасности и законности. В большем или меньшем объеме регулируются все сферы, относящиеся не только к исключительной компетенции, но и к сфере совместного ведения Союза и государств-членов[141]. В Договоре содержатся также положения о равенстве и недискриминации, а также защите персональных данных.

---

[139] Кашкин С. Ю., Четвериков А. О. Европейский союз: Основополагающие акты в редакции Лиссабонского договора с комментариями // СПС «КонсультантПлюс», 2007.

[140] Энтин Л. М. Право Европейского Союза. Новый этап эволюции: 2009–2017 годы. М. : Аксиом, 2009. С. 74.

[141] Энтин Л. М. Лиссабонский договор и реформа Европейского Союза // Журнал российского права. 2010. № 3 (159). С. 104.

Как мы продемонстрируем ниже, к сожалению, на практике почти каждый из принципов так или иначе подвергается риску нарушения при обработке биометрических данных человека.

Принцип уважения прав человека упоминается в ст. 2 и закреплен в ст. 6 ДЕС, а ранее был сформулирован в практике Суда с 1970 г.[142] Равенство и недискриминация также провозглашены статьей 2 ДЕС.

Отсюда в соответствии со ст. 8 ДФЕС Союз стремится устранять неравенство, а также бороться с любой дискриминацией по признакам пола, расы или этнического происхождения, религии или убеждений, инвалидности, возраста или сексуальной ориентации согласно ст. 10 того же документа. Предписания ст. 10 ДФЕС обосновываются непосредственной связью с персональными данными, так как сведения о поле, расе, религиозных убеждениях и т.д. являются специальной категорией, которая также подпадает под регулирование и отображена в виде запрета обработки таких сведений в п. 1 ст. 9 Регламента о защите данных.

Достаточно важной для понимания того, как осуществляется регулирование сферы персональных данных ЕС, является статья 16 ДФЕС, которая наделяет Европейский парламент и Совет полномочиями, направленными на установление правил по вопросу защиты физических лиц в отношении обработки персональных данных, и распространяет свое действие на органы, входящие в сферу применения права Союза. Кроме этого, в ст. 39 ДЕС закреплены аналогичные полномочия Совета по указанному вопросу. Данные статьи составляют правовую основу для любого законодательства ЕС по вопросу защиты персональных данных.

Деятельность Союза в рамках обеспечения пространства свободы, безопасности и правосудия при уважении основных прав, а также развития общей политики по вопросам предоставления убежища, иммиграции, контроля внешних границ и обеспечения направленных на предотвращение преступности мер

[142] Впервые в решении Суда ЕС от 17 декабря 1970 г. по делу «International Handelsgesellschaft c. Einfuhr- und Vorratsstelle für Getreide und Futtermittel» (C-11/70, Rec., p. 1125, pt. 2) было подтверждено: «Уважение основных прав является неотъемлемой частью общих принципов права, соблюдение которых обеспечивает Суд». Ранее вопрос об основных правах человека был также затронут Судом ЕС в решении от 12 ноября 1969 г. по делу № 29/69 «Erich Stauder c. City of Ulm — Sozialamt», когда было указано, что Суд ЕС будет защищать «основные права человека, как они вытекают из общих принципов Сообщества».

регламентирована также пунктами 1–3 ст. 67 ДФЕС. Статьей 73 ДФЕС допускается организация государствами-членами на взаимной основе и под свою ответственность форм сотрудничества и координации, которые они считают уместными, между компетентными службами своих ведомств, ответственных за обеспечение национальной безопасности. Как было рассмотрено в предыдущей главе, именно при реализации данных форм сотрудничества поднимались вопросы использования идентифицирующих сведений как граждан ЕС, так и иностранных граждан и беженцев, пересекающих территорию ЕС.

Глава 5 ДФЕС содержит положения, касающиеся организации полицейского сотрудничества в сферах предотвращения или выявления уголовных правонарушений и проводимых по ним расследований. Соответственно пункт 2 ст. 87 и пункт 2 ст. 88 ДФЕС предусматривают меры по сбору, хранению, обработке, анализу информации и обмену ею в рамках мероприятий по предотвращению и противодействию тяжкой преступности, терроризма и тех форм преступности, которые посягают на общие интересы, выступающие объектом политики Союза. Данные положения говорят об организации сотрудничества органов, которые в силу своих полномочий по обеспечению общей безопасности имеют право на доступ к базам данных, содержащих персональные сведения.

Хартия ЕС об основных правах является актом, содержащим основные права, которые государства-члены должны строго соблюдать при имплементации законодательства. Помимо защиты гражданских и политических прав, она охватывает нормы, направленные на защиту персональных данных, в частности, в ст. 8 каждому человеку гарантируются право на защиту относящихся к нему персональных данных, право на получение доступа к собранным в отношении него данным и право на устранение в них ошибок.

Анализ данной нормы позволяет прийти к выводу, что персональные данные должны обрабатываться исключительно в целях, установленных законодательством. Обработка таких данных допускается исключительно с согласия лица или при наличии других правомерных оснований. Однако в законе могут устанавливаться и другие основания для проведения обработки

персональных данных. Указанная статья наделяет человека правом на получение доступа к своим персональным данным и в случае обнаружения какого-либо расхождения правом на исправление ошибок.

Кроме того, дополнительно можно отметить, что право на защиту персональных данных тесно взаимосвязана с правами человека относительно уважения частной и семейной жизни, его жилища и корреспонденции, урегулированными статьей 7 Хартии. В связи с этим, исходя из п. 1 ст. 52 Хартии, а также п. 2 ст. 8 ЕКПЧ, допускается ограничение прав и свобод человека, если такая процедура предусмотрена законом, но она должна соответствовать сути таких прав, при быть необходимой и действительно соответствовать целями такого ограничения.

Статьей 21 Хартии запрещается всякая дискриминация, в частности по признакам пола, расы, цвета кожи, этнического или социального происхождения, генетических черт, языка, религии или убеждений, политических или любых других взглядов, принадлежности к национальному меньшинству, имущественного положения, рождения, нетрудоспособности, возраста или сексуальной ориентации. Риск создания дискриминационной ситуации при обработке биометрических данных всегда высок, так как биометрические данные способны раскрыть информацию о человеке, которая может повлечь неблагоприятные последствия при принятии решения, например, относительно выдачи визы лицу.

Источники первичного права ЕС содержат достаточно широкий спектр основополагающих принципов и правил, которые регламентируют деятельность ЕС в сфере защиты персональных данных, закрепляют основные права человека, в том числе затрагивающие конфиденциальность сведений о нем, а также определяют организационные основы сотрудничества в сферах, которые предполагают использование биометрических данных.

B. Источники вторичного права

Более конкретные нормы об использовании персональных данных в ЕС содержат нормативно-правовые акты, которые существуют в форме регламентов, директив и решений. Такие нормы обладают обязательной юридической силой.

Из статьи 288 ДФЕС следует, что *регламент* в силу его свойств (общее действие, обязательность, прямое применение) возглавляет иерархию источников вторичного права ЕС. Нормы регламента распространяются как на государства — члены ЕС и их органы, так и на физических и юридических лиц.

В рамках нашего исследования будет предложено рассмотреть нормы регламентов, действующих в сферах защиты персональных данных, искусственного интеллекта, пограничного контроля, визового режима и правоохранительной деятельности. Объемный блок будет составлять комплекс регламентов о создании и взаимодействии информационных систем, предусматривающих использование биометрических данных.

Регламент о защите данных, центральный в иерархии правовых актов, устанавливает общие правила обработки персональных данных (в том числе особые правила обработки биометрических данных), задает ориентир всем остальным отраслевым актам ЕС, а также государствам — членам ЕС при разработке норм в рамках национального законотворчества, регулирующих использование биометрических данных.

Вторым по роли в правовом регулировании биометрических данных мы бы назвали принятый в 2024 г. Регламент об ИИ. Системы искусственного интеллекта являются основой функционирования биометрических систем, а следовательно, без них бы не было технической возможности проводить многие операции с биометрическими данными, которые зачастую являются критически важными и необходимыми для поддержания безопасности в ЕС и по всему миру. Именно Регламент об ИИ содержит самые объемные и более конкретизированные нормы, регулирующие обращение с биометрическими данными.

Помимо вышеупомянутых, в ЕС за последние два десятилетия принято множество других регламентов, содержащих в большей или меньшей степени

правила использования биометрических данных в зависимости от того, какую роль в той или иной сфере они играют. Как правило, это регламенты о создании информационных систем, правилах их взаимодействия и обмена данными и т.д.

Отметим, что в 2024 г. ЕС проделана масштабная работа по принятию и актуализации актов, предусматривающих положения о биометрических данных. К таковым относится и принятый 14 мая 2024 г. Регламент (ЕС) 2024/1358[143] о создании Евродак с целью сравнения биометрических данных и выявления незаконно пребывающих граждан третьих стран и лиц без гражданства, а также о запросах на сравнение биометрических данных. Регламент принят в целях реализации регламентов от той же даты: Регламента 2024/1350[144] об установлении правил переселения и гуманитарного допуска в Союз; Регламента 2024/1351[145] об управлении предоставлением убежища и миграцией, вносящего изменения в регламенты (ЕС) 2021/1147 и 2021/1060 и отменяющего Регламент (ЕС) 604/2013.

Директива, как вытекает из ст. 288 ДФЕС, является нормативным актом, обязательным для исполнения государствами-членами в установленный срок, и не имеет прямого применения. Данный акт служит средством внедрения закрепленных в нем положений в национальное законодательство государств-членов, при этом «формы и методы имплементации остаются на усмотрение государств-членов».

Как происходит гармонизация законодательства государств — членов ЕС, наглядно отражено в параграфе 2.2, посвященном законодательству государств — членов ЕС об использовании биометрических данных. Например, Директиве (ЕС)

---

[143] Regulation (EU) 2024/1358 of the European Parliament and of the Council of 14 May 2024 on the establishment of ‘Eurodac’ for the comparison of biometric data in order to effectively apply Regulations (EU) 2024/1351 and (EU) 2024/1350 of the European Parliament and of the Council and Council Directive 2001/55/EC and to identify illegally staying third-country nationals and stateless persons and on requests for the comparison with Eurodac data by Member States’ law enforcement authorities and Europol for law enforcement purposes, amending Regulations (EU) 2018/1240 and (EU) 2019/818 of the European Parliament and of the Council and repealing Regulation (EU) No 603/2013 of the European Parliament and of the Council // OJ. 22.5.2024. L 2024/1358.

[144] Regulation (EU) 2024/1350 of the European Parliament and of the Council of 14 May 2024 establishing a Union Resettlement and Humanitarian Admission Framework, and amending Regulation (EU) 2021/1147 // OJ. 22.5.2024. L 2024/1350.

[145] Regulation (EU) 2024/1351 of the European Parliament and of the Council of 14 May 2024 on asylum and migration management, amending Regulations (EU) 2021/1147 and (EU) 2021/1060 and repealing Regulation (EU) No. 604/2013 // OJ. 22.5.2024. L 2024/1351.

от 27 апреля 2016 г. 2016/680/ЕС (далее — Директива 2016/680/ЕС)[146], устанавливающей принципы защиты физических лиц в отношении обработки персональных данных компетентными органами в целях предотвращения, расследования уголовных преступлений, а также проведения розыскных мероприятий, направленных на установление местонахождения лиц, в отношении которых ведется уголовное преследование, корреспондирует действующий в Германии Федеральный закон от 30 июня 2017 г. о защите данных (Bundesdatenschutzgesetz, BDSG)[147], в котором отдельно урегулированы вопросы реализации Регламента о защите данных и данной Директивы.

Такой вид источников вторичного права, как *решение,* принимается Европейским парламентом и (или) Советом Союза в отношении конкретного государства-члена или лица (группы лиц) и, в отличие от директивы, обладает прямым действием в отношении лиц, указанных в нем. В качестве примера приведем одно из последних — Решение Комиссии (ЕС) от 31 июля 2024 г. 2024/2100 об участии Ирландии в Регламенте 2024/1358.

Как было упомянуто, к актам вторичного права ЕС также относятся *нормативные договоры*. Данная группа источников включает международные договоры ЕС, конвенции между государствами-членами, принятые под эгидой Европейских Сообществ и Союза, а также соглашения между институтами ЕС (межинституциональные соглашения)[148].

В соответствии со ст. 47 ДЕС ЕС является международной организаций и обладает международной правосубъектностью, а следовательно, способен вести переговоры и заключать *международные соглашения* от своего имени[149].

---

[146] Directive (EU) 2016/680 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 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 // OJ. 4.5.2016. L 119. P. 89–131.

[147] Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097), das zuletzt durch Artikel 10 des Gesetzes vom 23. Juni 2021 (BGBl. I. S. 1858; 2022 I 1045) geändert worden ist [Электронный ресурс] // URL: https://www.gesetze-im-internet.de/bdsg_2018/BJNR209710017.html (дата обращения: 04.03.2024).

[148] Там же. С. 105.

[149] Черниченко С. В. Теория международного права : в 2 т. М. : НИМП, 1999. Т. 1 : Современные теоретические проблемы. С. 113.

Пункт 1 ст. 218 ДФЕС выделяет такие разновидности международных соглашений, как соглашения с третьими странами и соглашения с международными организациями. Согласно ст. 216–220 ДФЕС ЕС имеет полномочия заключать соглашения с третьими странами, когда это необходимо для реализации политики Союза, и эти соглашения имеют обязательную силу для институтов организации и государств-членов.

Исходя из анализа действующих соглашений ЕС с третьими странами, констатируем, что соглашений, предметом которых являлись бы вопросы регулирования именно биометрических данных, на сегодняшний день не заключено. Вместе с тем «биометрические данные» фигурируют в текстах соглашений, предметом которых являются, например, вопросы визового режима (Соглашение между ЕС и Республикой Беларусь об упрощении выдачи виз от 2019 г.[150], Соглашение между ЕС и Республикой Перу об отмене краткосрочных виз от 2016 г.[151]).

В рамках взаимодействия ЕС и Российской Федерации на основе Соглашения о партнерстве и сотрудничестве 1994 г.[152] хотелось бы отметить выявленную П. А. Калиниченко систему специальных секторных соглашений, которые существуют как на уровне отношений России с государствами-членами, так и на уровне отношений между Россией и ЕС. «Субсекторный» характер носят соглашения, заключенные между Россией и учреждениями ЕС, например с Европолом[153].

В исследовании, посвященном правовому регулированию отношений между Россией и ЕС, П. А. Калиниченко выделяет несколько основных сфер такого секторного сотрудничества, урегулированных нормами двусторонних

---

[150] Agreement between the European Union and the Republic of Belarus on the facilitation of the issuance of visas // OJ. 9.6.2020. L 180. P. 3–18.

[151] Agreement between the European Union and the Republic of Peru on the short-stay visa waiver // OJ. 24.3.2016. L 78. P. 4–10.

[152] Соглашение «О партнерстве и сотрудничестве, учреждающее партнерство между Российской Федерацией, с одной стороны, Европейскими сообществами и их государствами-членами, с другой стороны» (Agreement on partnership and cooperation establishing a partnership between the European Communities and their Member States, of one part, and the Russian Federation, of the other part) // OJ. 28.11.1997. L 327. P. 1 ; СЗ РФ. 1998. № 16. Ст. 1802.

[153] Калиниченко П. А. Правовое регулирование отношений между Россией и Европейским Союзом : дис. … докт. юрид. наук. М., 2011.

специальных соглашений. Среди них правоохранительная сфера, представляющая для настоящей диссертации особый интерес.

В правоохранительной сфере между ЕС и Россией заключены следующие соглашения.

Соглашение между Российской Федерацией и Европейским сообществом об упрощении выдачи виз гражданам Российской Федерации и Европейского Союза (г. Сочи, 25 мая 2006 г.)[154], подписанное в рамках первого этапа «безвизового диалога». По словам министра иностранных дел РФ С. В. Лаврова, «безвизовый диалог продолжался с прицелом на переход к полному безвизовому режиму… с технической точки зрения предусматривались и биометрические визы, и реадмиссия…»[155]. Соглашение предусматривало в том числе обязательство сторон обеспечивать высокую степень защиты дипломатических паспортов, в частности путем внесения в них биометрических идентификаторов. Однако в настоящее время действие данного Соглашения по политическим соображениям приостановлено в соответствии с Решением Совета ЕС от 9 сентября 2022 г.[156]

Соглашение между Российской Федерацией и Европейским сообществом о реадмиссии (г. Сочи, 25 мая 2006 г.)[157] содержит нормы общего характера о защите персональных данных, не выделяя при этом биометрических данных и специальных правил обеспечения их защиты (ст. 17 разд. VI «Защита данных»).

Соглашение о сотрудничестве между Российской Федерацией и Европолом (Рим, 6 ноября 2003 г.)[158], целью которого, в соответствии со ст. 1, является расширение сотрудничества между Российской Федерацией и государствами — членами ЕС, действующими через Европол, в борьбе с опасными формами транснациональной преступной деятельности. Статья 2 Соглашения подчеркивает,

---

[154] OJ. 17.5.2007. L 129. P. 27–34 ; СЗ РФ. 2007. № 23. Ст. 2694.

[155] Выступление и ответы на вопросы министра иностранных дел РФ С. В. Лаврова перед студентами и профессорско-преподавательским составом МГИМО по случаю начала учебного года, Москва, 1 сентября 2022 г. [Электронный ресурс] // URL: https://www.mid.ru/ru/press_service/video/posledniye_dobavlnenniye/1828196/ (дата обращения: 13.10.2024).

[156] Council Decision (EU) 2022/1500 of 9 September 2022 on the suspension in whole of the application of the Agreement between the European Community and the Russian Federation on the facilitation of the issuance of visas to the citizens of the European Union and the Russian Federation // OJ. 9.9.2022. L 2341. P. 1–3.

[157] OJ. 17.5.2007. L 129. P. 40–60 ; СЗ РФ. 2007. № 23. Ст. 2693.

[158] Бюллетень международных договоров. 2004. № 3. С. 58–62.

что оно не затрагивает вопросы обмена персональными данными, так как «обмен персональными данными будет осуществляться на основе отдельного соглашения между Сторонами».

Впрочем, как констатирует профессор А. Г. Волеводз, между Россией и ЕС какого-либо соглашения в сфере защиты персональных общего характера не разрабатывалось, и переговоры по его заключению целенаправленно не проводились[159]. К сожалению, изложенное позволяет прийти к выводу, что на данный момент перспектива обсуждения и заключения специального соглашения об обмене биометрическими данными (или хотя бы специальными категориями персональных данных) между Россией и ЕС представляется очень далекой и призрачной, если принять также во внимание сложившуюся политическую ситуацию.

Таким образом, за годы сложившегося сотрудничества России и ЕС в сфере правоохранительной деятельности, а также визовой и иммиграционной политики ни одна из сторон, несмотря на повсеместное применение биометрических данных, не инициировала диалог относительно установления правил использования таких данных. На наш взгляд, это упущение ввиду постоянно растущей актуальности международного сотрудничества по предупреждению и противодействию терроризму, а также расследованию, выявлению и преследованию уголовных преступлений.

Рекомендации и заключения, в соответствии со ст. 288 ДФЕС, не имеют обязательной силы, однако являются востребованным инструментом в нормотворческой практике ЕС. *Рекомендация* служит средством выдвижения предложений института в адрес государств-членов, физических или юридических лиц, например Рекомендация Комиссии от 12 мая 2009 г. о соблюдении принципов конфиденциальности и защиты данных в приложениях, поддерживаемых радиочастотной идентификацией[160]. Данная Рекомендация предусматривает

---

[159] Волеводз А. Г. Защита персональных данных в Европейском союзе. С. 311.

[160] Commission Recommendation of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification (notified under document number C(2009) 3200)) // OJ. 16.5.2009. L 122. P. 47–51.

обработку биометрических данных приложениями радиочастотной идентификации и подчеркивает, что такой обработке должно быть уделено особое внимание с точки зрения информационной безопасности и конфиденциальности.

Заключение является документом, отражающим официальную позицию заинтересованного института ЕС по конкретному вопросу, например Заключение Европейского надзорного органа по защите данных 2006 г. относительно предложения по проекту Регламента Европейского парламента и Совета, вносящему изменения в Общие консульские инструкции по визам для дипломатических представительств и консульских учреждений в связи с введением биометрических данных, включая положения об организации приема и обработки визовых заявлений[161]. В Заключении акцентируется внимание на чувствительной природе биометрических данных, требующей, чтобы введение обязательств по использованию этих данных происходило только после тщательной оценки связанных с ними рисков. Заключение Европейского комитета регионов 2021 г.[162] на проект Нового пакта о миграции и предоставлении убежища[163] содержало замечание относительно минимального возраста заявителей, ходатайствующих о предоставлении международной защиты, в котором возможен сбор биометрических данных. В соответствии с замечанием комитета каждое государство — член ЕС обязано обеспечить сбор данных каждого заявителя, достигшего 12 лет (вместо предложенного в проекте порога в шесть лет). В новом варианте Пакта предусмотрены предварительная идентификация и регистрация мигрантов на внешней границе ЕС. Как верно отметила О. Ю. Потемкина, такие предварительные «проверки безопасности» на внешней границе стали самой сложной проблемой при обсуждении проекта, ведь они включают в себя

[161] Opinion of the European Data Protection Supervisor on the Proposal for a Regulation of the European Parliament and the Council amending the Common Consular Instructions on visas for diplomatic missions and consular posts in relation to the introduction of biometrics including provisions on the organisation of the reception and processing of visa applications (COM (2006) 269 final) — 2006/0088 (COD) // OJ. 29.12.2006. C 321. P. 38–44.

[162] Opinion of the European Committee of the Regions – A New Pact on Migration and Asylum. COR 2020/04843 // OJ. 7.5.2021. C 175. P. 32–68.

[163] Proposal for a Regulation of the European Parliament and the Council on asylum and migration management and amending Council Directive concerning the status of third-country nationals who are long-term residents (COM(2020) 610 final).

медицинский контроль, проведение идентификации мигранта и дактилоскопию с последующей регистрацией результатов в Евродак[164].

В заключение в данном разделе хотелось бы отметить акты, которые регулярно принимаются в рамках попыток совершенствования правил обращения с биометрическими данными и которые зачастую относят к актам «мягкого» права, что является ошибочным. Речь идет об *актах особого рода или так называемых актах sui generis,* которые также входят в систему источников вторичного права ЕС. Данные акты не упоминаются в учредительных договорах, однако факт наличия таковых закреплен Судом в решении по делу «ERTA»[165].

На практике акты особого рода имеют широкое распространение в форме резолюций Совета и резолюций Европейского парламента, а также рамочных решений в области сближения уголовно-правового комплекса и актов, которые принимаются в области безопасности, а именно общих стратегий, общих позиций, совместных акций. Две указанные неэкономические сферы интеграции и сотрудничества до вступления в силу Лиссабонского договора были отнесены к ве́дению институтов ЕС в рамках его «опорной структуры»: общая внешняя политика и политика безопасности (далее — ОВПБ) — в рамках второй «опоры», сотрудничество полиций и судебных органов в уголовно правовой-сфере — в рамках третьей «опоры».

Приведем в качестве примера требование, изложенное в Резолюции Европейского парламента от 15 сентября 2022 г.[166], обращенное к Российской Федерации, о прекращении всех текущих процессов сбора и хранения биометрических данных украинских граждан ввиду того, что так называемый процесс «фильтрации» «носит систематический характер и представляет собой массовый незаконный сбор данных, предоставляя российским властям огромное количество персональных данных об украинских гражданах, включая их

---

[164] Потемкина О. Ю. Европейский Союз в ожидании Пакта о миграции и убежище // Научно-аналитический вестник Института Европы РАН. 2020. № 4. С. 72.

[165] C-22/70, Commission v. Council (ERTA), ECR [1971] 263.

[166] European Parliament resolution of 15 September 2022 on human rights violations in the context of the forced deportation of Ukrainian civilians to and the forced adoption of Ukrainian children in Russia (2022/2825(RSP)) // OJ. 5.4.2023. C 125. P. 67–71.

биометрические данные, что является явным нарушением права на неприкосновенность частной жизни и может подвергнуть тех, кто подвергся этому, риску стать мишенью в будущем».

В целях обеспечения транспарентности и широкого обсуждения биометрических инициатив ЕС также использует и инструменты «зеленых» и «белых» книг. Здесь необходимо отметить, что такие инициативы являются именно вспомогательными инструментами Комиссии, но не представляют собой самостоятельные правовые акты.

Л. Сэнден приводит в своем исследовании мнение Комиссии, что «зеленые книги» — это «документы для размышления и обсуждения», составленные с целью проведения общественных дебатов и консультаций. Это соответствует цели проводить более частые и регулярные консультации с заинтересованными сторонами, прежде чем предлагать какие-либо новые законы или действия Сообщества»[167]. «Белые книги», с одной стороны, представляют собой документы для обсуждения и консультаций; с другой стороны, они также направлены на определение основных направлений или стратегии действий на будущее. Для этого они обычно содержат конкретные предложения по действиям. В зависимости от того, на какой из этих двух аспектов делается акцент, «белые книги» могут значительно отличаться друг от друга: одни «белые книги» больше направлены на обсуждение, другие могут уже содержать (подробные) рабочие программы или графики действий[168].

«Белая книга» по искусственному интеллекту 2020 г.[169] содержит разъяснения по поводу рисков для основных прав человека, которые могут возникнуть в связи с внедрением систем распознавания лиц в общественных местах. Приводятся специальные требования к проведению удаленной биометрической идентификации: обработка должна осуществляться на основании законодательства ЕС или национального законодательства при соблюдении

[167] Commission Report for the Reflection Group (1995). P. 39. COM(94)333 final, p 3.
[168] Senden L. Soft Law in European Community Law. Oxford and Portland : Hart, 2004. P. 127.
[169] White paper on Artificial Intelligence — A European approach to excellence and trust. COM/2020/65 final.

требований пропорциональности, соблюдении сути права на защиту данных и надлежащих гарантий.

С. Источники прецедентного права (case law)

К источникам прецедентного права относятся решения Суда ЕС, а также Трибунала и специализированных трибуналов. Говоря о месте и роли источников данного вида, констатируем, что они занимают промежуточное положение в системе источников права ЕС. Право ЕС широко использует опыт, накопленный судебной практикой ЕС, для решения не только текущих проблем и споров, но и жизненно важных вопросов развития европейской интеграции[170].

Согласимся с утверждением А. В. Колосова, что особенностью Суда ЕС является то, что он представляет собой не только правоприменительный орган, но и правосоздающий, ведь именно благодаря деятельности Суда формируется прецедентное право ЕС, которое актуально для всех государств-членов и национальных судебных органов. Принимаемые Судом прецедентные решения призваны упорядочить и гармонизировать возникающие общественные отношения на территории ЕС для их единообразного понимания[171].

Одна из главных целей нашего исследования — показать, как на практике осуществляется правосудие в области прав человека при неправомерном или ненадлежащем использовании биометрических данных, с какими проблемами сталкиваются граждане и какие решения выносят судебные инстанции. Например, Судом ЕС неоднократно отмечалось, что защита персональных данных играет очень важную роль в реализации права на уважение частной жизни[172]. Чаще всего споры относительно биометрических данных возникают в связи с нарушением именно этого права. Однако сложность рассмотрения дел о нарушении прав человека при использовании биометрических данных заключается в том, что правам человека практически всегда противопоставляются интересы

---

[170] Энтин Л. М. Право Европейского Союза. Новый этап эволюции: 2009–2017 годы. С. 81.

[171] Колосов А. В. Указ. соч. С. 93.

[172] C-293/12 and C-594/12, Digital Rights Ireland of 8 April 2014 [Электронный ресурс] // URL: https://curia.europa.eu/ juris/liste.jsf?num=C-293/12 (дата обращения: 02.08.2024). Para. 48.

общественной или национальной безопасности, которые зачастую имеют больший вес при вынесении решения судами.

Об этом свидетельствует решение по делу «Шварц против Бохум», в котором Суд ЕС постановил, что сбор отпечатков пальцев является обоснованной и законной мерой, необходимой для защиты общественных интересов и ограничения нелегального въезда на территорию ЕС. Аналогично позднее, в 2020 г., Судом ЕС было подчеркнуто, 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[173].

Пункт 1 ст. 52 Хартии ЕС об основных правах также устанавливает, что любое ограничение на осуществление прав и свобод, признанных Хартией, должно предусматриваться законом и уважать основное содержание данных прав и свобод. При этом при соблюдении принципа пропорциональности ограничения могут вводиться лишь тогда, когда они являются необходимыми и действительно соответствуют целям общего интереса, признанным Союзом, или потребности в защите прав и свобод других лиц.

Отметим также пункт 3 ст. 52 Хартии ЕС об основных правах, который указывает на корреспондирующие закрепленным в Хартии правам права, гарантированные ЕКПЧ, участниками которой являются все государства — члены ЕС. Здесь же упоминается возможность «предоставления более широкой защиты со стороны права Союза».

Таким образом, на территории государств — членов ЕС действует две региональные европейские системы защиты прав человека, каждая из которых

---

[173] C-623/17, Privacy International v. Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service, Secret Intelligence Service, of 6 October 2020 [Электронный ресурс] // URL: https://gdprhub.eu/index.php?title=CJEU_-_C-623/17_-_Privacy_International_(BCD_case) (дата обращения: 02.08.2024).

имеет свой орган судебного контроля[174], а именно Суд ЕС (в рамках применения законодательства ЕС, в частности Хартии ЕС об основных правах) и ЕСПЧ (в рамках применения ЕКПЧ), решения которого не рассматриваются как источники права ЕС, однако правовые позиции которого могут оказывать влияние на правоприменительную практику ЕС и наоборот.

Вопрос о конкурирующем характере взаимодействия Суда ЕС и ЕСПЧ, а также о присоединении ЕС к ЕКПЧ широко обсуждается в науке международного и европейского права. Одним из последних является очень полное с точки зрения истории, теории и практики исследование М. Л. Энтина и Н. А. Цвейбы, которое посвящено кросс-цитатному взаимодействию Суда ЕС и ЕСПЧ[175]. Авторы отмечают высокую значимость метода перекрестных судебных отсылок в развитии института защиты прав и свобод человека в Европе.

Впрочем, имеет место и замечание Л. М. Чуркиной о том, что основным негативным последствием конкуренции двух систем, которая всё же сохраняется, является риск вынесения противоречивых, несовместимых решений различными международными судами, что впоследствии приводит к возникновению конфликтов юрисдикций разных международных судебных органов, а также противоречит принципу неделимости и принципу универсальности основных прав человека[176].

При рассмотрении споров о нарушении прав человека и неправомерном использовании биометрических данных очень важно руководствоваться едиными принципами и сохранять единообразие в принятии решений.

Взаимодействие Суда ЕС и ЕСПЧ является важнейшим элементом сохранения единства европейской правой системы в целом и европейской системы защиты прав человека в частности. Одновременно с этим А. С. Исполинов отмечает существование нескольких наиболее острых проблем в отношениях Суда

---

[174] Войников В. В. Право Европейского Союза в практике Европейского Суда по правам человека // Международное правосудие. 2020. № 1 (33). С. 51.

[175] Энтин М. Л., Цвейба Н. А. Взаимодействие судебных органов (на примере Суда Европейского союза и Европейского суда по правам человека) // Московский журнал международного права. 2023. № 3. С. 84–97.

[176] Чуркина Л. М. Конкуренция юрисдикций Европейского суда по правам человека и Суда Европейского Союза // Право и практика. 2023. № 3. С. 145.

ЕС и ЕСПЧ, в том числе в вопросах применения системы предоставления убежища в ЕС (Дублинской системы)[177]. Обозначенная А. С. Исполиновым проблема заключается в расхождении конструкции, лежащей в основе Дублинской системы[178], с устоявшейся практикой и стандартами ЕСПЧ. При рассмотрении вопросов, связанных с нарушением прав человека в пределах применения Дублинской системы, использование биометрических данных для внесения в Евродак может также стать объектом пристального внимания в рамках оценки рисков такого нарушения.

Провести более детальный анализ решений ЕСПЧ и взаимодействия с практикой Суда ЕС предлагается уже не в рамках рассмотрения источников права ЕС, а в контексте международной защиты прав человека в гл. 3 диссертационного исследования.

§ 2.2. Регулирование использования биометрических данных в национальном законодательстве государств — членов ЕС

Правила использования биометрических данных могут содержаться совершенно в любом нормативном правовом акте государства-члена — как в законодательстве о персональных данных, так, например, и в актах в области трудового или корпоративного права. Главное условие изложения таких правил заключается в том, чтобы они не противоречили нормам, закрепленным в правовых актах Союза. Это обусловлено в первую очередь спецификой права ЕС, а именно присущими ему функциональными принципами, и его соотношением с национальным правом государств-членов.

ЕС как наиболее развитая интеграционная организация превратился в общепризнанную самостоятельную правовую систему, в рамках которой действует принципы верховенства и прямого действия, существует обширное первичное,

[177] Исполинов А. С. Практика ЕСПЧ в отношении Европейского Союза: некоторые уроки для ЕврАзЭс // Журнал зарубежного законодательства и сравнительного правоведения. 2012. № 3. С. 112.

[178] Дублинская система — это особый региональный международно-правовой механизм, обеспечивающий предоставление международной защиты различным категориям мигрантов (лицам, ищущим убежище, беженцам и т.д.).

вторичное и прецедентное право, которому непосредственно подчиняются субъекты данного права[179].

Как и любые принципы права, принципы прямого действия и верховенства представляют собой основные начала правовой системы, которые определяют содержание правотворческой, правоприменительной и правоохранительной деятельности[180]. Благодаря практике Суда Европейских сообществ (в настоящее время — Суд ЕС) они были привнесены в теорию европейского права в качестве принципов функционального характера, определяющих соотношение права Сообщества с правовыми системами государств-членов[181].

На тот момент договоры о создании Европейских сообществ не содержали конкретных положений относительно взаимосвязи права Сообществ и национального права, однако со временем принцип верховенства был сформулирован Судом в решении по делу № 6/64 «Costa v. ENEL»[182] и подробно развит в решении по делу № 106/77 «Simmenthal»[183], а принцип прямого действия определен в решении по делу № 26/62 «Van Gend». Однако наиболее четкое и полное представление о взаимоподчинении национальных правовых систем и правовой системы ЕС формируется на основании выводов по вышеуказанным делам в решении по объединенному делу № 6/90 и 9/90 «Francovich»[184].

Суть первого заключается в том, что в случае коллизии норм права ЕС и норм национального законодательства государств — членов ЕС приоритет отдается нормам права ЕС. Кроме того, отметим закрепление принципа верховенства права в Декларации № 17 к Лиссабонскому договору, в которой всеми государствами-членами признается, что «согласно устойчивой судебной практике Суда ЕС, Договоры и право, создаваемое Союзом на основании Договоров, обладают

---

[179] Кашкин С. Ю. Интеграционное право как перспективное направление развития юридической науки и образования // Актуальные проблемы российского права. 2014. № 10. С. 21–52.

[180] Калиниченко П. А. Принципы прямого действия и верховенства: от права ЕС к праву ЕАЭС // Центральная и Восточная Европа: между Евросоюзом и Евразийским экономическим союзом: перспективы соперничества и сотрудничества. М. ; Люблин, 2019. С. 112.

[181] Rasmussen M. Revolutionazing European Law: A History of Van Gend en Loos Judgment // International Journal of Constitutional Law. 2004. Vol. 12. P. 136–163.

[182] C-6/64, Costa v. ENEL, ECR [1964] 585.

[183] C-106/77, Amministrazione delle Finanze dello Stato v. Simmenthal SpA, ECR [1978] 629.

[184] C-6/90 and C-9/90, Francovich and Bonifaci v. Italy, [1991]; C-7/90, Criminal proceedings against Paul Vandeyenne and others, [1991] ECR I-4371.

приматом над правом государств-членов на условиях, определенных упомянутой судебной практикой».

Принцип прямого действия означает, что право ЕС распространяется как на государств-членов, так и на их граждан. Прямым действием обладают учредительные договоры ЕС, нормативные и индивидуальные акты, издаваемые институтами (главными органами) ЕС в порядке ст. 288 ДФЕС, а также соглашения ЕС с третьими странами.

Согласно п. 3 ст. 4 ДЕС «Государства-члены предпринимают любые меры общего или специального характера, которые способны обеспечить исполнение обязанностей, вытекающих из Договоров или проистекающих из актов институтов Союза». В дополнение статья 291 ДФЕС также устанавливает обязанность государств-членов принимать все меры в области внутреннего права, необходимые для претворения в жизнь юридически обязательных актов Союза.

Возвращаясь к ст. 288 ДФЕС, напомним, что регламент имеет общее действие, является обязательным в полном объеме и подлежит прямому применению во всех государствах-членах. Директива аналогично имеет обязательную силу для каждого государства-члена, которому она адресована, в отношении результата, которого требуется достичь.

В рамках нашего исследования мы предлагаем провести анализ трансформации действующих в настоящее время актов ЕС, предусматривающих правила обращения с биометрическими данными, в национальном законодательстве государств — членов ЕС, в том числе Регламента о защите данных и Директивы 2016/680/ЕС.

В силу п. 10 Преамбулы Регламента о защите данных государствам-членам предоставляется возможность принимать собственные правила, в том числе и обработки особых категорий персональных данных. При этом Регламент не исключает право государства-члена определять обстоятельства для особых ситуаций обработки данных, включая определение более четких условий, при

которых такая обработка персональных данных будет правомерной[185].

Для нашего исследования особый интерес представляют нормы, конкретизирующие процедуры использования биометрических данных, оставленные на усмотрение государств-членов. Например, девять стран ЕС на данный момент отказались или не планируют внедрять криминалистическую аутентификацию на основе биометрических данных для судебно-медицинских целей: Бельгия, Болгария, Дания, Ирландия, Люксембург, Мальта, Польша, Португалия и Словакия. В то же время 11 государств — членов ЕС активно это используют: Австрия, Финляндия, Германия, Греция, Венгрия, Италия, Латвия, Литва, Нидерланды и Словения.

Отметим, что на момент принятия Директивы 95/46/ЕС подход государств-членов к определению понятия «биометрические данные», отнесению их к какой-либо категории персональных данных и правовому регулированию их обработки был различным в связи с тем, что унифицированного законодательного закрепления такого вида персональных данных в актах ЕС еще не существовало.

С принятием Регламента 2016/679 и Директивы 2016/680/ЕС нормы национального права государств-членов, касающиеся регулирования биометрических данных, стали унифицированными в части определения биометрических данных, отнесения их к специальным категориям персональных данных, а также условий обработки. Однако в силу п. 4 ст. 9 Регламента за государствами — членами ЕС оставлено право сохранять или вводить дополнительные условия, в том числе ограничения, в отношении обработки биометрических данных.

В *Германии* действует BDSG, в котором отдельно урегулированы вопросы реализации Регламента 2016/679 и Директивы 2016/680/ЕС, а также вопросы, в которых допускаются отступления в части обработки специальных категорий данных, в том числе биометрических.

В разделе 22 BDSG предусмотрено, что обработка таких категорий данных

[185] General Data Protection Regulation. P. 2.

разрешена в упомянутых BDSG случаях, например в целях профилактической медицины, постановки медицинского диагноза, обеспечения общественного интереса в сфере здравоохранения, для обеспечения значимого общественного интереса, предотвращения угрозы общественной безопасности. При этом такая обработка допустима при принятии мер защиты прав субъектов данных (включая технические меры, шифрование, псевдонимизацию, ограничение доступа к данным и пр.). Кроме того, раздел 27 BDSG предусматривает обработку конфиденциальных данных для целей научных или исторических исследований или статистических целей при соблюдении определенных условий.

Отдельно хотелось бы выделить разрешенные BDSG системы видеонаблюдения за публичными местами в установленных законом целях. К таким целям относятся выполнение государственным органом возложенных на него задач, обеспечение общественной безопасности, защита жизни и здоровья и иных интересов присутствующих в общественном месте, если ничто не указывает на законные интересы субъекта данных, которые определяются как первостепенные (разд. 4 BDSG). В том же разделе также предусмотрены условия как можно более раннего уведомления о слежке, информирования субъекта данных, чьи личные данные могут быть собраны в результате слежки, и удаления данных, если в этом больше нет необходимости.

Современные системы видеонаблюдения в настоящее время являются одним наиболее эффективных средств, способствующих реализации мероприятий по предупреждению преступности. Зачастую они оснащены специальными цифровыми камерами с функцией «интеллектуального видео». Данная функция позволяет анализировать статические (фотографии) и динамические (видеозаписи) изображения и сверять полученную информацию с имеющимися базами данных[186]. Если предположить, что подобные изображения могут сопоставляться с информацией из баз данных, содержащих сведения о биометрических

[186] Гусенкова А. А. Применение систем видеонаблюдения и автоматизированных систем биометрической идентификации человека при производстве портретных экспертиз и исследований (на примере аппаратно-программного комплекса «Безопасный город») // Вестник Московского университета МВД России. 2021. № 6. С. 86.

характеристиках, и таким образом лицо будет идентифицировано, то мы можем констатировать, что раздел 4 BDSG косвенно распространяется на обработку биометрических данных.

В национальном законодательстве *Кипра* действует Закон о защите физических лиц в отношении обработки их персональных данных и свободного перемещения таких данных от 16 октября 2018 г. № 125(I)[187].

В соответствии со ст. 9 разд. II Закона конкретно генетические и биометрические данные не подлежат обработке в целях получения медицинского страхования и страхования жизни, даже если субъект данных дал согласие. Если обработка генетических и биометрических данных основана на согласии субъекта данных, последующая обработка таких данных требует наличия отдельного согласия субъекта данных.

Франция является одной из самых продвинутых стран по внедрению специального регулирования использования биометрических данных на уровне национального законодательства, особенно в области трудовых правоотношений, что заслуживает отдельного внимания.

В настоящее время органом во Франции, осуществляющим надзор за соблюдением законодательства о защите персональных данных, является Национальная комиссия по делам информационных технологий и правам человека (Commission nationale de l'informatique et des libertés, CNIL), а основным законом в области защиты данных — Закон от 6 января 1978 г. № 78-17 об информационных технологиях, файлах данных и гражданских свободах с изменениями, принятыми в связи вступлением в силу Регламента о защите данных в 2018 г. (Закон от 20 июня 2018 г. № 2018-493).

Закон от 6 января 1978 г. № 78-17 устанавливает правила обработки конфиденциальных данных, включая биометрические данные, с ссылкой на условия и цели обработки, предусмотренные в Регламенте о защите данных, а

[187] Law providing for the protection of natural persons with regard to the processing of personal data and for the free movement of such data [Электронный ресурс] // URL: https://www.dataguidance.com/legal-research/law-125i-2018-providing-protection-natural (дата обращения: 04.04.2024).

также в ст. 44 Закона. Согласно указанной статье эти цели включают повторное использование информации, содержащейся в судебных определениях и решениях, при условии, что ни целью, ни результатом такой обработки не является повторная идентификация субъектов данных, а также обработку биометрических данных работодателями или административными органами, если строго необходимо контролировать доступ к рабочим местам, оборудованию и приложениям, используемым сотрудниками, агентами, стажерами или поставщиками услуг в своих заданиях.

На CNIL возложена ответственность за установление и доведение до общественности правил обработки биометрических, медицинских и генетических данных, которые Регламент о защите данных рассматривает как конфиденциальные. Так, в 2019 г. CNIL было подготовлено и опубликовано Типовое положение, предусматривающее правила использования работодателями биометрических средств контроля доступа на рабочем месте[188]. Типовое положение устанавливает жесткие требования к обработке биометрических данных для контроля доступа на рабочем месте:

1) обоснование использования биометрических данных. Такое обоснование должно быть четко задокументировано работодателем, включая обоснование выбора одной биометрической функции вместо другой для аутентификации;

2) обеспечение надежной защиты данных. В Типовом положении подробно описаны многочисленные способы, с помощью которых работодатели должны поддерживать надежные организационные и технические процедуры защиты биометрических данных. Типовое положение также устанавливает максимальные сроки хранения биометрических данных;

3) соблюдение обязательств в соответствии с Регламентом 2016/679.

---

[188] Goldsmith L., Pepin M. French DPA Issues Robust Model Regulation for Biometric Access Controls in the Workplace [Электронный ресурс] // The National Law Review. April 24. 2019. Vol. XIII. No. 75. URL: https://www.natlawreview.com/article/french-dpa-issues-robust-model-regulation-biometric-access-controls-workplace (дата обращения: 04.02.2024).

В *Испании* инструментом трансформации Регламента о защите данных служит Закон от 5 декабря 2018 г. № 3/2018 «О защите персональных данных и гарантии цифровых прав»[189], который не ввел дополнительных условий или ограничений в отношении обработки биометрических данных. Одновременно с этим Испанское агентство по защите данных (Spanish Data Protection Authority)[190] ведет разработку рекомендаций по ответственному использованию биометрических данных в различных областях и публикует аналитические и отчетные материалы, освещающие правовые проблемы, с которыми сталкиваются субъекты и контролеры данных на практике.

Статья 16-22 Закона *Португалии* от 12 февраля 2009 г. № 7/2009 (Трудовой кодекс Португалии) устанавливает правила обработки данных на рабочем месте, а именно правила, касающиеся обработки биометрических данных работника, требования медицинского осмотра как условия приема на работу и использования методов дистанционного наблюдения[191].

В Бельгии одновременно с вступлением в силу Регламента о защите данных начал действовать Закон о защите физических лиц в отношении обработки персональных данных от 30 июля 2018 г. (Рамочный закон), который предусматривает дополнительные требования к контролерам при обработке биометрических данных, а именно:

— вести список категорий лиц, имеющих доступ к персональным данным, с описанием их функций;

— предоставлять этот список по запросу Управления по защите данных[192];

— обеспечить, чтобы эти лица были связаны установленными законом или договором обязательствами по соблюдению конфиденциальности в отношении

---

[189] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales [Электронный ресурс] // Boletín oficial del estado legislación consolidada. 06.12.2018. N. 294. P. 119788–119857. URL: https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf (дата обращения: 04.03.2024).

[190] Независимый орган правительства Испании, который контролирует соблюдение правовых положений о защите личных данных. Штаб-квартира агентства находится в Мадриде.

[191] Lei nº 7/2009, de 12 de fevereiro [Электронный ресурс] // URL: https://diariodarepublica.pt/dr/detalhe/lei/7-2009-602073 (дата обращения: 04.05.2024).

[192] Act of 3 December 2017 establishing the Data Protection Authority (AH-2022-0020) [Электронный ресурс] // URL: https://www.autoriteprotectiondonnees.be/publications/opinion-on-preliminary-draft-law-amending-the-act-of-3-december-2017-establishing-the-data-protection-authority.pdf (дата обращения: 04.05.2024).

данных.

В соответствии с адаптированным под Регламент о защите данных национальным законодательством *Польши*[193] биометрические данные лиц, оказывающих услуги Польскому национальному банку или перевозящих активы с денежной стоимостью (отпечатки пальцев, голос, рисунки вен пальцев или рук), могут подлежать обработке Польским национальным банком. Такая обработка может осуществляться до тех пор, пока выполняются вышеуказанные услуги.

Национальное законодательство *Словении* является одним из наиболее насыщенных в части содержания норм, касающихся обработки биометрических данных.

Во-первых, Закон о защите данных Словении[194] отдельно предусматривает наложение незначительных штрафов на государственные органы за нарушение обязательств, связанных с обработкой биометрических данных.

Во-вторых, установлено, что в государственном секторе биометрические данные могут обрабатываться в соответствии с законом, только если соответствующие цели не могут быть достигнуты другими способами и только в следующих случаях:

— обеспечение безопасности людей или имущества;

— обеспечение безопасности секретных данных;

— соблюдение обязательств по международным договорам;

— обеспечение безопасности границ;

— идентификация пропавших без вести или умерших лиц;

— обеспечение коммерческой тайны.

В частном секторе обработка биометрических данных разрешена законом, если такая обработка необходима для следующих целей:

— обеспечение безопасности людей или имущества;

---

[193] Act of 10 May 2018 on the Protection of Personal Data (the Data Protection Act) ; Act of 21 February 2019 on the amendments of some legal acts in connection with the implementation of the GDPR [Электронный ресурс] // URL: https://www.dataguidance.com/legal-research/act-10-may-2018-protection-personal-data (дата обращения: 04.05.2024).

[194] Personal Data Protection Act (Zakon o varstvu osebnih podatkov, ZVOP-1) [Электронный ресурс] // URL: https://rm.coe.int/16806af30c (дата обращения: 04.05.2024).

— обеспечение безопасности секретных данных;

— обеспечение коммерческой тайны.

При обработке биометрических данных в частном секторе контролеры данных и обработчики обязаны заранее уведомить национальный орган, осуществляющий надзор в области защиты персональных данных, который в течение двух месяцев примет решение о том, соответствуют ли меры законодательству.

Обработка биометрических данных в маркетинговых целях в Словении запрещена, даже если она осуществляется в обмен на бесплатные услуги.

Национальное законодательство государств — членов ЕС так или иначе оказывает влияние на общую правоприменительную практику регулирования биометрических данных, вводя либо дополнительные ограничения в сфере использования биометрических данных (Германия, Франция, Италия, Словения, Бельгия и др.), либо дополнительные гарантии и меры защиты биометрических данных (Испания, Португалия, Литва и др.).

Вместе с тем национальное законодательство государств — членов ЕС, которые ввели дополнительные условия или ограничения в отношении обработки биометрических данных, не носит комплексного характера и не является гармонизированным. В большинстве случаев регулирование использования биометрических данных в государствах-членах ограничивается правовыми актами в области защиты персональных данных, и лишь в некоторых странах отдельные правила о биометрических данных установлены в иных сферах (трудовом, медицинском, визовом праве или в нормах об искусственном интеллекте).

§ 2.3. Международно-правовые основы регулирования использования биометрических данных в Европейском Союзе

Как было рассмотрено в первой главе, именно принятые международными организациями правила по внедрению биометрических данных в документы, удостоверяющие личность, стали истоком формирования единой правовой базы

выдачи биометрических паспортов и проездных документов в праве ЕС. Это представляется закономерным в силу того, что международное право развивается «на основе объективно непреложных закономерностей общественного развития, которые являются ключом к пониманию причин такого развития и его осуществления лишь по пути прогресса»[195].

Роль международного права в формировании регулирования правоотношений в любой области значительна, в особенности если речь идет о правах человека в связи с использованием его личных данных.

В соответствии с п. 5 ст. 3 ДЕС в своих отношениях с остальным миром Союз утверждает и продвигает свои ценности и интересы и содействует защите своих граждан. Он способствует «неукоснительному соблюдению и развитию международного права, особенно соблюдению принципов Устава Организации Объединенных Наций»[196].

Глава 1 «Общие положения о внешнеполитической деятельности Союза» ДЕС содержит основополагающие цели и принципы, которые должны соблюдаться ЕС при осуществлении действий на международной арене по всем вопросам и направлениям, с особой отсылкой к необходимости соблюдения принципов, закрепленных в Уставе ООН и других источниках международного права (ст. 21 ДЕС). Здесь к числу основополагающих принципов внешнеполитической деятельности Союза относятся такие фундаментальные начала, как демократия, правовое государство, всеобщность и неделимость прав человека и основных свобод и др.

Правовое регулирование использования биометрических данных на международном уровне исторически осуществлялось и в настоящее время осуществляется в двух направлениях: безопасность и права человека.

Под безопасностью подразумевается прежде всего информационная безопасность, объектами которой являются личность, общество и государство,

---

[195] Мовчан А. П. Кодификация и прогрессивное развитие международного права. М., 1972. С. 9.

[196] Договор о Европейском Союзе (г. Маастрихт, 7 февраля 1992 г.) // Кашкин С. Ю., Четвериков А. О. Указ. соч. С. 19.

согласно подходу, изложенному в монографии А. В. Корнева и О. В. Танимова[197]. Однако в контексте нашего исследования мы предложили бы не ограничиваться перечисленными категориями объектов и добавили бы региональный и международный аспекты, так как биометрические данные выступают инструментом решения глобальных задач безопасности (в том числе противодействия международному терроризму) и регулируются актами таких интеграционных объединений, как ЕС, а не только национальным законодательством.

Предметное определение угроз международной безопасности, которая в целом, как отмечает профессор Н. А. Соколова, имеет универсальный характер, позволяет направить усилия на оптимизацию международного сотрудничества в соответствующей сфере[198].

Роль международного сотрудничества особенно высока в условиях растущего числа новых проблем и угроз, с которыми сталкиваются государства всего мира и их граждане, особенно с учетом стремительного развития информационных и биотехнологий. А. Х Абашидзе в качестве инструмента эффективного противостояния таким вызовам и угрозам видит объединение усилий и согласованность действий государств. «Это можно достичь лишь на основе международных соглашений и с помощью эффективного функционирования международных межправительственных организаций»[199], — отмечает профессор.

При реализации государствами совместных мероприятий с использованием биометрических данных в рамках обеспечения безопасности личности, общества, государства, объединения, мира, так или иначе, гарантированные международными актами в области прав человека права прямо или косвенно могут подвергаться риску нарушения. Предлагаем установить, как регулируются

---

[197] Корнев А. В., Танимов О. В. Информационное право в условиях цифровой трансформации российского права : монография. М. : Проспект, 2022. С. 162.

[198] Соколова Н. А. Международно-правовые аспекты биобезопасности // Московский журнал международного права. 2006. № 1. С. 385.

[199] Абашидзе А. Х. Правозащитная роль современного международного права в условиях инноваций и широкого применения нанотехнологий // Legal Concept. 2012. № 1. С. 74.

правоотношения в сфере обращения с биометрическими данными в указанных направлениях через инструментарий международного права.

Сперва остановимся на основных принципах, которые представляют собой общие нормы международного права, определяющие его главное содержание и характерные черты, обладающие высшим политическим, моральным и юридическим авторитетом[200]. При определении данной группы источников О. Е. Кутафин особо отмечал их «общепризнанность», приводя в качестве примера тот факт, что отсутствие поддержки какого-либо акта большинством того или иного международного форума не даст серьезных шансов такому акту стать юридически обязательными «общепризнанными» нормами[201].

Г. И. Тункин определяет основные принципы как общепризнанные принципы международного права, имеющие наибольшее значение для решения основных проблем современных международных отношений. «Современное международное право отличается от буржуазного, или “классического”, международного права прежде всего своими основными принципами», — отмечал ученый[202].

Среди общепризнанных принципов международного права, которые имеют первостепенное значение для регулирования использования биометрических данных, важную роль играет «обязанность государств сотрудничать друг с другом», закрепленная в различных областях международных отношений с целью поддержания международного мира и безопасности. Она выступает одним из основных (руководящих) принципов международного права, закрепленных в Декларации о принципах международного права, касающихся дружественных отношений и сотрудничества между государствами в соответствии с Уставом Организации Объединенных Наций[203].

---

[200] Лукашук И. И. Нормы международного права в правовой системе России // Журнал российского права. 2002. № 3.

[201] Кутафин О. Е. Источники конституционного права Российской Федерации. М. : Юристъ, 2002.

[202] Тункин Г. И. Право и сила в международной системе. М. : Междунар. отношения, 1983. С. 33.

[203] Декларация о принципах международного права, касающихся дружественных отношений и сотрудничества между государствами в соответствии с Уставом Организации Объединенных Наций (принята 24 октября 1970 г. Резолюцией 2625 (XXV) на 1883-м пленарном заседании Генеральной Ассамблеи ООН) (Doc. A/RES/2625(XXV)).

В соответствии с Декларацией такая обязанность реализуется в том числе посредством сотрудничества государств в установлении всеобщего уважения и соблюдения прав человека и основных свобод для всех и в ликвидации всех форм расовой дискриминации и всех форм религиозной нетерпимости, а также осуществления государствами международных отношений в экономической, социальной, культурной, технической и торговой областях в соответствии с принципами суверенного равенства и невмешательства.

В статье 1 Устава ООН поддержание международного мира и безопасности и осуществление международного сотрудничества в разрешении международных проблем экономического, социального, культурного и гуманитарного характера и в поощрении и развитии уважения к правам человека и основным свободам для всех, без различия расы, пола, языка и религии, провозглашены целями ООН[204].

Рассуждая о принципах международного права в области нашего исследования, можно установить, что «вследствие ускорения темпов развития науки и техники, в частности биотехнологии, и значительного прогресса в генной инженерии» принцип поддержания международного мира и безопасности значительно эволюционировал в интересующем нас контексте. К такому выводу приходит Л. П. Ануфриева[205], отмечая, что изначально «главный фокус содержания принципа всеобщей безопасности концентрировался на военной безопасности», в то время как сегодня широкое распространение имеет такой аспект всеобщей безопасности, как информационная безопасность, которой в международных документах и литературе последних десятилетий отводится значительное место».

Вышеизложенное Л. П. Ануфриева иллюстрирует положением Итогового документа Венской встречи Организации по безопасности и сотрудничеству в Европе (1986 г.): «Отмечая прогресс, достигнутый в исследованиях и разработках в области биотехнологии, и создаваемые ими возможности, государства-участники

---

[204] Устав Организации Объединенных Наций (Сан-Франциско, 26 июня 1945 г.) [Электронный ресурс] // Официальный сайт ООН. URL: https://www.un.org/ru/about-us/un-charter/full-text (дата обращения: 03.04.2024).

[205] Ануфриева Л. П. Принципы в современном международном праве (некоторые вопросы понятия, природы, генезиса, сущности и содержания) // Московский журнал международного права. 2021. № 1. С. 18.

считают желательным расширить обмен информацией о законах и правилах, относящихся к аспектам безопасности генной инженерии. Они будут поэтому способствовать консультациям и обмену информацией по правилам безопасности».

Общепризнанные принципы международного права принято рассматривать в качестве императивных норм (jus cogens), которые имеют приоритет над нормами права ЕС. Это подтверждают положения учредительных документов Союза. Так, в Преамбуле Договора о Европейском сообществе провозглашалась приверженность «принципам Устава ООН»[206]. Однако в силу своей социальной сущности право ЕС не просто подчиняется таким нормам, но и преобразует их (используя методы гармонизации и унификации) в целях оптимального развития интеграционных процессов на территории Союза[207]. Как отмечает профессор А. Г. Волеводз, изначально основной нормативно-правовой базой ЕС в этой сфере являлись международные инструменты. По мере развития информационно-коммуникационных технологий в ЕС был взят курс на формирование своих внутренних, более детальных регуляций в этой области, которые динамически изменяются (совершенствуются)[208].

Что касается международных источников, которые содержат нормы, имеющие значение для регулирования биометрических данных, то было бы логичным их рассматривать прежде всего через категорию «персональные данные» и разделить по критерию «сфера прав человека — сфера безопасности»; дальнейшую классификацию можно было бы провести по следующим признакам:

— «общие — специальные», где первые направлены на регулирование отдельных сфер, например прав человека или безопасности, и являются косвенными регуляторами сферы биометрических данных, а вторые направлены конкретно на регулирование отношений, возникающих в связи с использованием биометрических данных, и установление специальных принципов и правил

---

[206] Введение в право Европейского Союза : учеб. для студентов вузов / С. Ю. Кашкин, П. А. Калиниченко, А. О. Четвериков ; под ред. С. Ю. Кашкина. 3-е изд., перераб. и доп. М. : Эксмо, 2010. С. 83.

[207] Введение в право Европейского Союза : учеб. для студентов вузов. С. 83.

[208] Волеводз А. Г. Защита персональных данных в Европейском союзе. С. 303.

поведения. Однако здесь же мы сталкиваемся с тем, что специальных актов регулирования на международном уровне исследуемой нами области практически нет, например, в отличие от сфер биомедицины[209] или генома человека[210];

— «универсальные — региональные», т.е. многосторонние, содержащие нормы, объект и цели которых представляют интерес для всех государств, и, напротив, для стран отдельного географического региона, института;

— по виду акта («международный договор — акт международной межправительственной/неправительственной организации»).

Предлагаем исследовать международные источники на наличие в них положений, способных регулировать сферу биометрических данных, через классификацию по организации (институту), принявшему акт (договор), которая, в свою очередь, позволит провести остальные вышеперечисленные классификации.

Организация объединенных наций

На сегодняшний день на международном уровне сложился организационно-правовой механизм обеспечения международной безопасности, во главе которого находится ООН[211].

Согласно Уставу ООН, главные органы ООН имеют ряд полномочий по поддержанию мира и международной безопасности. Основными органами, которые обеспечивают выполнение обязательств государствами — членами ООН и реализацию закрепленных Уставом ООН принципов, являются Генеральная Ассамблея и Совет Безопасности[212]. Данные органы принимают резолюции — письменные акты, отражающие официальную позицию ООН и подлежащие обязательному выполнению всеми странами — членами ООН[213]. В таких

---

[209] Конвенция о защите прав и достоинства человека в связи с применением достижений биологии и медицины: Конвенция о правах человека и биомедицине (СЕД No. 164). Открыта для подписания 4 апреля 1997 г. в г. Овьедо (Испания).

[210] Всеобщая декларация о геноме человека и правах человека от 11 ноября 1997 г. Принята на XXIX сессии Генеральной конференции ООН по вопросам образования, науки и культуры [Электронный ресурс] // URL: https://www.un.org/ru/documents/decl_conv/declarations/human_genome.shtml (дата обращения: 08.08.2024).

[211] Гуляева, Е. Е. Роль международных организаций в противодействии биотерроризму / Е. Е. Гуляева // Евразийский юридический журнал. 2023. № 10 (185). С. 34.

[212] Главными органами ООН являются Генеральная Ассамблея, Совет Безопасности, Экономический и социальный совет, Совет по опеке, Международный Суд и Секретариат ООН.

[213] Федоров В. Н. Организация Объединенных Наций, другие международные организации и их роль в XXI веке. М. : Логос, 2007. С. 67.

документах Совет Безопасности и Генеральная Ассамблея ООН подчеркивают, что государства обязаны обеспечить, чтобы любые меры, принимаемые в целях борьбы с терроризмом, соответствовали всем их обязательствам по международному праву, и прежде всего международным стандартам в области прав человека[214].

Первым международным актом, в котором была признана необходимость защиты прав и свобод человека, закреплено право на личную неприкосновенность и невмешательство в частную жизнь, является *Всеобщая декларация прав человека 1948 г.*[215] В статье 12 документа закреплено, что «никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произвольным посягательствам на неприкосновенность его жилища, тайну его корреспонденции или на его честь и репутацию. Каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств»[216].

Несмотря на то что Всеобщая декларация не относится к числу основных источников международного права и не является документом обязательной юридической силы (формально это документ, принятый Резолюцией Генеральной Ассамблеи ООН, а следовательно, он является производным актом рекомендательного характера), это единственный источник такого рода, который фактически имеет признанную всеми субъектами международного права юридическую силу, поскольку все права, гарантированные Декларацией, закреплены в основных источниках международного права[217].

Право на неприкосновенность и невмешательство в личную и семейную жизнь, закрепленное во Всеобщей декларации, подтверждено основными *международными договорами о правах человека*, имеющими силу для государств — членов ЕС. К таким документам относятся Международный пакт о гражданских и политических правах 1966 г., Конвенция о правах ребенка, ЕКПЧ (представляющая собой международный договор регионального уровня) и др.

---

[214] См., например, резолюции 1373 (2001), 1624 (2005), 2178 (2014) и 2396 (2017) Совета Безопасности; резолюции A/RES/68/276 и A/70/L.55 Генеральной Ассамблеи.

[215] Всеобщая декларация прав человека [Электронный ресурс] // URL: https://www.un.org/ru/documents/decl_conv/declarations/declhr.shtml (дата обращения: 15.03.2024).

[216] Всеобщая декларация прав человека.

[217] Котляр И. И. Права человека : учебное пособие. Минск : Право и экономика, 1996. С. 79.

В этих документах более подробно раскрыто право на неприкосновенность и невмешательство в личную и семейную жизнь[218], которое является основой для защиты персональных данных вообще и биометрической информации в частности[219].

Конвенция о правах ребенка не только закрепляет, но и детализирует индивидуальные права каждого человека до достижения им 18 лет, в том числе право на невмешательство в личную и семейную жизнь. Большое значение для защиты персональных данных имеет принятое в 2021 г. в рамках Конвенции Замечание Комитета по правам ребенка[220], в котором рекомендуется ограничить доступность персональных данных детей и предоставить к ним доступ только органам власти, организациям и лицам, уполномоченным законом обрабатывать их, с соблюдением таких процессуальных гарантий, как регулярные проверки и подотчетность.

Среди актов, принятых Генеральной Ассамблеей ООН, которые указывают на необходимость защиты конфиденциальной информации вообще, можно выделить также:

— Резолюцию Генеральной Ассамблеи ООН от 18 декабря 2013 г. 68/167 «Право на неприкосновенность личной жизни в цифровой век», в которой отмечено, что «сбор личных данных, особенно в массовом масштабе, может иметь негативные последствия для осуществления и реализации прав человека»[221];

— принятую 17 декабря 2018 г. Резолюцию Генеральной Ассамблеи ООН 73/179 «Право на неприкосновенность частной жизни в цифровую эпоху»; в отличие от ранее упомянутой она уже неоднократно обращает внимание на

---

[218] См. подробнее: Васякина Е. В. Роль Всеобщей декларации прав человека в развитии международного права // Труды Оренбургского института (филиала) Московской государственной юридической академии. 2018. № 37. С. 11–14.

[219] Bicskei H. Violations of Human Rights in Digital Environments // Fiat Iustitia. 2020. Vol. 14. Issue 1. P. 43–54.

[220] Замечания общего порядка и общие рекомендации. Замечание общего порядка № 25 о правах детей в связи с цифровой средой. CRC/C/GC/25 [Электронный ресурс] // URL: https://www.refworld.org/ru/policy/concobservations/crc/2021/ru/146359 (дата обращения: 02.03.2024).

[221] Резолюция, принятая Генеральной Ассамблеей 18 декабря 2013 г. по докладу Третьего комитета (A/68/456/Add.2), 68/167 «Право на неприкосновенность личной жизни в цифровой век» [Электронный ресурс] // URL: https://www.un.org/ru (дата обращения: 03.03.2024).

необходимость обеспечения усиленной правовой защиты именно персональных данных в цифровом пространстве[222];

— принятую 22 марта 2024 г. Резолюцию Генеральной Ассамблеи ООН «Использование возможностей безопасных, защищенных и надежных систем ИИ для устойчивого развития»[223], которая стала первым международным актом в сфере искусственного интеллекта, предусматривая, что права человека и основные свободы должны уважаться, защищаться и поощряться на протяжении всего жизненного цикла систем искусственного интеллекта.

Все вышеперечисленные резолюции представляют собой документы общего характера в отношении биометрических данных, так как они не содержат прямых рекомендаций, направленных на регулирование отношений в исследуемой нами области. Однако среди резолюций ООН есть и такие документы, принимаемые в рамках обсуждения вопросов безопасности и противодействию терроризму, которые содержат специальные руководства по использованию биометрии и биометрических данных в контртеррористических целях. К ним относятся резолюции Совета Безопасности ООН 2322 (2016)[224] и 2396 (2017)[225]. В Резолюции 2322 (2016) было впервые отмечено, что Совет Безопасности ООН призывает государства-члены обмениваться биометрическими данными для выявления и идентификации террористов, включая иностранных боевиков-террористов. Резолюция 2396 (2017) Совета Безопасности превратила этот призыв в обязательное требование в соответствии с гл. VII Устава ООН.

В Резолюции 2396 (2017) Совет Безопасности решил, что государства должны разработать и имплементировать системы для сбора биометрических данных, которые могут включать в себя отпечатки пальцев, фотографии, распознавание лиц и другие релевантные идентификационные биометрические

---

[222] Резолюция, принятая Генеральной Ассамблеей 17 декабря 2018 г. по докладу Третьего комитета (A/73/589/Add.2), 73/179 «Право на неприкосновенность частной жизни в цифровую эпоху» [Электронный ресурс] // URL: https://www.un.org/ru (дата обращения: 03.03.2024).

[223] Резолюция «Использование возможностей безопасных, защищенных и надежных систем ИИ для устойчивого развития» [Электронный ресурс] // URL: https://ai.gov.ru/ (дата обращения: 22.03.2024).

[224] Resolution 2322 (2016). Adopted by the Security Council at its 7831st meeting, on 12 December 2016 [Электронный ресурс] // URL: http://unscr.com/en/resolutions/2322 (дата обращения: 22.03.2024).

[225] Resolution 2396 (2017). Adopted by the Security Council at its 8148th meeting, on 21 December 2017 [Электронный ресурс] // URL: http://unscr.com/en/resolutions/doc/2396 (дата обращения: 22.03.2024).

данные с тем, чтобы ответственным и надлежащим образом идентифицировать террористов в соответствии с национальным законодательством и международными правами человека.

В Дополнении к руководящим принципам в отношении иностранных боевиков-террористов[226] даются дополнительные руководства государствам по эффективным мерам реагирования и имплементации, с особым акцентом на новых требованиях, введенных Резолюцией 2396 (2017). Руководство может применяться или использоваться в качестве отсылочной нормы государствами в рамках их усилий на национальном уровне. Руководящий принцип № 38 относится к ответственному использованию и обмену биометрическими данными.

В декабре 2019 г. Совет Безопасности выпустил Техническое руководство Контртеррористического комитета по имплементации Резолюции 1373 (2001)[227] Совета Безопасности и других резолюций, которые также касаются использования биометрии в рамках соответствующих резолюций Совета по борьбе с терроризмом.

В июне 2021 г. по итогам Седьмого обзора Глобальной контртеррористической стратегии ООН (A/RES/60/288[228]) Генеральная Ассамблея ООН вновь подтвердила Стратегию, приняв Резолюцию A/RES/75/291[229]. В соответствии со Стратегией все государства-члены призываются обратить внимание на угрозу роста потока международных рекрутов в ряды террористических организаций, в том числе через выполнение обязательств по использованию биометрических данных при полном уважении прав человека и фундаментальных свобод.

Совет Европы

---

[226] Letter dated 28 December 2018 from the Chair of the Security Council Committee established pursuant to Resolution 1373 (2001) concerning counter-terrorism addressed to the President of the Security Council. S/2018/1177 [Электронный ресурс] // URL: https://documents.un.org/doc/undoc/gen/n19/009/63/pdf/n1900963.pdf (дата обращения: 23.03.2024).

[227] Resolution 1373 (2001). Adopted by the Security Council at its 4385th meeting, on 28 September 2001 [Электронный ресурс] // URL: http://unscr.com/en/resolutions/doc/1373 (дата обращения: 23.03.2024).

[228] Resolution adopted by the General Assembly 60/288. The United Nations Global Counter-Terrorism Strategy [Электронный ресурс] // URL: https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/Terr%20ARES60288.pdf (дата обращения: 23.03.2024).

[229] Resolution adopted by the General Assembly on 30 June 2021. The United Nations Global Counter-Terrorism Strategy: seventh review [Электронный ресурс] // URL: https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/A_RES_75_291_E.pdf (дата обращения: 23.03.2024).

Значимую роль в сфере регулирования использования и защиты биометрических данных играют специальные международные конвенции Совета Европы, регулирующие конкретные вопросы использования персональных данных.

Большое значение для защиты персональных данных имеет рассмотренная ранее Конвенция 108, ставшая, по сути, первым международным договором регионального характера, который обязал участников привести национальное законодательство в соответствие с едиными требованиями для того, чтобы обеспечить надлежащий уровень защиты прав субъектов персональных данных в ходе автоматизированной обработки. Конвенция предусматривала запрет на обработку чувствительной информации, однако на тот момент биометрические данные в перечень чувствительных категорий персональных данных не входили.

Поправки 2018 г.[230] ввели более строгие ограничения для сбора данных и расширили понятие чувствительных данных, включив в них биометрическую информацию. В статье 6 обновленной Конвенции (Конвенция 108+) конфиденциальность информации биометрического характера особо отмечена путем отнесения данных, уникальным образом идентифицирующих физических лиц, к специальным категориям данных. Обработка особых категорий данных, таких как биометрические данные, может быть разрешена только в том случае, если для нее установлена надлежащая правовая база, а в законодательстве государства закреплены дополнительные и надлежащие гарантии.

Таким образом, Конвенция 108 закрепила уже специальные принципы защиты прав субъектов персональных данных в ходе автоматизированной обработки, определила условия такой обработки и предусмотрела гарантии, которые государства-участники должны установить в своем законодательстве.

Среди международных документов, имеющих рекомендательный характер, следует также выделить Руководство по распознаванию лиц[231], принятое 28 января

---

[230] Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108).

[231] Руководство по распознаванию лиц (T-PD (2020) 03rev4) (принято 28 января 2021 г. Консультативным комитетом Конвенции о защите физических лиц при автоматизированной обработке персональных данных

2021 г. Консультативным комитетом Совета Европы по Конвенции 108, в котором отмечается, что интеграция технологий распознавания лиц в существующие системы наблюдения представляет серьезную угрозу для права на конфиденциальность и права на защиту персональных данных, а также для других базовых прав, поскольку использование данных технологий не всегда требует осведомленности или согласия физических лиц, чьи биометрические данные обрабатываются, если рассмотреть, например, возможность получения доступа к цифровым изображениям людей в Интернете. В Руководстве конкретизируются рекомендации по обработке биометрических данных в публичном и частном секторах.

Обработка биометрических данных при осуществлении правоохранительной деятельности должна выполняться только уполномоченными в сфере безопасности органами и только в правоохранительных целях. Для обработки биометрических данных в иных целях иными государственными органами должны быть четко определены конкретные правила.

Обработка биометрических данных частными организациями возможна только при наличии добровольного, четко выраженного, информированного и однозначного согласия субъектов данных (согласно Регламенту о защите данных), чьи биометрические данные подвергаются обработке. Кроме того, использование технологий распознавания лиц может иметь место только в контролируемой обстановке для целей проверки, аутентификации или категоризации.

Руководством также вводятся такие понятия, как «контролируемая»[232] и «неконтролируемая обстановка»[233].

Обработка биометрических данных физических лиц в публичном секторе возможна как в контролируемой, так и в неконтролируемой обстановке, в то время

(Конвенция 108)) // Бюллетень Европейского Суда по правам человека. Российское издание. 2021. № 5 (227). С. 124–133.

[232] Под контролируемой обстановкой понимаются случаи, когда биометрические системы могут использоваться только с участием соответствующего лица.

[233] Под неконтролируемой обстановкой понимаются места, к которым у физических лиц есть свободный доступ, через которые они также могут проходить, в том числе общественные или квазиобщественные пространства, такие как торговые центры, больницы, школы.

как в частном секторе применение технологий распознавания лиц в неконтролируемой обстановке запрещено.

Особо отмечается необходимость принятия мер по повышению осведомленности субъектов данных о технологиях распознавания лиц и последствиях их применения для основных прав (подразд. 4 «Повышение осведомленности» разд. I «Руководство для законодателей и принимающих решения органов»).

Организация экономического сотрудничества и развития (ОЭСР)

Еще одним международным инструментом, имеющим вспомогательное значение для права ЕС, который может быть ориентиром для существующей международной практики в сфере использования биометрических данных, являются рекомендации ОЭСР — международной экономической организации развитых стран, признающих принципы представительной демократии и свободной рыночной экономики. В организацию входят 38 государств, в том числе большинство государств — членов ЕС, для которых акты ОЭСР будут международным «мягким правом», закрепляющим выработанные на практике правила.

Документом общего характера для сферы использования биометрических данных выступают Рекомендации ОЭСР, касающиеся основных положений о защите неприкосновенности частной жизни и международных обменов персональными данными (приняты 23 сентября 1980 г. и пересмотрены в редакции 2013 г.), которые применяются к персональным данным как в государственном, так и в частном секторе.

Отметим разработанную ОЭСР в 2013 г. Концепцию защиты данных[234], в которой в отличие от остальных документов организации содержится упоминание о биометрических данных. В Концепции отмечается обеспокоенность относительно повсеместного использования биометрической информации в

[234] OECD Guidelines governing the protection of privacy and transborder flows of personal data [Электронный ресурс] // URL: https://web-archive.oecd.org/2013-09-06/247725-2013-oecd-privacy-guidelines.pdf (дата обращения: 07.05.2024).

качестве средства идентификации и аутентификации и, как следствие, создания препятствий для реализации прав человека.

Международная организация миграции (МОМ)[235]

МОМ была одной из первых международных организаций, разработавших в 2009 г. собственное внутреннее руководство по защите данных — Принципы защиты данных МОМ[236], а уже в 2010 г. МОМ опубликовала Руководство по защите данных[237]. В Руководстве по защите данных МОМ содержатся рекомендации по осуществлению принципов защиты данных МОМ таким образом, чтобы признать как право отдельных лиц на защиту своих персональных данных, так и необходимость обработки персональных данных МОМ в ходе выполнения миграционного учета. При этом в Руководстве уже фигурирует понятие «биометрические данные», однако на этом всё.

Недавняя публикация МОМ 2023 г. под названием «Introduction to Biometrics», представляющая собой детальный обзор сферы биометрии — от исторического аспекта до практического применения биометрических данных в проездных документах, перечисляет минимальные требования к использованию биометрических данных, основанные на Руководстве по защите данных МОМ и принципах ООН по защите персональных данных и конфиденциальной информации, среди которых законность сбора биометрических данных; согласие всех лиц и/или законных представителей; информирование о необходимости предоставления биометрических данных; *наличие у людей возможности не соглашаться на биометрический процесс и предоставление альтернативного*

---

[235] МОМ была создана 5 декабря 1951 г. в Брюсселе по инициативе правительств западноевропейских государств в целях упорядочения перемещения населения европейских стран после окончания Второй мировой войны. Первоначальное название этой организации — Межправительственный комитет по вопросам европейской миграции (МКЕМ). Универсализация проблемы миграции расширила границы деятельности МКЕМ, в связи с чем в 1987 г. Совет МКЕМ принял решение о переименовании организации в МОМ (URL: https://www.mid.ru/ru/foreign_policy/humanitarian_cooperation/rossia-mezdunarodnoe-gumanitarnoe-sotrudnicestvo/1666104/?TSPD_101_R0=08765fb817ab2000592647b6fb43f2d82a5a5d6fa799f27fb4296ce6405e6958aef635bf2dd9bd4e08af91f4f5143000aa0d205d567a4b522fcf78b8b250ebb369e3819ac116c4a753e606afd761f63b04c7f0c2152509ae1024abf792f83c55 (дата обращения: 13.08.2024)).

[236] International Organization of Migration. IOM Data Protection Principles [Электронный ресурс] // URL: https://www.iom.int/sites/g/files/tmzbdl486/files/documents/2023-08/iom-dp-principles-en.pdf (дата обращения: 13.08.2024).

[237] International Organization of Migration. IOM Data Protection Manual [Электронный ресурс] // URL: https://publications.iom.int/books/iom-data-protection-manual (дата обращения: 13.08.2024).

способа идентификации.

Хотим отметить, что данный документ — один из немногих среди изученных в процессе исследования — предлагает предусмотреть право граждан на отказ от предоставления биометрических данных и возможность использовать другой метод идентификации.

ЮНЕСКО

Относительно новым источником вспомогательного характера, который содержит указание на то, что государствам-членам следует разработать правила и стандарты в отношении данных или эквивалентные рамочные принципы либо провести пересмотр существующих регламентирующих положений, с тем чтобы обеспечить всестороннюю защиту персональных и конфиденциальных данных, которые в случае их разглашения могут причинить людям значительный ущерб, физический вред или страдания, являются Рекомендации об этических аспектах искусственного интеллекта, принятые ЮНЕСКО в ноябре 2021 г.[238]

Как было отмечено в начале параграфа, количество специальных международных документов в области биометрических данных практически сводится к нулю. Среди документов, которые удалось найти, есть Резолюция от 16 сентября 2005 г. по итогам 27-й Конференции комиссаров по защите данных и конфиденциальной информации в Монтрё[239].

Резолюция призывает к тому, чтобы:

— эффективные гарантии были внедрены на ранней стадии для ограничения рисков, присущих природе биометрии;

— соблюдалось строгое разграничение между биометрическими данными, собранными и сохраненными для общественных целей (например, пограничный контроль) на основании юридических обязательств и для договорных целей на

[238] В качестве примера в Рекомендациях приводятся данные о совершении правонарушений, судебных разбирательствах и обвинительных приговорах и связанных с этим мерах пресечения, биометрические и генетические данные, а также данные, касающиеся здоровья, и персональные данные, касающиеся, в частности, расовой принадлежности, цвета кожи, происхождения, гендерной принадлежности, возраста, языка, религии, политических убеждений, национального, этнического, социального происхождения, экономических или социальных условий рождения, инвалидности и любых иных факторов.

[239] Resolution on the use of biometrics in passports, identity cards and travel documents. 27th International Conference of Data Protection and Privacy Commissioners, Montreux, 2005 [Электронный ресурс] // URL: https://www.refworld.org/legal/resolution/icdppc/2005/en/42434 (дата обращения: 13.08.2024).

основании согласия;

— было предусмотрено техническое ограничение использования биометрии в паспортах целями проверки, при сравнении данных в документе с данными, предоставленными владельцем при предъявлении документа.

Вышеперечисленные документы международных организаций выступают актами рекомендательного характера, не имеющими обязательной юридической силы. Акты международных межправительственных организаций, конференций, двусторонние акты государств рассматриваются в работах профессора И. И. Лукашука в контексте роли «мягкого права» в международных отношениях и его влияния на развитие международного права. Например, ученый отмечает, что «мягкое право» может использоваться некоторыми странами как способ изменить положения международных договоров для государства в обход установленных внутренним и международным правом процедур[240]. Однако, как указывает М. Ю. Велижанина, такие недостатки не умаляют полезной роли «мягкого права»[241].

Бесспорно, роль источников «мягкого права» в развитии регулирования любых правоотношений как на международном уровне, так и на уровне интеграционных объединений существенна. Об этом свидетельствует различное понимание в доктрине международного права как универсального[242], так и регионального[243] «мягкого права».

Профессор П. Н. Бирюков в универсальном смысле определяет «мягкое право» как «совокупность правил поведения (как обязывающих, так и необязывающих норм международного права), которые имеют юридические последствия, поскольку ими руководствуются субъекты международных правоотношений». Говоря о ЕС, ученый приходит к выводу, что ввиду того, что статья 288 ДФЕС не указывает «мягкое право» в качестве разновидности

---

[240] Лукашук И. И. Дипломатические переговоры и принимаемые на них акты. М., 2007. С. 90.

[241] Велижанина М. Ю. «Мягкое право»: его сущность и роль в регулировании международных отношений : дис. … канд. юрид. наук. М., 2007.

[242] Hillenberg H. A Fresh Look at Soft Law // European Journal of International Law. 1999. No. 10. P. 499–515 ; Bodenheimer E. Jurisprudence. The Philosophy and Method of Law. Universal Law Publishing Co Ltd., 2005.

[243] Craig P., Burca G. The Evolution of EU Law. Oxford University Press, 2011 ; Senden L. Op. cit. P. 533.

вторичного права ЕС, к «мягкому праву» могут относиться документы институтов ЕС, издаваемые не в формах, предусмотренных статьей 288 ДФЕС, а также документы иных органов и агентств ЕС[244].

Помимо вышеприведенного, в юридической науке существует еще немало подходов к определению источников «мягкого права», а также их роли и соотношения с источниками права ЕС. Объемные труды зарубежных[245] и отечественных[246] ученых посвящены указанному явлению, и это совершенно оправданно.

Д. Шелтон отмечает, что международные институты во всё большей мере принимают различные формы, переходящие от юридически обязательного характера к необязательному — «мягкое» право — и, наоборот, от юридически расплывчатых вариантов к четким, унифицированным, обязательным[247]. При этом термин «мягкое право», как указывают К. Эббот и Д. Снидал, используется для отличия международных рекомендательных актов от юридически обязательных международно-правовых актов, а также от политических договоренностей на уровне государств[248].

Л. Сенден констатирует: дать определение актам «мягкого права» достаточно сложно, вместе с тем предлагает собирательное определение, которое является, на наш взгляд, нейтральным и в то же время базисным: «Правила поведения, изложенные в документах, которым не придана юридически обязательная сила как таковая, но которые тем не менее могут иметь определенные (косвенные) юридические последствия и которые направлены на достижение практического эффекта и могут его вызвать»[249].

---

[244] Бирюков П. Н. О «мягком праве» ЕС // Актуальные проблемы современного международного права : материалы XIV Международного конгресса «Блищенковские чтения» : в 2 ч. Москва, 16 апреля 2016 г. Ч. I. М. : Российский университет дружбы народов (РУДН), 2016. С. 386.

[245] См., например: Senden L., Morth U., Di Robilant A.

[246] Такие ученые, как, например, Ю. Безбородов, М. Буроменский, В. Василенко, М. Велижанина, Г. Вельяминов, В. Денисов, В. Евинтов, А. Задорожный, И. Лукашук, В. Мицик, В. Муравьев, Н. Нешатаева, Г. Тункин, Х. Хиллингенберг, К. Чинкин, посвящали отдельные научные труды «мягкому праву».

[247] Shelton D. Normative Hierarchy in International Law // American Journal of International Law. 2006. April. Vol. 100. No. 2. P. 292.

[248] Abbott K. W., Snidal D. Hard and Soft Law in International Governance // International Organization. 2000. Vol. 54.

[249] Senden L. Soft Law In European Community Law. Vol. 1 2004.P. 112.

Вопрос об эффективности актов «мягкого права» также является актуальным. Как правило он рассматривается в рамках выдвижения различных утверждений относительно противопоставления «мягкого права» и «твердого права». Отметим, что обе категории являются совокупностью социальных норм, которая выступает результатом деятельности субъектов международного права. В своей работе А. ди Робилант[250] иллюстрирует такое противостояние именно через призму социальной интеграции. Так раскрывается утверждение сторонников «мягкого права» о том, что социальная интеграция лучше всего осуществляется через многоуровневые децентрализованные процессы, приводящие к разработке открытых и гибких руководящих принципов и стандартов. Здесь же приводится мнение, что «“мягкое право” способствует более активному и плюралистическому обсуждению, поощряет культурное и политическое разнообразие, стимулирует производство знаний и, наконец, является более эффективным, чем принято считать. “Мягкие” правовые инструменты стимулируют динамичное взаимодействие нескольких уровней власти, а также участие различных социальных субъектов».

Напротив, последователи концепции «твердого права» настаивают на том, что социальная политика должна осуществляться в рамках централизованного, вертикального и формального процесса принятия решений, в результате которого вырабатываются единые и обязательные правила, создающие права и подлежащие защите в судебном порядке.

В разрезе нашего исследования невозможно не согласиться частично со сторонниками первой концепции. В современном мире, где технологии развиваются с невероятной скоростью, вопросы конфиденциальности и защиты персональных данных встают особенно остро. Биометрические технологии, основанные на использовании уникальных физиологических или поведенческих характеристик человека, становятся всё более распространенными, но одновременно вызывают опасения по поводу конфиденциальности данных и

[250] Robilant A. di. Genealogies of Soft Law // The American Journal of Comparative Law. 2006. Vol. 54. No. 3.

потенциального риска нарушения прав человека. Поэтому по скорости реагирования на меняющиеся общественные отношения на первый план выходят именно акты «мягкого права» в разнообразных формах.

Вместе с тем нормы «мягкого права» не могут быть полноценными регуляторами правоотношений, так как они не обладают обязательной юридической силой, ни полной, ни частичной[251], в отличие от норм «твердого права». Это, в свою очередь, ставит вопрос о невозможности правопринуждения в «мягком праве» и замене его альтернативными механизмами добровольного исполнения и совместного мониторинга[252].

Безусловно, процедуры принятия законодательных актов, предусмотренные статьей 289 ДФЕС (обычная законодательная процедура и специальная законодательная процедура), занимают значительное количество времени, и, возможно, ввиду этого, законодательство ЕС не всегда способно оперативно реагировать на новые вызовы и угрозы, которые возникают в связи с внедрением цифровых технологий в жизнь человека, тем самым допуская риск нарушения основных прав.

Одновременно с этим проблема охраны биометрических данных требует строгого нормативного регулирования, обязывающего всех участников правоотношений соблюдать четко сформулированные правила поведения, в связи с чем мы можем сделать вывод о том, что рекомендательные акты, к сожалению, не закрывают данную задачу.

Впрочем, существенные характеризующие «мягкое право» черты, перечень которых предлагает П. А. Калиниченко[253], определяют его другие важные задачи (функции), которые являются также значимыми в формировании правового регулирования использования биометрических данных. Эти функции главным

---

[251] Бекяшев К. А., Сапронов В. Д. Мировое рыболовство: вопросы международного сотрудничества М., 1990. С. 235.

[252] Калиниченко П. А. Правовые основы регулирования отношений между Россией и Европейским Союзом : учебное пособие. М. : Университет имени О.Е. Кутафина, 2019. С. 69.

[253] Калиниченко П. А. Правовое регулирование отношений между Россией и Европейским Союзом.

образом определяют роль и значение «мягкого права» в правотворческом процессе. Среди них:

— функция «пред-права», т.е. преобразование «мягкого права» непосредственно в правовые нормы[254];

— функция «пост-права», означающая интерпретацию и дополнение норм «твердого права», а также предусматривающая восполнение пробелов регулирования и играющая важную роль в урегулировании споров между сторонами;

— функция «пара-права», т.е. нормы «мягкого права» способны фиксировать согласие сторон по определенному вопросу без принятия обязательств.

Таким образом, «мягкое право» может выступать своего рода вспомогательным механизмом и «помощником» «твердого права», несмотря на опасения некоторых ученых[255] относительно путаницы в восприятии и применении норм «мягкого» и «твердого права». Вместе с тем следует согласиться с мнением П. А. Калиниченко, что «мягкое право» не должно быть альтернативой правового регулирования на практике ввиду необходимости создания мощной правовой машины, которая в нашем случае будет реализовывать главную потребность — надежную правовую охрану биометрических данных. Именно «мягкое право» обеспечивает механизм формирования жестких норм, зачастую выступает предтечей обязательных норм и стандартов[256].

В заключение согласимся с П. Н. Бирюковым, что термин «мягкое право» вводит в заблуждение. Однако значимость «мягкого права» в правовом регулировании ЕС постоянно растет, и на сегодняшний день оно составляет около 10% всего законодательства Союза[257]. Оно оказывает серьезное влияние на весь правопорядок и правовые системы государств-членов. Учитывая данный факт,

---

[255] Колодкин Р. Л. Критика концепции «мягкого права» // Советское государство и право. 1985. № 12. С. 95–99.

[256] Калиниченко П. А., Некотенева М. В. Особенности правового регулирования геномных исследований на международном и европейском уровне // Вестник Университета имени О.Е. Кутафина (МГЮА). 2020. № 4. С. 71.

[257] Скурко Е. В. «Мягкое право» Европейского Союза: некоторые вопросы его применения // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Серия 4 «Государство и право»: Реферативный журнал. 2021. № 4.

хотелось бы наблюдать в практике институтов ЕС большее количество документов, предусматривающих предложения по обращению с биометрическими данными в различных сферах или комплексный подход к правовому регулирования их использования.

Анализ рассмотренных в параграфе международных документов также подтверждает вывод о сегментарности регулирования использования биометрических данных. На международном уровне сегодня нет специального источника, который бы содержал правовое регулирование конкретно данной сферы. Несмотря на особый характер биометрических данных, в мире практически не существует универсальных положений, которые бы не устанавливали режим использования биометрических данных фрагментарно, а учитывали бы и основные принципы защиты прав человека, и технические требования к системам обработки биометрических данных, и новые вызовы научно-технического прогресса. Обеспечить защиту биометрических данных от посягательств по всему миру, регулировать стандарты трансграничного обмена информацией и технические требования к сбору и хранению биометрических данных национальное право не может. Это приводит к необходимости создания единой международной системы защиты персональных данных — универсальной конвенции об использовании биометрических данных.

В контексте международной информационной безопасности наша позиция находит поддержку в исследовании Н. А. Молчанова и Е. К. Матевосовой, которые связывают проблему обеспечения международной информационной безопасности с рядом нерешенных вопросов, затрудняющих формирование ее системы, в числе которых состояние правовой регламентации информационной безопасности на международном уровне, а также отсутствие механизмов и процедур применения соответствующих нормативных требований[258].

[258] Молчанов Н. А., Матевосова Е. К. Доктрина информационной безопасности Российской Федерации (новелла законодательства) // Актуальные проблемы российского права. 2017. № 2 (75). С. 163.

ГЛАВА 3. СОВРЕМЕННЫЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ПРАВОВОЙ ОХРАНЫ БИОМЕТРИЧЕСКИХ ДАННЫХ: ОПЫТ ЕВРОПЕЙСКОГО СОЮЗА

§ 3.1. Использование биометрических данных в целях обеспечения частной, общественной и государственной безопасности в Европейском Союзе

С развитием технологий и внедрением цифровизации во все сферы жизни человека биометрические данные становятся все более востребованным инструментом в обеспечении безопасности как на индивидуальном, так и на общественном, государственном, региональном и даже мировом уровнях. Они используются во всех сферах повседневной жизни граждан по всему миру, в том числе граждан ЕС, включая сферы предоставления банковских услуг и обеспечения безопасности в домах и офисах. Например, системы умного дома все чаще оснащаются устройствами, использующими биометрические данные для доступа, такими как сканеры отпечатков пальцев или датчики распознавания лиц, а подтвердить свою личность при проведении необходимой банковской операции можно при помощи голоса, изображения лица или отпечатка пальца.

Биометрические данные находят широкое применение в сфере транспорта и логистики. Например, биометрические системы используются для доступа к транспортным средствам, таким как автомобили и грузовики, что позволяет управляющим компаниям контролировать доступ к транспортным ресурсам и обеспечивать безопасность грузов и пассажиров. Кроме того, воздушные и железнодорожные компании все чаще внедряют биометрические системы для идентификации пассажиров на этапах регистрации и посадки, что упрощает процедуры безопасности и сокращает время ожидания.

Исторически биометрические данные наиболее интенсивно применяются в сфере пограничного контроля и сфере борьбы с терроризмом/преступностью. Обе

имеют целью предупреждение случаев фальсификации удостоверяющих личность документов, а также обеспечение безопасности на границах (в аэропортах, на вокзалах) и в местах массового скопления людей.

Правовое регулирование биометрических данных сфокусировано на балансе между сферой безопасности и сферой защиты прав и свобод человека. Однако вместе с потенциалом повышения уровня безопасности повышаются риски, связанные с соблюдением приватности и защитой личных данных, и, наоборот, там, где закон встает на сторону граждан и защиты их уникальных личных данных, могут ослабевать механизмы обеспечения безопасности на более глобальном уровне.

Основу правового регулирования биометрических данных в области безопасности в ЕС, по нашему мнению, образуют сферы ведения, регламентированные учредительными договорами Союза:

1) сфера ОВПБ (гл. 2 разд. V ДЕС);

2) сферы в рамках создания ЕС пространства свободы, безопасности и правосудия (разд. V ДФЕС), среди которых:

— политика в отношении пограничного контроля, предоставления убежища и иммиграции (гл. 2 разд. V ДФЕС);

— судебное сотрудничество по гражданским делам (гл. 3 разд. V ДФЕС);

— судебное сотрудничество по уголовным делам (гл. 4 разд. V ДФЕС);

— полицейское сотрудничество (гл. 5 разд. V ДФЕС).

Сфере ОВПБ, а именно специальным положениям, посвящена глава 2 разд. V ДЕС. Цели общей внешнеполитической деятельности ЕС сформулированы в гл. 1 этого же раздела, среди них одновременно перечислены поддержка прав человека и принципов международного права, а также укрепление международной безопасности в соответствии с целями и принципами Устава ООН, принципами Хельсинкского Заключительного акта и целями Парижской хартии, что подчеркивает равную значимость вопросов безопасности и прав человека для Союза.

Для ОВПБ характерен акцент на традиционных межправительственных

формах сотрудничества государств-членов, стремящихся выработать общий подход на основе единогласия и со слабым привлечением наднациональных элементов.

Координация позиций государств-членов в вопросах ОВПБ осуществляется в международных организациях и на международных конференциях на основе позиции Союза (ст. 34 ДЕС). В сфере ОВПБ Союз уполномочен заключать международные соглашения с третьими странами и международными организациями в соответствии со ст. 37 ДЕС.

В ДЕС предусмотрен также комплекс односторонних мер ЕС в области ОВПБ. Вместе с тем инструментарий Союза в данной сфере ограничен, так как принятие законодательных актов по вопросам ОВПБ исключается в силу п. 1 ст. 31 ДЕС. В рамках ОВПБ возможны только меры незаконодательного характера, которые также относятся к актам «мягкого права», что значительно снижает юридическое значение односторонних действий Союза в данной области деятельности и констатирует проблему, изложенную в гл. II настоящего исследования.

Кроме этого, в соответствии со ст. 39 ДЕС Совет уполномочен принимать решение об установлении правила о защите физических лиц в отношении обработки персональных данных государствами-членами при осуществлении деятельности, которая входит в сферу применения ОВПБ, и о свободном перемещении таких данных.

Таким образом, нормативную базу регулирования биометрических данных в сфере ОВПБ будут составлять нормы «мягкого права» и в незначительной мере международные соглашения ЕС, рассмотренные в гл. II диссертационного исследования.

Пространство свободы, безопасности и правосудия является сферой совместной компетенции ЕС и государств-членов в соответствии с п. 2 ст. 4 ДФЕС.

Основной блок правового регулирования в этой области чаще всего составляют акты ЕС о создании и функционировании специализированных систем обмена и хранения данных между судебными и правоохранительными органами, в частности биометрических данных.

Так называемые Прюмские достижения представляют собой комплекс правовых решений, являющихся одним из главных правовых инструментов такого регулирования в рамках реализации судебного сотрудничества по уголовным делам и полицейского сотрудничества, охватываемого главами 4 и 5 разд. V ДФЕС.

Прюмская конвенция, как было указано ранее, была подписана в 2005 г. в немецком городе Прюм и первоначально предусматривала[259]:

— создание системы автоматизированного поиска криминалистической информации (геномной и дактилоскопической из национальных баз данных всех государств-членов, а также из баз данных регистрационных номеров транспортных средств);

— обеспечение процесса обмена информацией в целях предупреждения преступлений, особенно при проведении крупномасштабных мероприятий против трансграничной организованной преступности и терроризма;

— полицейское сотрудничество;

— защиту информации.

Основные аспекты Прюмской конвенции были официально включены в правовую базу ЕС 23 июня 2008 г. в соответствии с решениями 2008/615/JHA[260] и 2008/616/ JHA[261].

Впрочем, отдельного внимания в рамках нашего исследования заслуживает последний Регламент (ЕС) 2024/982 об автоматизированном поиске и обмене данными в целях обеспечения полицейского сотрудничества («Прюм II»), принятый Советом 26 февраля 2024 г.[262], который внес изменения в упомянутые решения, а также в Регламент (ЕС) 2018/1726 об Агентстве Европейского Союза по оперативному управлению крупномасштабными IT-системами в области свободы,

---

[259] Никитина И. Э., Нетрусова Т. И., Никитина А. Ю. Указ. соч.

[260] Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime // OJ. 6.8.2008. L 210. P. 1–11.

[261] Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime.

[262] Regulation (EU) 2024/982 of the European Parliament and of the Council of 13 March 2024 on the automated search and exchange of data for police cooperation, and amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, (EU) No 2019/817 and (EU) 2019/818 of the European Parliament and of the Council (the Prüm II Regulation) // OJ. 5.4.2024. L 2024/982.

безопасности и правосудия (eu-LISA)[263], Регламент (ЕС) 2019/817 об основах взаимодействия информационных систем Европейского Союза в сфере пограничного контроля и визового режима (Регламент 2019/817)[264] и Регламент (ЕС) 2019/818 об основах взаимодействия информационных систем Европейского Союза в области сотрудничества полиции и судебных органов, предоставления убежища и миграции (Регламент 2019/818)[265].

Статья 4 «Прюм II» под биометрическими данными понимает профили ДНК, отпечатки пальцев и изображение лица.

Пункт 17 Преамбулы подчеркивает, что автоматизированный поиск биометрических данных ответственными компетентными органами государств-членов должен касаться только данных, содержащихся в базах данных, созданных для предотвращения, выявления и расследования уголовных преступлений.

«Прюм II» выделяет в качестве одной из основных целей установление правил, касающихся обмена основными данными после подтверждения совпадения биометрических данных, наряду с установлением условий и процедуры автоматизированного поиска профилей ДНК, дактилоскопических данных, определенных регистрационных данных транспортных средств, изображений лиц и полицейских записей (ст. 1).

Статья 37 Регламента содержит требования к процессу обмена и передачи биометрических данных между базами данных государств-членов и Европола, а также закрепляет обязанность Комиссии принять имплементационные акты, регламентирующие техническую процедуру запроса данных и определяющие формат и технические правила сравнения и ранжирования соответствия между биометрическими данными.

---

[263] Regulation (EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and amending Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) No. 1077/2011 // OJ. 21.11.2018. L 295. P. 99–137.

[264] Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA // OJ. 22.5.2019. L 135. P. 27–84.

[265] Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816 // OJ. 22.5.2019. L 135.

В статье 47 сведения о месте и дате получения биометрических данных и сведения об уголовном преступлении, в связи с которым такие данные были получены, относятся к основным данным, которые должны быть известны при подтверждении совпадения данных с идентифицированным лицом или с данными неизвестного (неопознанного) лица.

Отдельная глава 5 «Прюм II» посвящена Европолу, а именно правилам доступа государств-членов к биометрическим данным, предоставляемым третьими странами и хранящимся в базе Европола, и, наоборот, правилам доступа Европола к биометрическим данным, хранящимся в базах данных государств-членов, в том числе данным, полученным от третьих стран (ст. 48 и 49).

Цели, задачи и основы деятельности Европола определены Регламентом Европейского парламента и Совета от 11 мая 2016 г. 2016/794 об Агентстве Европейского Союза по сотрудничеству правоохранительных органов (Европол)[266]. Европол, согласно ст. 3 Регламента, поддерживает и укрепляет действия компетентных органов государств-членов и их взаимное сотрудничество по вопросам предотвращения серьезных преступлений, затрагивающих два или более государства-члена, терроризма и форм преступности, которые касаются общих интересов, охватываемых политикой Союза, и борьбе с ними. Одними из задач, способствующих реализации указанной цели, являются сбор, хранение, обработка, анализ информации и обмен ею (ст. 4 Регламента).

В Регламенте от 11 мая 2016 г. 2016/794 ни разу прямо не упоминается о биометрических данных. Вместе с тем в Преамбуле Регламента подчеркивается, что при осуществлении своей деятельности Европолу следует особенно обращать внимание на разграничение категорий персональных данных. Европол должен обрабатывать специальные категории персональных данных только в том случае, если эти данные дополняют другие персональные данные, которые уже обрабатываются Европолом. В целях беспрепятственной реализации

[266] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA // OJ. 24.5.2016. L 135. P. 53–114.

основополагающего права на защиту таких персональных данных Европол не должен хранить персональные данные дольше, чем это необходимо для выполнения его задач. Статья 30 Регламента содержит правила обработки Европолом особых категорий персональных данных и различных категорий субъектов данных. При этом отметим, что пункт 2 ст. 30, устанавливающий запрет на обработку персональных данных, за исключением случаев, когда это строго необходимо и соразмерно для предотвращения или борьбы с преступлением, подпадающими под задачи Европола, перечисляет все специальные категории персональных данных кроме биометрических данных.

«Прюм II» в каком-то смысле восполняет этот пробел и отдельно акцентирует внимание на использовании Европолом биометрических данных при взаимодействии с государствами-членами.

В пункте 41 Преамбулы даже подчеркивается необходимость учета государствами-членами и Европолом при внедрении «Прюм II» прецедентной практики Суда ЕС по вопросам, касающимся использования биометрических данных.

«Прюм» в своих определениях так же, как и остальные акты ЕС, прошел путь от «дактилоскопии до биометрии» и сейчас затрагивает сферы, в которых организация условий безопасности стала практически невозможна без использования биометрических данных в соответствующих информационных системах. Однако наряду с этим в научном обществе отмечается обеспокоенность относительно усиления надзора и возвышения ЕС как полицейского государства, перераспределения власти от уголовных следователей к криминалистической технократии, легитимности режима «Прюм», вопросов защиты данных, несовместимости систем, технических проблем внедрения, подключения и обмена данными ДНК[267].

Упоминая другие сферы, вспомним, что «Прюм II» внес изменения в акты ЕС об основах взаимодействия информационных систем в сферах пограничного

[267] Дьяков В. Г., Ткачук В. В. Правовое обеспечение геномной безопасности в Европейском Союзе // Международный правовой курьер. 2020. № 3–4 (39–40). С. 52.

контроля/визового режима и предоставления убежища/иммиграции. Это свидетельствует о том, что правовое регулирование биометрических данных в области безопасности основывается на взаимодополнении различных информационных систем и баз данных, которые создаются и используются в разных областях, но цель такого использования единая — реализация эффективного сотрудничества компетентных органов в рамках борьбы с преступностью, которое может выражаться как в полицейском/судебном сотрудничестве по гражданским и уголовным делам, так и в процедуре прохождения паспортного контроля на границе.

Актуализированный *Регламент 2019/817*, назначением которого является установление правил взаимодействия информационных систем в сфере пограничного контроля и визового режима, значительное внимание уделяет месту биометрических данных и условиям их обработки, равно как и Регламент 2019/818 о взаимодействии информационных систем в области сотрудничества полиции и судебных органов, предоставления убежища и миграции.

Цель организации такого взаимодействия обусловлена следующими задачами (п. 9 Преамбулы Регламента 2019/817):

— повышение эффективности и результативности проверок на внешних границах;

— содействие предотвращению нелегальной иммиграции и борьбе с ней;

— содействие обеспечению высокого уровня безопасности в сфере свободы, неприкосновенности и правосудия Союза, включая поддержание общественной безопасности и государственной политики в ЕС, и на территориях государств-членов;

— совершенствование общей визовой политики, оказание помощи в рассмотрении ходатайств о международной защите;

— содействие предотвращению, выявлению и расследованию террористических преступлений и других серьезных уголовных правонарушений;

— содействие установлению личности неизвестных лиц, которые не могут идентифицировать себя, или неопознанных человеческих останков в случае

стихийного бедствия, несчастного случая или террористического акта;

— поддержание общественного доверия к системе миграции и предоставления убежища Союза.

Согласно Преамбуле Регламента 2019/817 и ст. 1 Регламента 2019/818 указанные акты составляет правовую основу взаимодействия таких информационных систем, как:

— Централизованная информационная система регистрации въезда и выезда (Entry-Exit System, EES)[268];

— VIS[269], куда включаются биометрические данные (отпечатки пальцев и фотография) иностранцев, обратившихся за выдачей визы;

— Европейская система информации о путешествиях и авторизации (European Travel Information and Authorisation System, ETIAS)[270];

— Евродак[271];

— SIS[272];

— Централизованная система государств-членов, обладающих сведениями о судимости граждан третьих стран и лиц без гражданства (Centralised System for the Identification of Member States Holding Conviction Information on Third-Country Nationals and Stateless Persons, ECRIS-TCN)[273].

Вспомогательными инструментами такого взаимодействия выступают

---

[268] Regulation (EU) No. 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No. 767/2008 and (EU) No. 1077/2011 // OJ. 9.12.2017. L 327. P. 20–82.

[269] Regulation (EC) No. 767/2008 of the European Parliament and of the council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation) // OJ. 13.8.2008. L 218. P. 0060–0081.

[270] Proposal for a Regulation of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No. 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624. Brussels, 16.11.2016 COM(2016) 731 final 2016/0357(COD).

[271] Council Regulation (EC) No. 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention // OJ. 15.12.2000. L 316. P. 1–10.

[272] The Schengen acquis — Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders // OJ. 22.9.2000. L 239. P. 0019–0062.

[273] Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726 // OJ. 22.5.2019. L 135. P. 1–26.

специально созданные Европейский поисковый портал (European Search Portal, ESP), Общая система сопоставления биометрических данных (Shared Biometric Matching Service, BMS), Общее хранилище идентификационных данных (Common Identity Repository, CIR) и Система многократной идентификации (Multiple-Identity Detector, MID) (ст. 1 Регламента 2019/817 и ст. 1 Регламента 2019/817).

Биометрические данные подлежат обработке всеми перечисленными информационными и поисковыми системами, в связи с чем Регламент 2019/817 особенно отмечает характер таких данных и особые условия их обработки в этих системах.

В Регламенте подчеркивается, что биометрические данные (к ним Регламент относит в рамках закрытого перечня только отпечатки пальцев и изображение лица) являются уникальными и, следовательно, гораздо более надежными для идентификации человека, чем буквенно-цифровые данные. При этом биометрические данные представляют собой конфиденциальные персональные данные, ввиду чего упомянутый Регламент должен определять основу и меры предосторожности для обработки таких данных с целью однозначной идентификации соответствующих лиц.

Предлагаем рассмотреть информационные системы, в которых биометрические данные наиболее часто подвергаются обработке и соответственно в отношении которых установлены более объемные и четкие правила обращения с биометрической информацией.

Общая система сопоставления биометрических данных (Biometric Matching Service)

Оба регламента содержат зеркальные нормы, касающиеся функционирования информационных систем, в частности BMS, которой отведена глава 3 регламентов, устанавливающая правила хранения, поиска, сопоставления биометрических данных и биометрических шаблонов.

BMS, согласно положениям регламентов, должна представлять собой технический инструмент для оптимизации работы соответствующих информационных систем ЕС и других компонентов взаимодействия. Основной

целью BMS должно быть упрощение процесса идентификации физического лица, зарегистрированного в нескольких базах данных, путем использования единого технологического компонента для сопоставления биометрических данных этого лица в различных системах вместо нескольких компонентов.

В соответствии со ст. 12 регламентов BMS является хранилищем биометрических данных, полученных из CIR и SIS, позволяющим запрашивать биометрические данные сразу в нескольких информационных системах ЕС в целях поддержки взаимодействия CIR и MID и задач EES, VIS, Евродак, SIS и ECRIS-TCN. Срок хранения биометрических данных в BMS ограничивается сроком хранения в CIR или SIS (ст. 15 регламентов).

Согласно п. 3 ст. 12 регламентов на eu-LISA возложены обязанности по разработке BMS и обеспечению ее технического управления.

Биометрические шаблоны, хранящиеся в общей BMS, должны состоять из данных, полученных в результате извлечения признаков из реальных биометрических образцов и добытых таким образом, чтобы процесс извлечения в обратном порядке был невозможен. Биометрические шаблоны должны быть получены на основе биометрических данных, при этом должна быть исключена возможность получить те же самые биометрические данные из биометрических шаблонов.

В соответствии со ст. 18 на eu-LISA возложена обязанность по ведению журналов всех операций по обработке данных, проводимых в BMS. Такие журналы должны содержать информацию:

— о государстве — члене ЕС или агентстве Союза, отправляющем запрос;

— об истории создания и хранения биометрических шаблонов;

— о том, какие информационные системы ЕС запрашивали биометрические шаблоны, хранящиеся в BMS;

— о дате и времени запроса;

— о типе биометрических данных, используемых для запуска запроса;

— о результатах запроса, а также дате и времени получения результата.

В отношении обработки данных в BMS уполномоченные органы государства-

члена, которые являются контролерами для Евродак, SIS и ECRIS-TCN соответственно, выступают контролерами данных в соответствии с Регламентом о защите данных в отношении биометрических шаблонов, которые они вводят в базовые системы, и несут ответственность за обработку таких биометрических шаблонов в BMS (п. 1 ст. 40 гл. VII «Защита данных»).

Централизованная информационная система регистрации въезда и выезда (Entry-Exit System)

В соответствии с п. 20 Преамбулы Регламента о создании системы EES[274] биометрические данные в EES обрабатываются в первую очередь в целях обеспечения управления внешними границами, предотвращения нелегальной миграции и способствования управлению миграционными потоками, а также содействия предотвращению, выявлению и расследованию террористических и других серьезных уголовных преступлений.

В Регламенте отмечается влияние использования биометрических данных на реализацию права на неприкосновенность частной жизни пересекающих границу лиц, но одновременно с этим такое использование признается обоснованным: во-первых, ввиду того, что биометрические средства идентификации являются надежным методом распознавания граждан третьих стран, находящихся на территории государств-членов, но не имеющих проездных документов или каких-либо других документов, позволяющих установить личность, что особенно распространено среди нелегальных мигрантов; во-вторых, по той причине, что биометрические данные позволяют более точно сопоставлять данные о въезде и выезде добросовестных путешествующих. Использование изображений лица в сочетании с данными отпечатков пальцев позволяет сократить общее количество отпечатков пальцев, необходимых для регистрации, при этом обеспечивая тот же результат с точки зрения точности идентификации.

[274] Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011 // OJ. 9.12.2017. L 327. P. 20–82.

Отпечатки пальцев граждан третьих стран, не имеющих визу, регистрируются в EES (если это физически возможно) в целях обеспечения точной проверки и идентификации, чтобы убедиться, что гражданин третьей страны уже не зарегистрирован под другим именем или с другим проездным документом, а также чтобы гарантировать наличие достаточного количества данных для обеспечения достижения целей EES при любых обстоятельствах (п. 21 Преамбулы).

Отпечатки пальцев граждан третьих стран, имеющих визу, должны быть сверены с данными VIS. Изображение лица как граждан третьих стран, имеющих визу, так и граждан без визы должно быть зарегистрировано в EES. Отпечатки пальцев или изображение лица должны использоваться в качестве биометрического идентификатора для установления личности граждан третьих стран, которые ранее были зарегистрированы в EES, до тех пор, пока файлы с их данными не будут удалены.

Национальные власти обязаны использовать отпечатки пальцев и изображение лица в качестве основных биометрических идентификаторов для проведения требуемой проверки на границах с учетом особенностей каждого пограничного пункта и видов границ.

Пунктом 5 ст. 4 установлено, что государство-член, не применяющее Шенгенское законодательство в полном объеме, но при этом использующее EES, может применять систему без использования биометрических данных на своих внутренних сухопутных границах с государством-членом, которое еще не применяет Шенгенское законодательство в полном объеме, но также использует EES. Если на таких внутренних границах гражданин третьей страны еще не зарегистрирован в EES, личное дело этого гражданина третьей страны создается без сбора биометрических данных. Биометрические данные добавляются в следующем пункте пересечения границы, где EES доступна с использованием биометрических данных.

Каждый уполномоченный на то орган должен обеспечить сбор биометрических данных и их использование в EES с учетом соблюдения гарантий, изложенных в ЕКПЧ, Хартии ЕС об основных правах и Конвенции ООН о правах

ребенка. В частности, при сборе данных о ребенке в первую очередь учитываются его наилучшие интересы (п. 2 ст. 10).

Важным является положение об отказе гражданину третьей страны во въезде в случае его отказа от предоставления биометрических данных для регистрации, сверки или проведения идентификации посредством EES, о чем гражданин третьей страны должен быть проинформирован в соответствии со ст. 50 Регламента.

Централизованная система государств-членов, обладающих сведениями о судимости граждан третьих стран и лиц без гражданства (ECRIS-TCN)

Новейшей централизованной информационной системой в ЕС является ECRIS-TCN, которая предназначена для хранения информации о гражданах третьих стран, включая лиц с двойным гражданством (лиц, имеющих гражданство государства — члена ЕС и третьей страны), которые имеют судимость за уголовные преступления в одном или нескольких государствах — членах ЕС[275]. Согласно Регламенту, учреждающему ECRIS-TCN, главная цель системы заключается в определении страны, где хранится информация о судимости, относящаяся к конкретному гражданину третьей страны.

ECRIS-TCN является аналогом уже существующей Информационной системы европейской уголовной регистрации (European Criminal Records Information System, ECRIS), правовую основу функционирования которой составляют Рамочное решение Совета 2009/315/JHA[276], а также Рамочное решение Совета 2009/316/JHA[277].

ECRIS — это децентрализованный механизм обмена информацией, способствующий сотрудничеству судебных органов по уголовным делам. ECRIS-TCN служит ее альтернативой в случаях, когда государствам — членам ЕС требуется информация о предыдущих судимостях в отношении граждан третьих стран, и укажет государства-члены, которые обладают такой информацией.

---

[275] Vavoula N. The Establishment of ECRIS-TCN (Chapter 7) // Immigration and Privacy in the Law of the European Union. Leiden, The Netherlands: Brill, 2022. P. 540–598.

[276] Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States // OJ. 7.4.2009. L 93. P. 23.

[277] Council Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA // OJ. 7.4.2009. L 93. P. 33.

Подробная информация об этой судимости затем будет получена через запрос ECRIS.

В интересующем нас ключе отметим, что в соответствии с актами ЕС о создании и функционировании ECRIS обмену между государствами — членами ЕС в этой системе подлежит информация об обвинительных приговорах. О хранении и обмене биометрическими или дактилоскопическими данными не упоминается.

Усовершенствованная система ECRIS-TCN, напротив, предусматривает обмен биометрическими данными граждан третьих стран, в частности информацией об изображениях лица.

В пункте 24 Преамбулы Регламента 2019/816 подчеркивается, что изображения лица, содержащиеся в ECRIS-TCN, должны использоваться исключительно для подтверждения личности гражданина третьей страны с целью определения государств-членов, располагающих информацией о предыдущих судимостях этого гражданина третьей страны. При этом отмечается необходимость предусмотреть возможность использования изображений лица для автоматизированного биометрического сопоставления, при условии, что технические и политические требования для этого будут выполнены.

Биометрия, согласно п. 25 Преамбулы, признана самым надежным методом идентификации граждан третьих стран на территории государств-членов, которые зачастую не имеют документов или других средств идентификации.

Подпунктом 1 п. 1 ст. 10 Регламента предусмотрены разработка и принятие исполнительных актов, необходимых для технической разработки и внедрения ECRIS-TCN, и, в частности, актов, устанавливающих минимальные спецификации и требования к биометрическим характеристикам в ECRIS-TCN, в том числе в отношении требуемого коэффициента ложноположительной идентификации и коэффициента ложноотрицательной идентификации.

В отчет Комиссии об оценке реализации работы в ECRIS-TCN, который подготавливается каждые четыре года, включается аналитическая информация о том, сохраняется ли целесообразность использования биометрических данных для целей, преследуемых системой, о безопасности системы и о любых последствиях

для безопасности будущих операций (п. 9 ст. 36 Регламента).

Особенно хотелось бы отметить, что в ст. 1 последней редакции Регламента[278] условия, при которых ECRIS-TCN способствует содействию в корректной идентификации лиц, зарегистрированных в системе посредством хранения идентификационных данных, данных проездных документов и биометрических данных в Общем хранилище данных (Common Identity Repository, CIR[279]), выступают качественно новым и одним из основных вопросов регулирования Регламента.

Централизованная система регистрации дактилоскопических данных (Евродак)

Система Евродак была создана в соответствии с Регламентом Совета 2725/2000[280] (утратил силу) для эффективного применения Конвенции, определяющей государство-член, ответственное за рассмотрение ходатайств о предоставлении убежища, поданных в одном из государств — членов Европейского сообщества, 1990 г., именуемой «Дублин I» или «Дублинская конвенция»[281].

Система изначально предназначена для сравнения данных отпечатков пальцев иностранных граждан и лиц без гражданства, подавших ходатайства о предоставлении в ЕС убежища или въехавших в ЕС нелегально, однако со временем область применения Евродак расширилась.

В первой редакции Регламента о создании Евродак не содержалось упоминания о биометрических данных и применении биометрических систем идентификации. Вместе с тем в Регламенте 2725/2000 подчеркивалось, что отпечатки пальцев являются важным элементом в точном установлении личности

---

[278] Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816 // OJ. 22.5.2019. L 135. P. 85–135 ; Regulation (EU) 2021/1151 of the European Parliament and of the Council of 7 July 2021 amending Regulations (EU) 2019/816 and (EU) 2019/818 as regards the establishment of the conditions for accessing other EU information systems for the purposes of the European Travel Information and Authorisation System // OJ. 14.7.2021. L 249. P. 7–14.

[279] Dimitrova D. Connecting the dots in the Area of Freedom, Security and Justice (AFSJ) — Part I. 2017.

[280] Council Regulation (EC) No. 2725/2000 of 11 December 2000 concerning the establishment of ‘Eurodac’ for the comparison of fingerprints for the effective application of the Dublin Convention. P. 1–10.

[281] Convention determining the state responsible for examining applications for asylum lodged in one of the Member States of the European Communities — Dublin Convention // OJ. 19.8.1997. C. 254. P. 1–12.

лиц, обратившихся с заявлением о предоставлении убежища, и лиц, задержанных в связи с незаконным пересечением внешних границ, в связи с чем создана система, состоящая из центрального подразделения, сформированного в рамках Европейской комиссии, которое будет работать с компьютеризированной центральной базой данных об отпечатках пальцев, а также электронными средствами взаимного обмена сведениями между государствами — членами ЕС и центральной базой данных.

Уже на тот момент в Регламенте отмечалась «чувствительность» категории персональных данных, которые использовались при проведении идентификации лиц. В соответствии с п. 13 Преамбулы обязанность государств — членов ЕС в рамках данной работы «касается особо деликатной области обработки персональных данных, что может оказать влияние на осуществление индивидуальных свобод, имеются особые основания для Совета ЕС оставить за собой осуществление определенных полномочий, в частности, по принятию мер для обеспечения безопасности и достоверности указанных данных».

В последующем в Евродак вносились изменения наряду с реформированием Дублинской системы, которое происходило постепенно посредством принятия Регламента 343/2003 («Дублин II»)[282] и Регламента 604/2013 («Дублин III»)[283]. На смену Регламенту 2725/2000 пришел Регламент 603/2013[284], представляющий собой второе поколение правовой основы функционирования системы Евродак и действующий в настоящее время.

В Преамбуле обновленного текста Регламента, в отличие от

---

[282] Council Regulation (EC) No. 343/2003 of 18 February 2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national // OJ. 25.2.2003. L 50. P. 1–10.

[283] Regulation (EU) No. 604/2013 of the European Parliament and of the Council of 26 June 2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person // OJ. 29.6.2013. L 180. P. 31–59.

[284] Regulation (EU) No. 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No. 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast) // OJ. 29.6.2013. L 180. P. 1–30.

предшествующего, отмечалась роль системы Евродак в содействии достижению цели ЕС по постепенному созданию зоны свободы, безопасности и справедливости (п. 2), а также в борьбе с террористическими преступлениями и иными тяжкими уголовными преступлениями (п. 8). То есть цель Евродак уже не ограничивается только обеспечением идентификации личности незаконных иммигрантов или лиц, ищущих в ЕС международной защиты.

Впервые в документе 2013 г. была обозначена проблема возможного нарушения основного права на уважение частной жизни лиц, чьи персональные данные обрабатываются в Евродак, в связи с изменением первоначальной цели системы, поэтому подчеркивается, что любое такое вмешательство должно осуществляться в соответствии с законом, который должен защищать права человека и быть сформулирован с достаточной точностью, чтобы люди могли корректировать свое поведение (п. 13 Преамбулы).

Таким образом, по общему правилу в целях защиты персональных данных и для исключения систематических сравнений, которые должны быть запрещены, обработка данных должна осуществляться только в определенных случаях и когда это необходимо для целей предотвращения, выявления или расследования террористических преступлений или других серьезных преступлений. При этом обработка персональных данных органами государств-членов в целях предотвращения, выявления или расследования террористических преступлений или других серьезных уголовных преступлений должна регулироваться стандартом защиты персональных данных в соответствии с их национальным законодательством.

В целом в редакции Регламента о Евродак 2013 г. качественное изменение по отношению к ранее действовавшему состояло в том, что значительное внимание стало уделяться именно защите персональных данных и более конкретизированным мерам, которые необходимо принимать государствам-членам и ответственным органам в этой области.

Говоря об основных положениях Регламента 2013 г., уместно обозначить круг субъектов, к данным которых применяется обработка, сроки хранения и условия

обработки, а также положения о защите данных и об ответственности (лица, ходатайствующие о предоставлении убежища (ст. 9 Регламента); граждане третьих стран и лица без гражданства, задержанные пограничными службами при попытке незаконного пересечения границы на территории государства — члена ЕС и которые не возвращены в страну, откуда они прибыли (ст. 14 Регламента); граждане третьих стран и лица без гражданства, незаконно находящиеся на территории государств – членов ЕС (ст. 17 Регламента)). При этом минимальный возраст лиц, отпечатки пальцев которых могут быть сняты, составляет 14 лет. Срок хранения в системе данных ходатайствующих о предоставлении убежища лиц составлял 10 лет с даты снятия отпечатков пальцев; задержанных пограничными службами при попытке незаконного пересечения границы на территории государства — члена ЕС — 18 месяцев.

В качестве основного признака, отличающего Евродак от VIS и SIS, следует отметить обезличивание данных о субъектах, ходатайствующих о предоставлении убежища. В соответствии с Регламентом в базу данных вносятся только следующие сведения: наименование государства — члена ЕС, внесшего указанные сведения; место и дата подачи заявления о предоставлении убежища; данные отпечатков пальцев; пол; условный номер, используемый государством-членом; дата изъятия отпечатков пальцев; дата, когда данные об отпечатках пальцев были переданы в центральную базу данных. Требования в отношении сбора, передачи, актуальности хранения и обработки результатов сравнения данных отпечатков пальцев также были урегулированы Регламентом 603/2013.

Перечисленные и рассмотренные нормы законодательства о Евродак не являются окончательными, так как в рамках реформы Общей европейской системы предоставления убежищ 4 мая 2016 г. Комиссия представила на рассмотрение Европейского парламента и Совета ЕС первый пакет законопроектов, включающий новую редакцию Регламента, учреждающего систему Евродак[285], ввиду пересмотра

[285] Proposal for a Regulation of the European Parliament and of the Council on the establishment of ‘Eurodac’ for the comparison of fingerprints for the effective application of Regulation (EU) No. 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], for identifying an illegally staying third country

Дублинской системы[286], и на сегодняшний день уже мы имеем актуализированный Регламент 2024/1358 о Евродак, который своим названием указывает на центральный объект его регулирования — «биометрические данные, сравниваемые с целью эффективного применения нормативных актов ЕС для выявления незаконно пребывающих граждан третьих стран и лиц без гражданства, а также запросы правоохранительных органов государств-членов о сравнении с данными Евродак».

Согласно новому Регламенту, сфера действия системы Евродак существенно расширяется и применяется для идентификации нелегальных иммигрантов в целях содействия их возвращению в страну постоянного проживания[287].

Важнейшим для нашего исследования изменением в новой редакции Регламента о Евродак является введение понятий «биометрия» и «биометрические идентификаторы», а также расширение перечня данных, подлежащих обработке в системе, речь идет главным образом об изображении лица.

Теперь законодательство о Евродак не ограничивается только понятием «данные отпечатков пальцев», что представляло эту систему исключительно дактилоскопической. Упомянутые нововведения, на наш взгляд, делают ее биометрической.

Ожидается, что упрощение идентификации незаконно пребывающих граждан третьих стран или лиц без гражданства с использованием биометрических данных будет способствовать повышению эффективности политики ЕС в отношении возвращения нелегальных мигрантов, которые используют обманные и мошеннические средства, чтобы избежать своей идентификации.

Биометрия теперь признана важным элементом в установлении личности лиц, в отношении данных которых применяется обработка в системе Евродак, а к данным изображения лица будет применяться следующее определение:

---

national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes COM/2016/0272 final/2 — 2016/0132 (COD).

[286] Proposal for a Regulation of the European Parliament and of the Council establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person COM/2016/0270 final — 2016/0133 (COD).

[287] Войников В. В. Реформа законодательства Европейского Союза об убежище как ответ на миграционный кризис в Европе // Труды Института государства и права РАН. 2017. № 5 (63). С. 149–169.

«изображение лица — цифровое изображение лица с достаточным разрешением и качеством изображения для использования при автоматическом сопоставлении биометрических данных».

Среди других ключевых изменений в предлагаемой редакции Регламента 2024 г. отметим:

— увеличение срока хранения персональных данных для нелегальных иммигрантов с 18 месяцев до пяти лет. Для просителей убежища срок хранения персональных данных останется прежним — 10 лет;

— снижение возраста детей для снятия отпечатков пальцев до шести лет. Регламент 2013 г. не содержал требования о снятии отпечатков пальцев у детей, не достигших возраста 14 лет;

— обмен информацией, хранящейся в Евродак, с третьими странами. Регламент теперь закрепляет возможность для целей высылки передавать третьим странам персональные данные нелегальных иммигрантов, в то время как Регламент 2013 г. содержал категорический запрет на разглашение какой-либо информации[288].

Отдельное внимание новым Евродак уделяется вопросам обработки биометрических данных несовершеннолетних в целях регулирования миграционных процессов с учетом основных прав ребенка. В соответствии со ст. 14 Регламента 2024/1358 биометрические данные несовершеннолетних в возрасте от шести лет должны собираться должностными лицами, специально обученными для сбора биометрических данных несовершеннолетнего с учетом интересов ребенка и при полном соблюдении наилучших интересов ребенка и гарантий, изложенных в Конвенции ООН о правах ребенка. Подчеркивается, что наилучшие интересы ребенка должны учитываться в первую очередь при применении упомянутого Регламента.

Визовая информационная система (VIS) и Шенгенская информационная система (SIS)

[288] Мальцева Ю. В. Реформирование общей Европейской системы предоставления убежища // Современная Европа. 2017. № 4 (76). С. 121–129.

Данным информационным системам хотелось бы уделить отдельное внимание, так как правовые основы их функционирования неразрывно связаны с такими фундаментальными актами в области миграционного права ЕС, как Визовый кодекс (имеющий в полном объеме юридически обязательную силу и распространяющий действие на все Шенгенское пространство, которое охватывает как государства — члены ЕС, так и некоторые ассоциированные государства) и Шенгенский кодекс о границах[289] (устанавливающий единые правила пересечения всеми людьми как внутренних, так и внешних границ Шенгенского пространства).

Визовая информационная система (VIS) — информационная система обмена данными между государствами-членами о заявлениях и принятых по ним решениях, целями которой являются упрощение процедуры подачи заявлений о получении визы, предотвращение незаконной иммиграции, борьба с мошенничеством и оптимизация проверочных мероприятий в пунктах пересечения внешних границ и на территории государств-членов.

Обработка биометрических данных в VIS признается необходимой для обеспечения проверки и идентификации ходатайствующего о предоставлении визы лица в соответствии с п. 10 Преамбулы Регламента 767/2008. Далее по тексту Регламента понятие «биометрические данные» практически не применяется. Вместо него употребляются более конкретизированные данные, такие как «отпечатки пальцев» и «фотография».

В соответствии со ст. 20 «Доступ к данным для идентификации» гл. III «Доступ к данным других органов» компетентные в проведении проверок на внешних пунктах пересечения границ органы получают доступ к поиску по отпечаткам пальцев лица, которое не соответствует или перестало соответствовать условиям въезда, пребывания или проживания на территории государств — членов ЕС, исключительно для целей идентификации такого лица.

Доступ к поиску по отпечаткам пальцев также предусмотрен для уполномоченных органов исключительно в целях определения государства —

[289] Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code) // OJ. 23.3.2016. L 77. P. 1–52.

члена ЕС, ответственного за рассмотрение ходатайств о предоставлении убежища (ст. 21 «Доступ к данным для определения ответственности за ходатайства о предоставлении убежища»). При этом ходатайствующие лица должны быть письменно проинформированы о целях, сроках, категориях получателей данных, когда фотографии и отпечатки пальцев уже собраны.

Статья 45 Регламента подчеркивает важность обеспечения координации центральной системы VIS с национальными интерфейсами государств — членов ЕС, отмечая обеспечение возможности и условий для обработки именно биометрических данных.

Подобно ст. 57 Визового кодекса, в Регламенте 767/2008 содержится положение о необходимости представления Комиссией отчета о техническом прогрессе в отношении использования отпечатков пальцев на внешних границах и своих предложениях по продолжительности поисков с использованием номера визовой марки в сочетании с проверкой отпечатков пальцев владельца визы, в том числе не является ли предполагаемая продолжительность такого поиска причиной чрезмерного затягивания времени ожидания на пунктах пересечения границ. Комиссия должна передавать данные оценки в Европейский парламент и Совет (ст. 50 «Мониторинг и оценка»).

В соответствии с п. 9 Преамбулы Визового кодекса одними из существенных требований к ходатайству о предоставлении визы выступают явка ходатайствующего лица при подаче своего первого ходатайства и регистрация его элементов биометрической идентификации в VIS. Пункт 11 Преамбулы также признает биометрические идентификаторы, полученные государством-членом в рамках процедуры по ходатайству о предоставлении визы, в качестве консульских документов согласно Венской конвенции о консульских сношениях от 24 апреля 1963 г., в связи с чем в отношении их использования должно обеспечиваться надлежащее обращение.

В Визовом кодексе отдельная статья отведена роли биометрических данных в процедуре ходатайства о получении визы (ст. 13 «Биометрические элементы идентификации» гл. II «Ходатайство»).

В пункте 1 ст. 13 установлено требование о соблюдении гарантий, предусмотренных ЕКПЧ, Хартией ЕС об основных правах и Конвенцией ООН о правах ребенка, при получении государствами-членами у ходатайствующего лица биометрических идентификаторов, включающих сканированную или сделанную непосредственно при подаче ходатайства фотографию и его десять отпечатков пальцев, дактилоскопированных в горизонтальном положении и преобразованных в цифровую форму (п. 2 ст. 13).

В пунктах 4, 5 ст. 13 содержится отсылка к международным стандартам Doc 9303 ИКАО и Решению 2006/648/ЕС Комиссии от 22 сентября 2006 г. об установлении технических спецификаций стандартов в отношении биометрических идентификаторов для VIS, где акцентируется внимание на обязательном порядке получения отпечатков пальцев и строгом выполнении установленных требований и стандартов к фотографии.

Ввиду п. 6 функции по сбору биометрических данных могут осуществляться исключительно уполномоченными на то должностными лицами, указанными в Визовом кодексе. Принятие биометрических идентификаторов, помимо уполномоченных лиц, прописанных в Визовом кодексе, может проводиться уполномоченным на то персоналом консульств в ходе исполнения им консульского надзора или внешним поставщиком услуг.

Кроме этого, в визовом законодательстве ЕС имеются положения, на основании которых установлен круг лиц, освобожденных от обязанности предоставления дактилоскопических данных. Например, согласно п. 7 ст. 13 Визового кодекса к ним относятся:

— дети до 12 лет;

— лица, у которых физически невозможно получить отпечатки пальцев. В таком случае дактилоскопии подлежит возможное количество пальцев. Однако если данная причина носит временный характер, то в следующий раз такое лицо обязано предоставить отпечатки пальцев. Уполномоченные лица имеют право затребовать документы, подтверждающие временную невозможность. При наличии определенных трудностей в процессе отбирания отпечатков пальцев

государства — члены ЕС обязаны предоставить надлежащие средства, с помощью которых будут произведены отпечатки пальцев, но такие средства не должны ущемлять достоинство лица;

— главы государств или правительств и члены национальных правительств вместе с сопровождающими их супругами, члены их официальной делегации, когда они приглашены правительствами государств-членов или международными организациями с официальной целью;

— монархи и другие высокопоставленные члены королевской семьи, когда они приглашены правительствами государств-членов или международными организациями с официальной целью.

Статьями 18 «Проверка компетенции консульства» и 19 «Приемлемость» гл. III «Рассмотрение ходатайства и принятие по нему решения» предусмотрена проверка консульством наличия полученных у ходатайствующего лица биометрических данных в рамках принятия решения о компетентности консульства. В случае признания ходатайства неприемлемым в соответствии с п. 1 ст. 19 биометрические данные подлежат немедленному уничтожению.

При организации процедур в отношении ходатайств государства-члены несут обязательства по оснащению своих консульств и ответственных за выдачу виз на границах органов необходимым оборудованием для получения биометрических идентификаторов (пп. «а» п. 2 ст. 40 «Формы сотрудничества» разд. IV «Административное управление и организация»).

В случае сотрудничества государств-членов по организации приема ходатайств в форме «совместного размещения» персонал консульств одного или нескольких государств-членов выполняет процедуры в отношении получения биометрических идентификаторов с использованием оборудования последнего (п. 1 ст. 41 «Сотрудничество между государствами»). При создании «совместного центра по приему ходатайств» персонал консульств двух или более государств-членов объединяется в одном здании, предназначенном для подачи ходатайствующими лицами своих ходатайств (включая биометрические идентификаторы) (п. 2 ст. 41).

При сотрудничестве с внешними поставщиками услуг в соответствии со ст. 43 «Сотрудничество с внешними поставщиками услуг» Визового кодекса внешнему поставщику услуг могут быть поручены получение ходатайств и биометрических данных и передача их в консульство. Вместе с тем пунктом 1 ст. 45 получение биометрических данных в рамках организации подачи ходатайств при сотрудничестве государств-членов с коммерческими посредниками не предусмотрено.

В рамках мониторинга и оценки практического применения положений Визового кодекса Комиссией в предусмотренные ст. 57 «Мониторинг и оценка» сроки представляется доклад Европейскому парламенту и Совету. В том числе каждые четыре года представляется доклад о получении и использовании биометрических идентификаторов, пригодности выбранного стандарта ИКАО, соблюдении правил в области защиты данных, опыте сотрудничества с внешними поставщиками услуг, особенно в том, что касается получения биометрических данных, реализации правила 59 месяцев для копирования отпечатков пальцев и организации процедур в отношении ходатайств. Доклад также охватывает случаи, в которых отпечатки пальцев фактически не смогли быть предоставлены или не являлись обязательными по юридическим причинам, в сопоставлении с количеством случаев, в которых отпечатки пальцев были дактилоскопированы. Доклад включает информацию о случаях, когда лицу, которое фактически не смогло предоставить отпечатки пальцев, было отказано в визе.

Шенгенский кодекс о границах (п. 13 Преамбулы) предусматривает, что биометрические данные, которые первоначально предоставляются для формирования первого заявления для получения визы в VIS, копируются при повторном обращении и в обязательном порядке используются в VIS для проверки при въезде на внешних границах.

Это единственный раз, когда Шенгенский кодекс упоминает биометрические данные в качестве категории персональных данных, далее в тексте они конкретизируются как отпечатки пальцев. Например, п. 10 Преамбулы признает отпечатки пальцев единственным способом подтвердить личность человека,

который собирается въехать в шенгенскую зону, и установить, что данное лицо является именно тем человеком, которому выдана виза. Для этой цели и предназначена VIS, в которой осуществляется поиск данных человека по номеру визовой наклейки и отпечаткам пальцев.

Впрочем, в исключительных случаях, определяемых самостоятельно государствами-членами, такая проверка может не проводиться ввиду длительного времени поиска и влияния на время ожидания в пунктах пересечения границы. При этом четко устанавливаются условия и обстоятельства использования VIS без проверки отпечатков пальцев, а случаи такого отступления должны сводиться к строгому минимуму в отдельных пунктах пересечения границы (п. 14 Преамбулы).

Пункт «c» ст. 8 Шенгенского кодекса о границах содержит положения об организации пограничного контроля, в том числе процедурах проверки граждан третьих стран при въезде/выезде. Данной статьей установлено, что во всех случаях, когда имеются сомнения в личности владельца визы и (или) в подлинности визы, данные в VIS должны подлежать проверке по номеру визовой наклейки в сочетании с проверкой отпечатков пальцев. В остальных предусмотренных этой же статьей случаях проверка может предусматривать только поиск по визовой наклейке. Указанные случаи связаны прежде всего с такими факторами, как длительное время проверки и организационные ресурсы (персонал, оборудование).

Шенгенская информационная система составляет техническую основу сотрудничества стран Шенгенской зоны[290]. Это информационная система, с помощью которой полиция, службы пограничного и таможенного контроля, ответственные за проверку данных на внешних границах Шенгенской зоны, а также в пределах Шенгенской зоны, распространяют уведомления о разыскиваемых или пропавших людях и предметах, например похищенных автомобилях и документах.

SIS прошла несколько ступеней совершенствования начиная с 1995 г., когда она была создана. Вторая версия этой системы, известная как SIS II, была введена

[290] Шенгенская зона — это территория ряда стран, занимающих бóльшую часть европейского континента, которые отменили пограничный контроль на границах между собой. В странах-участницах действуют единые правила пограничного контроля на внешних границах Шенгенской зоны, а также правила выдачи виз и механизмы сотрудничества органов юстиции и охраны правопорядка в вопросах борьбы с преступностью.

в работу в 2013 г. с возможностью включения в уведомления отпечатков пальцев и изображений лица.

В марте 2023 г. Европейская комиссия в своем коммюнике объявила о запуске актуализированной версии SIS, которая, как заявлено, стала настоящим прорывом в сфере обеспечения безопасности и пограничного контроля в ЕС[291]. Новые возможности системы предусмотрели доступ к более широкому кругу биометрических данных, а также сведениям о ДНК пропавших без вести лиц.

Текст действующего на сегодняшний день Регламента о SIS признает обработку именно биометрических данных надежным способом идентификации лиц. При этом использование биометрических данных должно ограничиваться целями обработки и соответствовать законодательству о защите данных, а также правах человека, включая права ребенка (п. 20 Преамбулы).

Вопросы технического и консультационного обеспечения процессов обработки биометрических данных являются одними из приоритетных в Регламенте. Например, пункт 23 Преамбулы особое внимание обращает на необходимость установления стандартов качества, применимых к хранению биометрических данных. Европейскому надзорному органу по защите данных в соответствии с п. 46 Преамбулы должны быть предоставлены достаточные ресурсы для выполнения задач, возложенных на него в соответствии с упомянутым Регламентом, включая помощь лиц, обладающих опытом работы с биометрическими данными.

Помимо дактилоскопических данных, статья 3 Регламента к биометрическим данным относит фотографии и изображения лица. Определение биометрических данных, содержащееся в Регламенте, практически копирует дефиницию биометрических данных, закрепленную в Регламенте о защите данных.

Специальным правилам по обращению с биометрическими данными отведена глава VI Регламента «Поиск по биометрическим данным».

Статья 32 устанавливает правила ввода в систему фотографий, изображений

[291] URL: https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/schengen-information-system_en (дата обращения: 12.12.2024).

лица и дактилоскопических данных, соответствующих минимальным стандартам качества данных и техническим спецификациям. Перед вводом таких данных должна быть проведена проверка качества в целях подтверждения соблюдения минимальных стандартов качества данных и технических спецификаций. Для хранения биометрических данных должен проводиться аналогичный контроль соответствия стандартам качества данных, необходимый для проверки личности человека и его идентификации. На Комиссию, согласно упомянутой статье, возлагается обязанность по принятию имплементационных актов, устанавливающих минимальные стандарты качества данных и технические спецификации.

Статья 33 предусматривает специальные правила проверки и поиска с применением биометрических данных. Так, если биометрические данные стали доступны в уведомлении в SIS, такие данные подлежат использованию для подтверждения личности человека, который был обнаружен в результате буквенно-цифрового поиска, выполненного в системе.

Обе статьи (32 и 33) Регламента предусматривают поиск и ввод дактилоскопических данных, хранящихся в SIS, по полным или неполным наборам отпечатков пальцев или ладоней, обнаруженных на месте преступления, если с высокой степенью вероятности можно установить, что они принадлежат лицу, совершившему тяжкое преступление или террористический акт, при условии, что поиск проводится одновременно в соответствующих национальных базах данных отпечатков пальцев.

Поиск по дактилоскопическим данным в соответствии со ст. 33 возможен во всех случаях для установления личности человека, если личность этого человека не может быть установлена другими способами. Для этой цели Центральная SIS должна содержать автоматизированную систему идентификации по отпечаткам пальцев (AFIS).

Статья 33 также регламентирует, что при наличии технической возможности и при обеспечении высокой степени надежности идентификации фотографии и изображения лица могут быть использованы для проверки личности человека в

обычных пунктах пересечения границы. Внедрению в SIS предшествует предоставление Комиссией отчета о доступности, готовности и надежности требуемой технологии, а также консультация с Европейским парламентом. После начала использования технологии в обычных пунктах пересечения границы Европейская комиссия будет уполномочена принимать делегированные акты, касающиеся определения других обстоятельств, при которых фотографии и изображения лиц могут использоваться для идентификации лиц.

Статья 55 Регламента предписывает государствам — членам ЕС обеспечить их надзорные органы достаточными ресурсами для выполнения задач, возложенных на них в соответствии с Регламентом, и доступом к консультациям лиц, обладающих достаточными знаниями в рамках работы с биометрическими данными.

Все вышеупомянутые акты и информационные системы ЕС направлены прежде всего на обеспечение безопасности общественной жизни, групп людей и общества в целом. Однако в контексте безопасности самих биометрических данных и личных границ их субъектов регулирование осуществляется в плоскости других актов ЕС, таких как Регламент о защите данных, Регламент об ИИ и Регламент (ЕС) от 20 июня 2019 г. 2019/1157 об усилении безопасности удостоверений личности граждан Союза и документов о проживании, выдаваемых гражданам Союза и членам их семей при осуществлении их права на свободное передвижение (Регламент 2019/1157)[292].

Регламент об ИИ. Большим правовым достижением в мировой практике регулирования новых технологий стало принятие Регламента об ИИ. Значительная его часть посвящена вопросам применения биометрических систем и биометрических данных в рамках эксплуатации систем ИИ на внутреннем рынке ЕС. Сам Регламент положения об использовании систем искусственного интеллекта для удаленной биометрической идентификации рассматривает в

[292] Regulation (EU) 2019/1157 of the European Parliament and of the Council of 20 June 2019 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement // OJ. 12.7.2019. L 188. P. 67–78.

контексте правового регулирования защиты физических лиц в отношении обработки персональных данных и определяет свое правовое назначение в этой связи как основанное на ст. 16 ДФЕС (п. 3 Преамбулы Регламента об ИИ).

Статья 3 Регламента об ИИ копирует определение биометрических данных, закрепленное Регламентом о защите данных. Дополнительно приводятся такие ключевые категории, как:

— «биометрическая идентификация» — автоматическое распознавание физических, физиологических, поведенческих или психологических особенностей человека с целью установления личности физического лица путем сравнения биометрических данных этого лица с биометрическими данными физических лиц, хранящимися в базе данных (п. 35 ст. 3);

— «биометрическая верификация» — автоматизированная индивидуальная проверка, включая аутентификацию (подтверждение), личности физических лиц путем сравнения их биометрических данных с ранее предоставленными биометрическими данными (п. 36 ст. 3);

— «биометрическая система категоризации» — система, предназначенная для отнесения физических лиц к определенным категориям на основе их биометрических данных, за исключением случаев, когда она является вспомогательной для другой коммерческой услуги и строго необходима по объективным техническим причинам (п. 40 ст. 3);

— «система удаленной биометрической идентификации» — система, предназначенная для идентификации физических лиц без их активного участия, как правило, на расстоянии путем сравнения биометрических данных человека с биометрическими данными, содержащимися в базе данных (п. 41 ст. 3);

— «система удаленной биометрической идентификации в режиме реального времени» — система удаленной биометрической идентификации, посредством которой сбор биометрических данных, сравнение и процесс идентификации происходят без существенных задержек, с возможностью мгновенной идентификации (п. 42 ст. 3);

— «система пост-удаленной биометрической идентификации» — система,

осуществляющая удаленную биометрическую идентификацию по факту, не в режиме реального времени (п. 43 ст. 3).

«Система распознавания эмоций» отдельно выделена как система искусственного интеллекта, предназначенная для идентификации или определения эмоций или намерений физических лиц на основе их биометрических данных (п. 39 ст. 3 Регламента об ИИ).

Вокруг использования перечисленных систем ИИ и процессов обработки и строится основное регулирование Регламента в части биометрии. Сводится такое регулирование, по нашему мнению, к двум главным аспектам:

1) запрет на использование систем ИИ с применением биометрических технологий (в рамках регулирования гл. 2);

2) особое регулирование использования биометрических систем ИИ с высоким уровнем риска (в рамках регулирования гл. 3).

Пункт 1 ст. 5 устанавливает *запрет* на ввод в эксплуатацию и использование на рынке биометрических систем категоризации, которые позволяют определить такие признаки физического лица, как раса, политические убеждения или сексуальная ориентация. Этот запрет является абсолютным и направлен на предотвращение случаев, когда результаты обработки биометрических данных системой способны привести к дискриминации или раскрыть конфиденциальную информацию о человеке.

Аналогично в пункте 30 Преамбулы подчеркивается, что применение систем биометрической категоризации при помощи биометрических данных физических лиц (лицо или отпечатки пальцев) в целях определения политических взглядов человека, членства в профсоюзе, религиозных или философских убеждений, расы, сексуальной жизни или сексуальной ориентации строго запрещено, за исключением предусмотренных законодательством ЕС или государств-членов случаев.

Кроме того, под запрет подпадает использование систем удаленной биометрической идентификации в режиме реального времени, за исключением случаев, когда обработка биометрических данных необходима в целях:

— поиска конкретных жертв похищения, торговли людьми или сексуальной эксплуатации, а также пропавших без вести лиц;

— предотвращения конкретной, существенной и неминуемой угрозы жизни или физической безопасности лиц или реальной и присутствующей в настоящее время или реальной и прогнозируемой угрозы террористического нападения;

— установления местонахождения или идентификации лица, подозреваемого в совершении уголовного преступления, с целью проведения уголовного расследования, или судебного преследования, или исполнения уголовного наказания за преступления.

Пункт 2 ст. 5 обращает внимание на то, что использование систем удаленной биометрической идентификации в режиме реального времени в общедоступных местах при осуществлении деятельности правоохранительных органов возможно только для подтверждения личности конкретного лица. При этом каждое использование удаленной биометрической идентификационной системы в режиме реального времени в общедоступных местах требует предварительного разрешения, выдаваемого судебным органом или независимым административным органом, решение которого является обязательным для государства-члена, в котором предполагается использование. Такое разрешение выдается по мотивированному запросу и в соответствии с конкретными нормами национального законодательства (п. 3 ст. 5).

К *системам ИИ с высоким уровнем риска* пункт 2 ст. 6 и приложение 3 к Регламенту относят:

— системы удаленной биометрической идентификации;

— все системы, предназначенные для проведения биометрической категоризации на основе конфиденциальных характеристик;

— системы искусственного интеллекта, предназначенные для распознавания эмоций.

Использование перечисленных систем прямо не запрещено, но их применение подлежит строгому регулированию ввиду особой природы биометрических данных и возможного влияния на результаты принятия решений в отношении

физического лица. Пункт 54 Преамбулы более подробно иллюстрирует данную проблему через пример дискриминационных последствий использования биометрических данных, которые происходят в результате технических ошибок, допущенных системами ИИ. Как указывается, риск принятия необъективных решений и дискриминационных последствий особенно актуален в отношении возраста, этнической принадлежности, расы, пола или инвалидности. При этом классификация биометрических систем в качестве систем с высоким уровнем риска исключает системы, предназначенные для биометрической верификации, включая аутентификацию, целями которой является:

- подтверждение того, что конкретное физическое лицо является тем, за кого себя выдает;

- подтверждение личности физического лица для получения доступа к услуге, разблокировки устройства или безопасного доступа в помещения. Биометрические системы, предназначенные для использования исключительно в целях обеспечения кибербезопасности и защиты персональных данных, не являются системами с высокой степенью риска.

Лица, использующие систему распознавания эмоций или биометрическую систему категоризации, обязаны руководствоваться пунктом 3 ст. 50, в том числе информировать людей об обработке биометрических данных и проводить такую обработку в соответствии с Регламентом о защите данных и другими соответствующими нормативными актами ЕС. Это отражает намерение создателей Регламента об ИИ обеспечить прозрачность и защитить права личности даже в системах с высоким уровнем риска.

Регламент 2019/1157. Пункт 17 Преамбулы Регламента 2019/1157 признает интеграцию биометрических данных в удостоверяющие личность и подтверждающие вид на жительство документы важным шагом для повышения безопасности в ЕС, а также наиболее эффективным инструментом проверки подлинности документов и установления личности человека. Предполагается, что включение таких биометрических идентификаторов должно позволить гражданам ЕС в полной мере пользоваться своими правами на свободное передвижение.

Регламент не содержит правовой основы для создания и ведения централизованной базы данных на уровне ЕС, а также баз данных на национальном уровне для хранения биометрических данных в государствах-членах. Данный вопрос является предметом национального законодательства в соответствии с п. 20 Преамбулы, которое должно соответствовать законодательству ЕС о защите данных.

Статья 3 Регламента 2019/1157 устанавливает к удостоверениям личности требование о содержании высокозащищенного носителя информации, который должен включать изображение лица владельца удостоверения и два отпечатка пальцев в совместимых цифровых форматах. При этом субъекты данных должны быть осведомлены о наличии в их документах носителя информации, содержащего их биометрические данные, включая его доступность в бесконтактной форме, а также обо всех случаях, когда используются данные, содержащиеся в их удостоверениях личности и документах о проживании. Субъект данных также имеет право на их исправление путем выдачи нового документа, если такие данные являются ошибочными или неполными.

Правилам сбора биометрических идентификаторов посвящена статья 10 Регламента, согласно которой:

— биометрические идентификаторы должны собираться исключительно квалифицированным и должным образом уполномоченным персоналом, назначенным органами, ответственными за выдачу удостоверений личности или видов на жительство;

— в целях обеспечения соответствия биометрических идентификаторов личности заявителя последний должен лично присутствовать по крайней мере один раз в процессе выдачи каждой заявки;

— государства-члены должны обеспечить наличие надлежащих и эффективных процедур сбора биометрических идентификационных данных и соответствие этих процедур правам и принципам, изложенным в Уставе ООН, Конвенции о защите прав человека и основных свобод и Конвенции ООН о правах ребенка;

— за исключением случаев, когда это требуется для целей обработки в соответствии с законодательством ЕС и национальным законодательством, биометрические идентификаторы, сохраняемые с целью персонализации удостоверений личности или документов о проживании, должны храниться в условиях повышенной безопасности, только до даты получения документа и в любом случае не дольше, чем 90 дней с даты выдачи. По истечении этого срока указанные биометрические идентификаторы должны быть немедленно стерты или уничтожены.

Пункт 6 ст. 11 содержит закрытый перечень целей использования биометрических данных, хранящихся на носителях удостоверений личности и документов, подтверждающих вид на жительство, среди которых:

— установление подлинности удостоверения личности или документа о проживании (о виде на жительство);

— установление личности владельца с помощью непосредственно доступных сопоставимых признаков в тех случаях, когда по закону требуется предъявление удостоверения личности или документа о проживании.

За государствами — членами ЕС закреплено обязательство вести и ежегодно направлять в Комиссию список компетентных органов, имеющих доступ к биометрическим данным, хранящимся на носителях информации. Комиссия публикует в Интернете подборку таких национальных списков (п. 7 ст. 11).

Помимо этого, государствам-членам в соответствии с п. 32 Преамбулы рекомендуется предпринять все необходимые шаги для обеспечения высокоточной идентификации лица, которому выдается удостоверение личности. С этой целью государства-члены могут предусматривать сбор биометрических идентификаторов, в частности изображения лица, путем регистрации в режиме реального времени национальными органами, выдающими удостоверения личности.

В рамках анализа соответствия положений Регламента 2019/1157 нормам Регламента о защите данных констатируем, что в Преамбуле Регламента 2019/1157 особенно подчеркиваются природа биометрических данных и отнесение их к

специальным категориям персональных данных, как это предусмотрено Регламентом о защите данных, в связи с чем должны приниматься соответствующие меры предосторожности на всех стадиях обработки биометрических данных, а также при сотрудничестве государств-членов с внешними поставщиками услуг. Государства-члены несут ответственность за надлежащую обработку биометрических данных, от сбора до интеграции данных на высокозащищенном носителе, в соответствии с Регламентом о защите данных (п. 41 Преамбулы).

Использование биометрических данных в целях обеспечения частной, общественной и национальной безопасности в ЕС является важным инструментом для борьбы с преступностью, защиты граждан и обеспечения безопасности общественных пространств. Биометрические технологии предоставляют высокий уровень идентификации и аутентификации личности, что делает их эффективным средством контроля доступа к помещениям, объектам и информационным системам.

Впрочем, вместе с потенциалом для улучшения безопасности существуют и риски, связанные с защитой приватности и прав граждан. Необходимо строго соблюдать законодательство о защите персональных данных, включая хоть и несовершенный Регламент о защите данных, и обеспечивать прозрачность, согласие субъектов данных и минимизацию данных при использовании биометрических систем.

Кроме того, важно продолжать исследования и разработки в области безопасности и защиты данных, чтобы улучшать надежность и эффективность биометрических технологий и совершенствовать механизмы контроля и надзора за их использованием. Только с соблюдением высоких стандартов защиты данных и приватности граждан можно обеспечить устойчивое и безопасное использование биометрических данных в ЕС, что содействует общественной безопасности и защите прав и свобод граждан в цифровой эпохе.

Отдельно подчеркнем, что исследование в рамках настоящего параграфа демонстрирует разнообразие правовых актов, регулирующих взаимодействие

информационных систем ЕС, в которых обрабатываются и хранятся биометрические данные граждан как государств-членов, так и граждан третьих стран.

Сложившаяся в России практика свидетельствует о не таком большом количестве информационных систем, предназначенных для хранения и обмена биометрической информацией, отмечается стремление свести к минимуму риски широкомасштабного распространения биометрических данных граждан в цифровом поле.

В 2021 г. на международной конференции по искусственному интеллекту и анализу данных AI Journey 2021 Президент РФ В. В. Путин заявил, что биометрические данные должны храниться в единой биометрической системе, а государство должно быть ответственным за их хранение. В. В. Путин разъяснил: «Особые решения следует предпринять в отношении информации, имеющей критическое значение для безопасности граждан. Речь прежде всего о биометрических данных, которые все чаще используются для совершения финансовых и других операций, в том числе для оплаты проезда, скажем, в метро, как в Москве сейчас это уже делается. Считаю, что такая предельно личная информация должна храниться в единой государственной системе биометрической идентификации, то есть государство должно взять на себя ответственность за ее хранение»[293].

30 декабря 2021 г. Президентом РФ был подписан соответствующий Закон[294], наделяющий единую биометрическую систему статусом государственной информационной системы. При этом законом допускается обработка биометрических данных в государственных информационных системах аккредитованных государственных органов.

---

[293] Выступление Президента Российской Федерации В. В. Путина в рамках основной дискуссии конференции по искусственному интеллекту и анализу данных Artificial Intelligence Journey 2021 на тему «Технологии искусственного интеллекта для решения социальных задач» 12 ноября 2021 г. [Электронный ресурс] // URL: http://www.kremlin.ru/events/president/news/67099 (дата обращения: 19.10.2024).

[294] Федеральный закон от 30 декабря 2021 г. № 441-ФЗ «О внесении изменений в статью 15.3 Федерального закона “Об информации, информационных технологиях и о защите информации” и статьи 3 и 5 Федерального закона “О внесении изменений в отдельные законодательные акты Российской Федерации”» // СЗ РФ. 2022. № 1 (ч. I). Ст. 10.

В контексте отечественного опыта хотелось бы отметить, что Россия не так давно начала работу по совершенствованию собственной миграционной политики именно через правовые инструменты, предусматривающие сбор биометрических данных иностранных граждан. Об этом свидетельствует план мероприятий по реализации в 2024-2025 годах Концепции государственной миграционной политики Российской Федерации на 2019-2025 годы[295], принятый во исполнение Указа Президента Указа Президента Российской Федерации от 31 октября 2018 г. № 622 «О Концепции государственной миграционной политики Российской Федерации на 2019-2025 годы»[296].

План мероприятий предусматривает такие меры как: создание цифрового профиля иностранного гражданина, проведение эксперемента по апробации сбора биометрических данных иностранных граждан в пунктах пропуска через государственную границу Российской Федерации аэропортов московского транспортного авиаузла, регистрация иностранного гражданина в единой биометрической системе за пределами Российской Федерации с использованием специализированного мобильного приложения, расширение перечня виз, выдаваемых в электронной форме.

Целью создания цифрового профиля иностранного гражданина является именно выявление случаев незаконной миграции. Эксперимент по апробации правил и условий въезда в Российскую Федерацию и выезда из Российской Федерации иностранных граждан и лиц без гражданства[297] также предусматривает создание и развитие информационных систем в целях идентификации на основе биометрических персональных данных иностранных граждан и лиц без гражданства в пунктах пропуска через государственную границу страны.

---

[295] Принят распоряжением Правительства Российской Федерации от 16.01.2024 г. № 30-р «О плане мероприятий по реализации в 2024 - 2025 годах Концепции государственной миграционной политики Российской Федерации на 2019 - 2025 годы» // СЗ РФ. 2024. № 4. (ч. 2). Ст. 560.

[296] Указ Президента Российской Федерации от 31 октября 2018 г. № 622 «О Концепции государственной миграционной политики Российской Федерации на 2019-2025 годы» // СЗ РФ. 2018. № 45. (ч. 1). Ст. 6917.

[297] Постановление Правительства Российской Федерации от 7 ноября 2024 г. № 1510 «О проведении эксперимента по апробации правил и условий въезда в Российскую Федерацию и выезда из Российской Федерации иностранных граждан и лиц без гражданства» // СЗ РФ. 2024. № 47. (ч. 1). Ст. 7114.

§ 3.2. Охрана биометрических данных в Европейском Союзе в контексте обеспечения прав человека

Биометрические данные — это прежде всего персональные данные, защита которых гарантирована ст. 16 ДФЕС и ст. 8 Хартии ЕС об основных правах. Персональные данные, включая биометрические, содержащиеся в удостоверяющих личность документах, подлежат обработке в национальных регистрационных системах, которые в свою очередь составляют основу государственного управления[298].

Биометрические данные используются как эффективный механизм обеспечения не только информационной безопасности граждан и компаний, но и национальной безопасности государств. В настоящее время в ЕС биометрические системы идентификации активно используются при обеспечении миграционного контроля (выдача биометрических паспортов, оформление виз, идентификация беженцев и пассажиров), в банковском секторе, в области здравоохранения, противодействия терроризму и иных сферах[299].

Наряду с удобством применения биометрических средств идентификации и заявленной надежностью использования биометрических данных зачастую обработка таких данных влечет нарушение прав человека. Как было отмечено ранее, согласно п. 51 Преамбулы Регламента о защите данных такие данные «заслуживают особой защиты, поскольку контекст их обработки может создать значительные риски для основных прав и свобод».

Отношения, связанные с установлением правовых гарантий защиты прав человека на неприкосновенность частной жизни в связи с применением комплекса технологий систем искусственного интеллекта для удаленной биометрической идентификации личности, стали одной из наиболее чувствительных сфер общественной жизни, подвергшихся влиянию практического внедрения

---

[298] Смирнова Я. В. Проблемы обеспечения права на охрану частной жизни при обработке биометрических данных в Европейском Союзе // Актуальные проблемы российского права. 2022. № 10 (143). С. 183–192.

[299] Волеводз А. Г. Удостоверяющие личность документы с биометрическими персональными данными.

технологий[300]. Аналогичное подтверждает Е. В. Васякина: «С развитием технологий растет и число вопросов, которые вызывают бесконтрольное применение искусственного интеллекта»[301].

Впрочем, использование биометрических данных оказывает влияние на реализацию гораздо более широкого круга прав человека, чем может показаться на первый взгляд. Это обусловлено технической стороной природы биометрических данных.

В зависимости от применяемого вида технологии биометрической идентификации такие данные могут раскрывать информацию о здоровье или другую личную информацию. Например, при помощи системы распознавания лиц можно получить информацию о шрамах, татуировках и иных особых приметах. Если в информационной биометрической системе используется часть или вся информация, полученная из ДНК, используемые данные могут содержать личную информацию о здоровье субъекта данных и даже о здоровье его родственников[302]. Даже ограниченное количество ДНК, используемое сегодня для биометрической идентификации, может в итоге раскрыть иные личные сведения.

Всё перечисленное, в том числе сферы миграции, противодействия терроризму, регулирования охраны генетической и иной информации через биометрические данные и т.д., по нашему мнению, является воплощением проблемы, которая на протяжении многих лет является основной, в большей степени способствующей росту количества споров об использовании биометрических данных, а именно столкновения интересов человека как индивида и интересов безопасности (другого человека / общественной безопасности / национальной безопасности).

Вторая явная проблема касается согласия на обработку биометрических данных, и заключается она, на наш взгляд, в том, что законодательно

---

[300] Кутейников Д. Л., Ижаев О. А., Алексеевич Л. В., Зенин С. С. Неприкосновенность частной жизни в условиях использования систем искусственного интеллекта для удаленной биометрической идентификации личности // Lex Russica. 2022. Т. 75. № 2 (183). С. 121.

[301] Васякина Е. В. Правовое регулирование искусственного интеллекта в России и зарубежных странах: от этики к новой парадигме // Юридический мир. 2023. № 11. С. 49.

[302] Gellman R. Privacy and Biometric ID Systems: An Approach Using Fair Information Practices for Developing Countries. CGD Policy Paper 028. Washington DC : Center for Global Development, 2013.

регламентированная форма такого согласия (какой бы она ни была) предопределяет уровень защищенности биометрических данных и риска нарушения прав человека.

Наряду с обозначенными проблемами существуют также и другие, имеющие не меньшее значение и распространение в судебной практике, например проблема соответствия национального законодательства государств — членов ЕС законодательству ЕС, вопрос о допустимых сроках хранения биометрических данных и т.д.

Настоящий параграф представляет собой исследование практического характера, которое предусматривает в том числе:

— анализ конкретных норм законодательства ЕС на предмет содержания положений, прямо способствующих возникновению указанных проблем;

— разъяснение того, как данные проблемы находят отражение при нарушении различных прав человека в результате использования биометрических данных;

— анализ решений Суда ЕС и ЕСПЧ, иллюстрирующих указанные проблемы.

Регламент о защите данных

Определение биометрических данных содержится в п. 14 ст. 4 Регламента 2016/679, п. 13 ст. 3 Директивы 2016/680/ЕС и п. 18 ст. 3 Регламента 2018/1725 и звучит как «биометрические данные — это персональные данные, полученные в результате специфической технической обработки, относящиеся к физическим, физиологическим или поведенческим признакам физического лица, которые позволяют провести или подтвердить уникальную идентификацию указанного физического лица, например, изображение человеческого лица или дактилоскопические данные».

Согласно законодательству ЕС, биометрические данные, наряду с генетическими и другими данными, относятся к специальным категориям персональных данных (ст. 9 Регламента 2016/679, ст. 10 Регламента 2018/1725), в отношении которых устанавливаются специальные требования обработки. Соответственно, рассматриваемые нормы не представляют собой регулирование индивидуального характера конкретно для биометрических данных, однако их анализ необходим для выявления «пробелов», которые приводят или могут

привести к нарушению прав человека.

В пункте 1 ст. 9 Регламента о защите данных и аналогичных положениях Директивы 2016/680/ЕС и Регламента 2018/1725 установлен запрет на обработку биометрических данных в целях уникальной идентификации физического лица. Однако здесь же, в п. 2 ст. 9 Регламента о защите данных, перечисляются такие условия, при которых данный запрет не будет применяться.

К одному из таких исключений, имеющих значение для нашего исследования, относится согласие субъекта на проведение обработки биометрических данных, но с учетом особенностей, прописанных в законах Союза или государства — члена ЕС, если указанный запрет не будет отменен самим субъектом (пп. «а» п. 2 ст. 9 Регламента о защите данных).

Под «согласием субъекта данных» в соответствии с п. 11 ст. 4 Регламента о защите данных понимается «явно выраженное желание в любой форме, на основании которого лицо совершает действия, подтверждая тем самым свое волеизъявление на обработку персональных данных».

Какая форма согласия будет считаться «явно выраженной» и приемлемой в рамках пп. «а» п. 2 ст. 9 Регламента о защите данных, не уточняется. Логично предположить, что «чувствительная» природа биометрических данных обусловливает наличие согласия субъекта на обработку, выходящего за рамки обыкновенного «волеизъявления или явного позитивного действия» со стороны субъекта данных. Установление письменной формы такого согласия или согласия посредством электронной цифровой подписи внесло бы ясность в вопрос требований к «добровольному, конкретному, информированному и однозначному волеизъявлению», однако таких конкретизаций в законодательстве ЕС не приведено.

В современном мире широко распространены биометрические технологии, позволяющие распознавать лица с точностью до 100 % через системы видеонаблюдения в общественных местах. Однако возникает вопрос о том, является ли использование этой технологии в метро или других местах «добровольным, конкретным, информированным и однозначным

волеизъявлением», выражающим явное согласие на обработку биометрических данных. Что служит правовым основанием для обработки таких данных и как контроллер данных должен демонстрировать, что субъект дал согласие на обработку своих уникальных данных?

Аналогичные вопросы возникают и в отношении еще одного исключения из общего запрета обработки биометрических данных, а именно случаев, когда такая «обработка касается персональных данных, которые субъект данных явным образом сделал публичными» (пп. «e» п. 2 ст. 9 Регламента о защите данных). Когда и каким образом в таком случае данные становятся «общедоступными»? Как установить, намеревалось ли лицо сделать свои биометрические данные общедоступными? По нашему мнению, упомянутое исключение косвенно может быть отнесено к проблеме «согласия» на обработку биометрических данных.

Предусмотренные случаи, при которых «обработка необходима для защиты жизненных интересов субъекта данных либо другого физического лица, когда субъект данных физически или юридически не способен дать согласие» (пп. «c» п. 2 ст. 9 Регламента о защите данных), снова подталкивают нас к дискуссии о роли согласия субъекта данных, однако приведенное исключение приобретает иной правовой окрас в связи с наличием такого фактора, как «защита жизненного интереса субъекта данных».

В связи с этим целесообразно привести п. 46 Преамбулы Регламента о защите данных, где устанавливаются условия правомерности обработки персональных данных. В частности, такими случаями являются действия, направленные на защиту общественно важных прав субъекта или другого лица. Кроме этого, к указанным случаям можно отнести действия при возникновении гуманитарных ситуаций, таких как эпидемия или стихийные антропогенные бедствия.

Подпункт «b» п. 2 ст. 9 Регламента о защите данных допускает также обработку биометрических данных без согласия субъекта при наличии такой «необходимости» в сфере трудового права, права социального обеспечения и социальной защиты. При этом, как отмечается экспертами в области защиты

данных[303], в ЕС в основном регулирование в этой области осуществляется на уровне национального законодательства государства — члена ЕС для того, чтобы понять, насколько соблюдаются права отдельных лиц. Таким образом, в законодательстве ЕС не существует единого правила, которое будет применимо ко всем субъектам Союза.

Целесообразно также рассмотреть в рамках одной группы случаи обработки биометрических данных, предусмотренные подпунктом «g» п. 2 ст. 9 Регламента о защите данных (из соображений важного публичного интереса на основании законодательства Союза или государства-члена) и подпунктом «i» п. 2 ст. 9 того же Регламента (по причинам важного публичного интереса в области общественного здравоохранения, например защиты от серьезных трансграничных угроз здоровью).

Регламент о защите данных не приводит разъяснений относительно того, что понимается под «существенным публичным интересом» в обоих случаях. Поскольку в исключениях речь идет о праве Союза или государства-члена, национальным юрисдикциям предоставляется свобода усмотрения при решении на локальном уровне вопроса о том, что представляет собой «существенный публичный интерес». Логично, что «существенный» публичный интерес требует достижения более высокого стандарта, чем просто «публичный интерес». Вероятно, в первом случае «существенный публичный интерес» может быть связан с обеспечением безопасности, например борьбой с терроризмом, и данное исключение не будет применяться к специальным категориям персональных данных, которые уже подпадают под исключение, предусмотренное в области общественного здравоохранения. Зачастую сложно определить, какое из исключений применимо в том или ином случае. Необходимо обратиться к конкретным обстоятельствам и внимательно изучить факты, чтобы решить, какое из них является наилучшим правовым основанием для обработки специальных категорий персональных данных.

[303] См., например, комментарий Луи-Филиппа Граттона к Регламенту о защите данных.

Рассмотрение всех вышеперечисленных условий обработки биометрических данных без согласия субъекта данных представляется исключительно важным, так как каждое из условий может быть сопоставлено с практическим использованием биометрических данных физических лиц в той или иной сфере и оправдывать нарушение тех или иных прав и свобод.

Заключительным положением ст. 9 Регламента о защите данных является пункт 4, оставляющий за государствами-членами право сохранять или вводить дополнительные условия, в том числе ограничения, в отношении обработки биометрических данных, что, с одной стороны, предоставляет возможность государствам-членам совершенствовать правовое регулирование конкретно в сфере биометрических данных, с другой — минимизирует шансы достичь максимального единообразия в правовом регулировании на уровне ЕС.

Права человека, подвергающиеся риску нарушения при использовании биометрических данных

На сегодняшний день улицы и общественные места большей части городов всего мира оснащены камерами видеонаблюдения, которые устанавливаются в правоохранительных целях. Такие камеры позволяют с высокой точностью установить личность прохожего благодаря встроенным системам биометрической идентификации, что позволяет, например, быстро вычислить преступника. Однако некоторые исследования демонстрируют[304], что осознание людьми того, что за ними наблюдают, может привести к отказу от участия в публичных собраниях, в социальной или культурной жизни, от свободного выражения мыслей, мнений и религиозных убеждений в общественном пространстве. Таким образом приватность и безопасное общение ставятся под угрозу.

Так называемый биометрический контроль может также создавать препятствия для реализации человеком права на свободу выражения мнений, права на мирные собрания, демонстрации и митинги. Права журналистов также могут

[304] См., например, Доклад АПП 2020 г., указ. соч., стр. 20; или London Policing Ethics Panel, Final Report on Live Facial Recognition. May. 2019.

быть затронуты при проведении ими расследований. Обе приведенные в пример категории граждан могут испытывать опасения, что их биометрические данные могут быть использованы против них органами власти.

Перечисленное подтверждает замечание профессора С. Ю. Кашкина, который констатирует наличие сложившейся в мире повсеместной цифровой идентификации человека, «которая позволяет собирать, хранить всю политическую, финансово-экономическую, деловую, семейно-конфиденциальную, социально-коммуникативную, медицинскую и любую иную информацию, характеризующую личность и могущую повлиять на ее поведение»[305].

Свобода передвижения как право охватывает возможность свободно перемещаться в пространстве, независимо от ее реализуемости, проживания, профессии, и находить для себя новые места[306]. Свобода передвижения гарантирована статьей 44 Хартии ЕС об основных правах.

Согласно ст. 12 Международного пакта о гражданских и политических правах каждый человек имеет право покинуть любую страну, включая свою собственную, и также въехать в свою собственную страну. Въезд иностранного гражданина на территорию государства может быть ограничен только тогда, когда применяемые ограничения не нарушают международных обязательств в области прав человека, которые характеризуются: защитой от дискриминации, запретом жестокого, бесчеловечного или унижающего достоинство обращения, недопущением вмешательства в семейную жизнь[307]. В качестве примера приведем процедуру выявления преступника на борту авиарейса, которая осуществляется посредством сравнения полученных биометрических данных с уже имеющимися специальными списками и базами данных. Как и любые информационные системы, биометрические системы могут иметь погрешности, что способно повлечь ложную

---

[305] Кашкин С. Ю. Искусственный интеллект и робототехника: возможность вторжения в права человека и правовое регулирование этих процессов в ЕС и мире // Lex Russica. 2019. № 7 (152). С. 151–159.

[306] BVerfG, Urt. v. 16.01.1957 — 1 BvR 253/56 (Elfes) — E 6, 32 (35). См. об этом: Schmidt-Bleibtreu B., Hofmann H., Hopfauf A. Kommentar zum Grundgesetz. 11. Aufl. 2007. Art. 11. Rn. 7 ; Durner in: Grundgesetz Kommentar / begründet von T. Maunz, G. Dürig. Stand: 2010. Art. 11. Rn. 92 ff.

[307] CCPR General Comment No. 15: The Position of Aliens Under the Covenant Adopted at the Twenty-seventh session of the Human Rights Committee, on 11 April 1986 [Электронный ресурс] // URL: https://www.refworld.org/pdfid/45139acfc.pdf (дата обращения: 03.03.2024). Para. 5.

или некорректную идентификацию. Точность биометрических данных и исправная работа биометрических систем играют важную роль для обеспечения права на *свободу передвижения* и недискриминационного распознавания субъекта данных.

Несмотря на то, что биометрические данные являются действительно уникальными и индивидуальными, они могут подвергаться изменениям, связанным с течением времени или иными обстоятельствами (например, старение кожи, пластическая операция и т.д.). Про системы распознавания лиц, использующие биометрические данные, говорят, что они неизбежно несут в себе возможность ошибки, поскольку в их основе лежит статистическая вероятность[308].

Степень погрешности у алгоритмов биометрического распознавания лиц в значительной степени зависит от пола, цвета кожи и возраста человека. В ходе исследований было выявлено, что существующим алгоритмам сложнее распознавать женские лица и они выдают больше ложных отказов и ложных подтверждений для женщин. Помимо этого, они лучше распознают лица со светлым тоном кожи, а показатель ошибок был выше всего для смуглых женских лиц[309]. Это может привести, например, *к дискриминации* темнокожих женщин, поскольку результаты анализа биометрических данных именно этой группы содержат самый большой процент ошибок.

Как справедливо отмечается в концептуальной записке Бюро ОБСЕ по демократическим институтам и правам человека 2021 г., полученные посредством биометрических систем некорректные результаты, связанные с полом, цветом кожи, этнической принадлежностью или другими защищаемыми характеристиками, могут привести к дискриминации и другим серьезным последствиям для лиц, пользующихся транспортом. Могут возникнуть и другие

---

[308] Azria S., Wickert F. Facial Recognition: Current Situation and Challenges. Strasbourg, 13 November 2019 [Электронный ресурс] // URL: https://rm.coe.int/t-pd-2019-05rev-facial-recognitionreport-003-/16809eadf1https://rm.coe (дата обращения: 29.04.2024). P. 15–16.

[309] Buolamwini J., Gebru T. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification [Электронный ресурс] // Proceedings of Machine Learning Research. 2018. Vol. 81. Conference on Fairness, Accountability, and Transparency. URL: http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf (дата обращения: 12.12.2024). P. 1–15. См. также: Grother P., Ngan M., Hanaoka K. NISTIR 8280. Face Recognition Vendor Test (FRVT), Part 3 : Demographic Effects / National Institute of Standards and Technology (NIST), U.S. Department of Commerce. December 2019 [Электронный ресурс] // URL: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf (дата обращения: 29.04.2024).

сложности при пересечении границы, вплоть до невозможности совершить поездку. Все это ставит под угрозу заявленное и гарантированное статьей 26 Международного пакта о гражданских и политических правах и статьей 20 Хартии ЕС об основных правах *равенство* всех людей перед законом и их право на равную защиту закона без какой-либо дискриминации, а также недопустимость дискриминации (ст. 21 Хартии ЕС об основных правах).

Статьей 18 Хартии ЕС об основных правах гарантировано право на убежище «при соблюдении правил Женевской конвенции от 28 июля 1951 г. и протокола от 31 января 1967 г. о статусе беженцев, и в соответствии с Договором, учреждающим Европейское сообщество».

Получение убежища является неотъемлемым правом лица, а его предоставление — международным обязательством государства, впервые прописанным в Женевской конвенции 1951 г. Для стран ЕС из-за открытых границ и свободы передвижения необходим комплексный подход, гарантирующий соблюдение требуемых стандартов защиты беженцев. Процедуры должны быть в то же время справедливыми и эффективными для всего Европейского союза и не допускающими злоупотребления[310].

При подаче ходатайства о предоставлении убежища обязательными требованиями в ЕС являются снятие отпечатков пальцев и снимок лица беженцов и лиц, ищущих убежище. Способ получения таких данных, их хранение и использование могут прямо затрагивать права человека, а также повлечь риски высылки, применения жестокого, бесчеловечного и унижающего достоинство обращения. Как отметил Специальный докладчик ООН по вопросу о современных формах расизма, «в связи со сбором данных в контекстах, характеризующихся очевидным неравенством возможностей, возникают вопросы информированного согласия и способности отказаться»[311]. Отказ от предоставления биометрических

[310] Грнчарова Юст Н. Реализация права на убежище в Европейском союзе // Вестник ОмГУ. Серия «Право». 2015. № 3 (44). С. 191.

[311] Доклад Специального докладчика ООН по вопросу о современных формах расизма, расовой дискриминации, ксенофобии и связанной с ними нетерпимости. UN Doc. A/75/590, 10 ноября 2020 г. Электронный ресурс] // URL: https://undocs.org/en/A/75/590.

данных указанными категориями лиц действительно может быть обусловлен опасениями относительно передачи их данных стране происхождения или недостаточной информированностью обо всех действиях, которые будут совершаться с ними в процессе обработки.

Управление Верховного комиссара ООН по делам беженцев подчеркивает опасность передачи данных лица, ищущего убежище, стране его происхождения, так как человек может быть подвергнут репрессиям после возвращения в страну или его родственники, оставшиеся в стране, могут столкнуться с преследованиями[312].

Риск нарушения перечисленных прав человека при использовании биометрических данных возникает главным образом в связи с пробелами в правовом регулировании обработки специальных категорий данных. При этом, на наш взгляд, такие пробелы не являются случайными в законодательстве ЕС, а напротив, представляют собой правовой инструмент по реализации иных интересов, имеющих явное преимущество перед правами человека.

Обеспечение *права на неприкосновенность частной жизни*, провозглашенного в рассмотренных в гл. II диссертационного исследования источниках международного права, и права на уважение частной жизни в соответствии со ст. 7 Хартии ЕС об основных правах является обязательным условием для обеспечения других прав человека, поскольку нарушение этого права ставит под угрозу множество других прав. Как отмечают исследователи, эти права все чаще подвергаются риску нарушения при использовании биометрических данных, с одной стороны, в связи со стремительным развитием систем искусственного интеллекта, применяемых государственными органами и частными компаниями для биометрической идентификации личности, с другой — ввиду новых вызовов и угроз, с которыми сталкивается человечество в последние годы[313].

---

[312] Addressing Security Concerns without Undermining Refugee Protection — UNHCR's Perspective [Электронный ресурс] // URL: https:// www.refworld.org/docid/5672aed34.html (дата обращения: 29.04.2024). Para. 17.

[313] Правовые и этические аспекты, связанные с разработкой и применением систем искусственного интеллекта и робототехники: история, современное состояние и перспективы развития : монография / В. В. Архипов,

Одним из таких вызовов стали пандемия COVID-19 и меры государств по предупреждению ее распространения[314]. Системы распознавания лиц с применением биометрических технологий послужили удобным инструментом в ряде европейских стран для мониторинга распространения коронавирусной инфекции, а также соблюдения гражданами карантинных мероприятий. Использование таких систем стало возможным в сочетании с другими технологиями, включая тепловизионное изображение с искусственным интеллектом, позволяющее отслеживать граждан, у которых может быть положительный результат теста на COVID-19.

Несмотря на преимущества в отношении возможности контроля стабилизации состояния здоровья общества[315], «использование биометрических данных в ответ на COVID-19 вызывает ряд проблем в области конфиденциальности и безопасности, особенно когда эти технологии используются в отсутствие конкретных указаний или полностью информированного и явного согласия. У субъектов данных также могут возникнуть проблемы с осуществлением широкого спектра основных прав, включая право на доступ к своим личным данным, право на удаление, право на получение информации о целях обработки и о том, кому эти данные передаются»[316].

Пандемический кризис COVID-19, по экспертной оценке[317], является яркой иллюстрацией глобализации дебатов о конфиденциальности данных и необходимости защиты общественного здравоохранения, а законодательная база ЕС по защите данных и конфиденциальности за счет отсутствия жестких правовых

Г. Г. Камалова, Н. Б. Наумов [и др.]. СПб., 2020.

[314] Киселева А. В. Механизмы предупреждения утечки персональных данных при чрезвычайной ситуации в области здравоохранения на примере пандемии коронавирусной инфекции COVID-19 в странах Европы и Азии // Молодой ученый. 2021. № 21 (363). С. 214–217.

[315] Gomez-Barrero M., Drozdowski P., Rathgeb Ch. et al. Biometrics in the Era of COVID-19: Challenges and Opportunities. Jul. 2022 [Электронный ресурс] // URL: https://arxiv.org/pdf/2102.09258.pdf (дата обращения: 29.04.2024).

[316] Organisation for Economic Co-operation and Development (OECD). Tracking and tracing COVID: Protecting privacy and data while using apps and biometrics. Tech. Rep. 2020 [Электронный ресурс] // URL: https://www.oecd.org/en/publications/tracking-and-tracing-covid-protecting-privacy-and-data-while-using-apps-and-biometrics_8f394636-en.html (дата обращения: 30.04.2024).

[317] Communication from the Commission to the European Parliament and the Council «Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition — two years of application of the General Data Protection Regulation», 24.6.2020 [Электронный ресурс] // URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52020DC0264 (дата обращения: 29.04.2024).

рамок, возможности государств — членов ЕС самостоятельно принимать решения, регламентации процедур обработки биометрических данных нормами «мягкого права» оказалась достаточно гибким инструментом, позволяющим разрабатывать практические решения (например, приложения для отслеживания), обеспечивая при этом высокий уровень защиты персональных данных[318].

Поощрение на законодательном уровне применения систем массового наблюдения, нарушающих право на неприкосновенность частной жизни, рискует создать ложное ощущение, что постоянное наблюдение и отслеживание является нормальным и приемлемым в современных реалиях. Как утверждает Комитет Европейского парламента по гражданским свободам, правосудию и внутренним делам (European Parliament Committee on Civil Liberties, Justice and Home Affairs, LIBE), массовое наблюдение не способствует повышению безопасности общества[319]. Оно накладывает неоправданные ограничения на наши свободы и права, которые могут действовать еще долгое время после того, как чрезвычайная ситуация, подобная пандемии COVID-19, будет ликвидирована.

Кроме того, исследования Европейской комиссии в рамках работы над законодательством об искусственном интеллекте[320] показывают, что везде, где действует такая система, можно определять местонахождение лиц, включенных в справочную базу данных, тем самым затрагивая их личные данные, частную жизнь, автономию и достоинство. В этом смысле Управление Италии по защите данных заявило, что автоматизированная обработка биометрических данных для распознавания лиц может представлять собой форму неизбирательного массового наблюдения[321].

---

[318] Карцхия А. А. Тенденции развития правовых институтов под влиянием пандемии: российский и зарубежный опыт // Мониторинг правоприменения. 2021. № 1 (38). С. 10.

[319] European Parliament. Use of smartphone data to manage COVID-19 must respect EU data protection rules. 2020 [Электронный ресурс] // URL: https://www.europarl.europa.eu/news/en/press-room/20200406IPR76604/use-of-smartphone-data-to-manage-covid-19-must-respect- eu-data-protection-rules (дата обращения: 29.04.2024).

[320] European Commission. Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts. 2021 [Электронный ресурс] // URL: https://eurlex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206 (дата обращения: 29.04.2024).

[321] Parliamentary question — E-002182/2021 for written answer E-002182/2021 to the Commission Rule 138 Sophia in ’t Veld (Renew) [Электронный ресурс] // URL: https://www.europarl.europa.eu/doceo/document/E-9-2021-002182_EN.html#def2 (дата обращения: 29.04.2024).

Помимо этого, использование биометрических систем распознавания лиц в данном контексте вызывает серьезные опасения в отношении ряда других гражданских свобод, включая *религиозные свободы*[322] и *права ребенка* как уязвимого лица, заслуживающего более высокого уровня защиты, особенно при использовании в целях охраны правопорядка и пограничного контроля[323], учитывая низкую точность, с которой технология распознает быстро меняющиеся молодые лица.

Обратим внимание на оценку некоторыми зарубежными правоведами положений нового Регламента о Евродак, одной из целей которого является соблюдение прав ребенка при обработке биометрических данных. Отмечается неясность относительно того, предназначены ли все же новые правила Евродак для надлежащего решения вопросов защиты детей или они скорее направлены на обеспечение управления миграцией. «Представляется, что доступ к этим данным довольно широк. Например, правоохранительные органы могут иметь широкий доступ к этим данным, и в то же время не имеется никаких ограничений и никаких фильтров. В связи с этим появляются сомнения, что реальной целью нового акта реально является защита детей. Система разрабатывается не с этой целью... не гарантируется, что способ сбора этих данных будет удобным для детей»[324].

Кроме того, в материалах Комиссии было подчеркнуто, что использование технологий распознавания лиц для обработки изображений лиц, снятых видеокамерами в общественном пространстве, может нарушить *свободу выражения мнений*, гарантированную статьей 19 Международного пакта о гражданских и политических правах и статьей 11 Хартии ЕС об основных правах,

---

[322] Rowe E. Regulating Facial Recognition Technology in the Private Sector // Stanford Technology Law Review. 2021. Vol. 24 (1). P. 31.

[323] European Union Agency for Fundamental Rights. Report 2020. P. 28.

[324] Riedl M. Biometric Borders and Minors' Rights: A critical analysis of European Migration Management under the new Eurodac Regulation. Submission date: 03.07.2024 [Электронный ресурс] // URL: https://docs.yandex.ru/docs/view?tm=1727616757&tld=ru&lang=en&name=Riedl_BA_BMS.pdf&text=Biometric%20Borders%20and%20Minors'%20Rights&url=https%3A%2F%2Fessay.utwente.nl%2F101676%2F1%2FRiedl_BA_BMS.pdf&lr=10715&mime=pdf&l10n=ru&sign=26c6450ac7a2a7c2a500059c6634e28b&keyno=0&nosw=1&serpParams=tm%3D1727616757%26tld%3Dru%26lang%3Den%26name%3DRiedl_BA_BMS.pdf%26text%3DBiometric%2BBorders%2Band%2BMinors%25E2%2580%2599%2BRights%26url%3Dhttps%253A%2F%2Fessay.utwente.nl%2F101676%2F1%2FRiedl_BA_BMS.pdf%26lr%3D10715%26mime%3Dpdf%26l10n%3Dru%26sign%3D26c6450ac7a2a7c2a500059c6634e28b%26keyno%3D0%26nosw%3D1 (дата обращения: 01.09.2024).

и оказать негативное влияние на свободу собраний и объединений, гарантированную пунктом 1 ст. 20 Всеобщей декларации, статьей 21 Международного пакта и статьей 12 Хартии об основных правах.

Аналогичное заключение о негативных последствиях для прав на неприкосновенность частной жизни, свободу выражения мнений и мирных собраний содержится в отчете Совета по правам человека ООН[325].

Практика Суда ЕС и ЕСПЧ

Согласно практике ЕСПЧ защита персональных данных рассматривается как часть права на неприкосновенность частной жизни, которое гарантировано статьей 8 ЕКПЧ. Именно нарушение этой нормы является наиболее часто рассматриваемым вопросом в практике ЕСПЧ при регулировании споров об использовании биометрических данных. Однако, как мы увидим далее, нарушение этого права может влечь за собой нарушение и других прав человека, как в приведенном ниже деле.

Решение ЕСПЧ по делу «Глухин против России» 2023 г.[326] 4 октября 2023 г. ЕСПЧ признал нарушающими ст. 8 ЕКПЧ действия правоохранительных органов г. Москвы в отношении гражданина России Н. Глухина.

В 2019 г. Н. Глухину было предъявлено обвинение в совершении административного правонарушения по ст. 20.2 Кодекса РФ об административных правонарушениях «Нарушение установленного порядка организации либо проведения собрания, митинга, демонстрации, шествия или пикетирования». В обвинении констатировалось, что заявитель провел одиночную демонстрацию на станции метро «Чистые пруды» и непосредственно в поезде метро с использованием «быстро (де)собираемого предмета» (картонной фигуры в натуральную величину и баннера), сопровождающуюся лозунгами в поддержку политического активиста г-на Котова, ранее осужденного по ст. 212.1 Уголовного

[325] Report of the United Nations High Commissioner for Human Rights, Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests. 2020 [Электронный ресурс] // URL: https://www.ohchr.org/en/press-releases/2020/09/un-human-rights-experts-belarus-must-stop-torturing-protesters-and-prevent?LangID=E&NewsID =26199 (дата обращения: 29.04.2024).

[326] Glukhin v. Russia, Application No. 11519/20, Judgment of 4 July 2023.

кодекса РФ «Неоднократное нарушение установленного порядка организации либо проведения собрания, митинга, демонстрации, шествия или пикетирования».

Фиксация факта нарушения и установление личности Н. Глухина были произведены при помощи записей камер видеонаблюдения с системой распознавания лиц Московского метрополитена в рамках Федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности»[327] и Федерального закона от 7 февраля 2011 г. № 3-ФЗ «О полиции»[328].

В силу представленных органами полиции доказательств в виде скриншотов с камер видеонаблюдения Мещанский районный суд г. Москвы признал г-на Глухина виновным и назначил обвиняемому штраф в размере 20 тыс. руб., однако далее дело рассматривалось в Московском городском суде в рамках апелляционной инстанции в связи с доводами обвиняемого, которые характеризовались следующим образом:

— оперативно-розыскные мероприятия, проведенные для установления его личности, были незаконными, поскольку применяемый закон не разрешает проводить такие мероприятия для расследования административных правонарушений. Поэтому полученные таким образом доказательства являются недопустимыми;

— осуждение за мирную одиночную демонстрацию нарушило его право на свободу выражения мнения. Никогда не утверждалось, что такая демонстрация создавала или могла создать какую-либо угрозу общественному порядку или жизни и здоровью других людей.

Впрочем, суд апелляционной инстанции оставил решение без изменения, отметив, что мирный характер демонстрации не имеет значения, поскольку заявитель был осужден за нарушение установленного порядка проведения публичных мероприятий, а именно за непредставление предварительного уведомления. Его сопровождение в полицейский участок и административный арест были законными. Правонарушение было выявлено, и доказательства были

[327] СЗ РФ. 1995. № 33. Ст. 3349.
[328] СЗ РФ. 2011. № 7. Ст. 900.

собраны полицией в соответствии с законодательством РФ.

К обратному решению позднее пришел ЕСПЧ, констатировав, что обработка персональных данных заявителя Н. Глухина в рамках возбужденного против него дела об административном правонарушении, включая использование технологии распознавания лиц, равносильна вмешательству в его право на уважение частной жизни по смыслу ст. 8 ЕКПЧ. Помимо этого, было обращено внимание на то, что «личные данные, раскрывающие политические взгляды, такие как информация об участии в мирных протестах, относятся к специальным категориям чувствительных данных, требующих повышенного уровня защиты. Суд установил, что использование технологии распознавания лиц для идентификации заявителя по фотографиям и видео, а также использование технологии распознавания лиц в реальном времени для его обнаружения и ареста не соответствовало реальной социальной потребности».

В свете всех вышеизложенных соображений Суд пришел к выводу, что использование «крайне интрузивной технологии распознавания лиц в контексте осуществления заявителем его права на свободу выражения мнения, гарантированного ЕКПЧ, несовместимо с ценностями демократического общества, управляемого верховенством закона, которые Конвенция была призвана поддерживать и продвигать. Подобная обработка персональных данных заявителя с использованием технологии распознавания лиц в рамках производства по делу об административном правонарушении не может рассматриваться как необходимая в демократическом обществе и является нарушением ст. 8 ЕКПЧ».

Решение Суда ЕС по делу Министерства труда Болгарии 2023 г.[329] раскрывает главным образом позицию Суда относительно согласия на обработку биометрических данных, а точнее, случаев, когда субъект данных отказывается давать такое согласие, а также впоследствии случаев необходимости принудительного сбора биометрических данных. Также, немаловажно, формируется заключение о возможностях государств-членов на законодательном

[329] C-205/21, Ministerstvo na vatreshnite raboti (Enregistrement de données biométriques et génétiques par la police), Judgment of the Court (Fifth Chamber) of 26 January 2023.

уровне регламентировать такой сбор с учетом определенных целей и условий.

Специализированный уголовный суд Болгарии обратился в Суд ЕС за разъяснением о соответствии болгарского законодательства, предусматривающего обязательное включение в полицейское досье биометрических данных и данных ДНК подозреваемых/обвиняемых, положениям Директивы 2016/680 в свете Хартии ЕС об основных правах.

Разъяснение требовалось в связи с поступившим в Специализированный уголовный суд Болгарии обращением местных правоохранительных органов Болгарии с просьбой дать разрешение на принудительный сбор биометрических данных и данных ДНК обвиняемого по делу о налоговом мошенничестве для формирования досье. Обращение сопровождалось приложениями в виде обвинительного постановления и заявления обвиняемого об отказе от предоставления указанных персональных данных.

Решение Суда ЕС содержало следующие выводы:

1. Ни Директива 2016/680, ни Хартия ЕС об основных правах не препятствуют принятию национального законодательства, согласно которому суд обязан санкционировать обязательный сбор биометрических и генетических данных обвиняемых, даже если на тот момент он еще представляет возможным оценить, имеются ли в действительности разумные основания для подозрений в отношении обвиняемого. Прежде всего обработка биометрических и генетических данных полицейскими органами в целях их следственной деятельности для борьбы с преступностью и поддержания правопорядка должна быть разрешена национальным законодательством при условии, что национальное законодательство содержит достаточно ясную и четкую правовую основу для разрешения такой обработки.

2. Государства-члены должны обеспечить четкое разграничение между данными различных категорий субъектов данных таким образом, чтобы они не подвергались без различия — независимо от категории, к которой они принадлежат, — одинаковой степени вмешательства в их фундаментальное право на защиту персональных данных. Однако это обязательство не является

абсолютным. Кроме того, поскольку в Директиве говорится о категории лиц, в отношении которых имеются серьезные основания полагать, что они совершили уголовное преступление, Суд отмечает, что наличие достаточных доказательств, указывающих на виновность лица, в принципе, является серьезным основанием считать, что оно совершило рассматриваемое преступление. Таким образом, Директива 2016/680 не препятствует принятию национального законодательства, предусматривающего обязательный сбор данных о лицах, в отношении которых собраны достаточные доказательства их виновности в совершении умышленного преступления, подлежащего государственному преследованию, и которые были обвинены по этой причине.

3. Право на презумпцию невиновности также не препятствует обязательству суда санкционировать сбор биометрических данных. Во-первых, сбор данных ограничивается теми лицами, уголовная ответственность которых еще не установлена. Следовательно, этот сбор не может отражать мнение властей о виновности этих лиц. Во-вторых, тот факт, что суд, который должен принять решение о виновности соответствующего лица, не может на этой стадии уголовного процесса оценить, являются ли доказательства, на которых основано обвинение этого лица, достаточными, выступает гарантией соблюдения его права на презумпцию невиновности.

Наряду с этим Суд ЕС постановил, что систематический сбор данных без проверки на соразмерность будет являться незаконным, т.е. Директива 2016/680 не допускает принятия национального законодательства, предусматривающего систематический сбор биометрических и генетических данных любого лица, обвиняемого в совершении умышленного преступления, подлежащего государственному преследованию, без требования к компетентному органу проверить, является ли такой сбор соразмерным. Национальное законодательство должно предусматривать обязанность властей проверять и доказывать, с одной стороны, является ли сбор строго необходимым для достижения конкретных целей, а с другой стороны, могут ли эти цели быть достигнуты с помощью мер, представляющих собой менее серьезное вмешательство в права и свободы субъекта

данных.

В этом контексте Суд ЕС указал, что целью Директивы 2016/680 является обеспечение повышенной защиты чувствительных данных, к которым относятся биометрические и генетические данные, поскольку их обработка может представлять значительный риск для основных прав и свобод. Требование о том, что такая обработка разрешена «только в случае крайней необходимости», должно быть истолковано как установление более строгих условий для законности обработки таких чувствительных данных.

Помимо этого, Судом отмечено, что национальное законодательство, предусматривающее систематический сбор данных у любых лиц, обвиняемых в совершении умышленного преступления, в принципе противоречит этому требованию. Такой подход может привести к неизбирательному сбору данных большинства обвиняемых, поскольку понятие «умышленное уголовное преступление» является очень общим и может быть применено к большому количеству уголовных преступлений, независимо от их характера, тяжести, конкретных обстоятельств этих преступлений, их возможной связи с другими текущими процессами, судимости соответствующего лица или его/ее индивидуальных характеристик.

Еще одно решение, вынесенное в *2024 г. Судом ЕС по запросу Верховного административного суда Болгарии в рамках разбирательства по делу «НГ против Директора Главного управления «Национальная политика» Министерства иностранных дел — София»*[330], отражает две проблемы: соответствия национального законодательства законодательству ЕС и сроков хранения биометрических данных.

В Болгарии в ходе уголовного расследования в полицейские протоколы была внесена запись о том, что свидетель по делу дал ложные показания, в результате чего был привлечен к уголовной ответственности и приговорен к одному году лишения свободы условно. После отбытия наказания он обратился с просьбой

[330] C-118/22, NG v. Direktor na Glavna direktsia «Natsionalna politsia» pri Ministerstvo na vatreshnite raboti — Sofia, Judgment of the Court (Grand Chamber) of 30 January 2024.

исключить его данные из полицейских архивов. Однако согласно болгарскому законодательству, относящиеся к обвиняемому лицу данные хранятся в архивах и подлежат обработке властями, которые имеют к ним доступ, без каких-либо ограничений по времени до наступления смерти лица. Таким образом, ходатайство было отклонено по той причине, что отбывание наказания не является одним из оснований для удаления записи и данных из полицейского архива. После подачи апелляции Верховный административный суд Болгарии передал вопрос на усмотрение Суда ЕС.

В своем решении Суд также постановил, что хранение биометрических и генетических данных лиц, осужденных за умышленное преступление, до момента их смерти противоречит законодательству ЕС.

Суд отмечает, что личные данные, хранящиеся в полицейских протоколах в Болгарии, включают, среди прочего, отпечатки пальцев, фотографию и образец ДНК, взятые для целей профилирования. Эти записи также содержат данные, касающиеся уголовных преступлений, совершенных субъектом данных, и его или ее приговоров в этой связи. Эти данные могут быть важны для проверки причастности субъекта данных к другим уголовным преступлениям, кроме тех, в отношении которых он был осужден окончательным приговором. Однако не все такие лица в перспективе могут быть фигурантами в других уголовных преступлениях, что оправдывает единый срок хранения относящихся к ним данных. Поэтому такие факторы, как характер и тяжесть совершенного преступления или отсутствие рецидива, могут означать, что риск, представляемый осужденным лицом, необязательно оправдывает хранение данных, касающихся этого лица, в полицейских архивах до его смерти. Следовательно, этот срок уместен только в конкретных обстоятельствах, которые должным образом его оправдывают. Иначе обстоит дело, когда он применяется в целом и без разбора к любому лицу, осужденному окончательным приговором за совершение умышленного преступления. Согласно законодательству ЕС, национальное законодательство должно предусматривать обязанность контролера данных периодически проверять, сохраняется ли необходимость в таком хранении, и

предоставлять субъекту данных право на удаление этих данных, если это больше не так.

Решение Суда ЕС по запросу о законности положений Регламента 2019/1157 в рамках разбирательства по делу «РЛ против столицы земли Висбаден (Германия)» 2024 г.[331] касается отказа в выдаче удостоверения личности (ID-карт), не содержащего биометрические данные. Это решение, по нашему мнению, имеет глобальное практическое значение для исследования в сфере биометрических данных, ведь Регламент 2019/1157 был признан недействительным, как соответственно и правовые акты государств-членов, реализующие положения названного Регламента. Как упоминалось ранее, в соответствии с Регламентом в целях повышения безопасности и реализации гражданами ЕС в полной мере права на свободное передвижение удостоверения личности, выданные государствами — членами ЕС, должны содержать изображение лица владельца удостоверения и два отпечатка пальца.

В 2021 г. заявитель по первичному делу «РЛ против столицы земли Висбаден (Германия)» обратился в администрацию города Висбадена с просьбой выдать ему новое удостоверение личности в связи с неисправностью электронного чипа в его старом удостоверении. При этом заявитель просил, чтобы в новом удостоверении не содержалось его биометрических данных (отпечатков пальцев). Городские власти Висбадена отклонили заявление на двух основаниях: во-первых, ввиду имеющегося у заявителя действующего удостоверения (в независимости от исправности/неисправности чипа); во-вторых, ввиду обязательного включения с 2021 г. отпечатков пальцев в носитель информации удостоверения в соответствии с национальным и европейским законодательством.

В том же году заявитель подал иск в Административный суд Висбадена с

[331] C-61/22, Landeshauptstadt Wiesbaden: Judgment of the Court (Grand Chamber) of 21 March 2024 (request for a preliminary ruling from the Verwaltungsgericht Wiesbaden — Germany) — RL v. Landeshauptstadt Wiesbaden (Reference for a preliminary ruling — Regulation (EU) 2019/1157 — Strengthening the security of identity cards of EU citizens — Validity — Legal basis — Article 21(2) TFEU — Article 77(3) TFEU — Regulation (EU) 2019/1157 — Article 3(5) — Obligation for Member States to include two fingerprints in interoperable digital formats in the storage medium of identity cards — Article 7 of the Charter of Fundamental Rights of the European Union — Respect for private and family life — Article 8 of the Charter of Fundamental Rights — Protection of personal data — Regulation (EU) 2016/679 — Article 35 — Obligation to carry out a data protection impact assessment — Maintaining the effects for a certain time of a regulation which has been declared invalid) // OJ. 21.5.2024. C/2024/3129.

требованием вынести постановление, обязывающее администрацию города выдать ему удостоверение личности без сбора отпечатков пальцев.

Впрочем, у Суда появились сомнения в законности двух оснований решения, рассматриваемого в рамках основного производства. Что касается, в частности, второго основания, то Суд склоняется к мнению, что действительность Регламента 2019/1157 может быть оспорена.

Вопросы, поставленные Судом в отношении законности Регламента, касались:

— компетенции ЕС в соответствии с ДФЕС принимать положения об удостоверениях личности;

— нарушения процедуры принятия Регламента, заключающегося в непроведении оценки воздействия обработки персональных данных в соответствии со ст. 35 Регламента о защите данных;

— соответствия п. 5 ст. 3 Регламента ст. 7 и 8 Хартии ЕС об основных правах, касающимся права на уважение частной и семейной жизни и защиты персональных данных.

Относительно последнего Суд ЕС пришел к выводу, что ограничения осуществления прав, гарантированных Хартией, в положениях Регламента отсутствуют. А включение биометрических данных в удостоверения личности является приемлемой и обоснованной мерой в целях минимизации случаев фальсификации документов.

Второй довод также не был поддержан Судом ЕС ввиду того, что сам по себе Регламент предусматривает не проведение каких-либо операций с персональными данными или наборами персональных данных, а лишь выполнение государствами-членами определенных операций по обработке данных в случае подачи заявления на получение удостоверения личности, при этом принятие данного Регламента не было обусловлено проведением оценки воздействия предусмотренных операций по обработке данных в значении п. 1 ст. 35 Регламента о защите данных. Кроме этого, как указал Суд, пункт 1 ст. 35 Регламента не применялся на момент принятия Регламента 2019/1157, поэтому нарушение п. 10 ст. 35 Регламента о защите данных не имеет места.

В части первого довода Суд подчеркнул, что принятие Регламента является одной из мер, подпадающих под действие п. 3 ст. 77 ДФЕС, соответственно, приняв Регламент 2019/1157 на основании п. 2 ст. 21 ДФЕС, законодательный орган ЕС нарушил п. 3 ст. 77 ДФЕС и прибегнул к ненадлежащей законодательной процедуре. Из этого следует, что первое основание недействительности, упомянутое Судом, утверждающим, что Регламент 2019/1157 был принят ошибочно на основании п. 2 ст. 21 ДФЕС и в рамках обычной законодательной процедуры, является таковым, что приводит к недействительности этого Регламента. В соответствии с решением Суда ЕС его действие будет прекращено 31 декабря 2026 г. или в связи с вступлением в силу нового акта, его заменяющего.

ЗАКЛЮЧЕНИЕ

Сегодня биометрические данные являются чувствительной категорией персональных данных, обработка которой оказывает непосредственное влияние на реализацию субъектом основных прав и свобод, что обусловливает необходимость создания специального правового регулирования данной сферы. Однако, прежде чем занять такое положение в системе персональных данных, биометрические данные прошли определенный путь как с технической точки зрения — в прогрессивном развитии, так и с точки зрения правового регулирования.

Несмотря на то что первые разработки международных организаций и региональных объединений в области защиты данных и технических стандартов безопасности, которые заложили основу регулирования биометрических данных, пришлись на 1960-е гг., основным толчком к внедрению по всему миру и в ЕС использования биометрических данных стала международная инициатива по организации мер безопасности с применением биометрических систем в рамках противодействия терроризму.

Постепенное совершенствование биометрических систем позволило человечеству осознать, что биометрические данные можно применять в гораздо более широком спектре. Каждый рассмотренный в диссертационном исследовании этап развития правового регулирования биометрических данных объединяет в себе как нормы, развивающиеся в сферах визового режима, пограничного контроля, полицейского и судебного сотрудничества, так и нормы в области защиты прав человека и персональных данных. Таким образом, права человека на протяжении всего развития норм о биометрических данных пронизывают их и находятся в тесной взаимосвязи с ними.

Анализ международно-правого регулирования вопросов использования биометрических данных позволяет констатировать отсутствие на международном уровне единого подхода к обработке биометрических данных. Международно-правовая основа такого регулирования в большей степени находит проявление в актах общего характера о правах человека, безопасности и защите данных, и лишь

немногие документы международных правительственных организаций содержат специальные нормы о биометрических данных.

Что касается права ЕС, вынуждены утверждать, что главный закон о защите данных ЕС — Регламент 2016/679 — в части регулирования обработки биометрических данных не удовлетворяет современной потребности в особом и внимательном правовом регулировании такой категории данных. Нормы Регламента о защите данных представляются разрозненными, не формирующими общей картины правового регулирования исследуемой категории. Более конкретизированные правила использования биометрических данных содержатся в иных отраслевых актах ЕС, однако они сконцентрированы на достижении отдельных целей, чаще всего обусловленных соображениями безопасности, и носят скорее технический характер, нежели правовой.

Специальный характер регулирования имеют, хоть и очень немногочисленные, акты «мягкого права» как на международном уровне, так и на уровне ЕС. С учетом того, что акты «мягкого права» отчасти выполняют функцию «пред-права», они могли бы заложить основные постулаты качественного правового регулирования биометрических данных.

На наш взгляд, в международном праве и праве ЕС не хватает единого международного стандарта и единого акта ЕС о биометрических данных, которые решили бы изложенные в диссертационном исследовании следующие проблемы.

1. Проблема правовой дефиниции биометрических данных. Сюда же отнесем и проблему содержания биометрических характеристик, которые могут стать в результате специальной технической обработки биометрическими данными.

2. Проблема столкновения интересов общественной безопасности и реализации субъектом биометрических данных основных прав и свобод может быть решена путем конкретизированного подхода к каждому случаю обработки биометрических данных и установления конкретных правил сбора, обработки, хранения таких данных в отдельной сфере.

3. Проблема согласия субъекта, которая заключается в том, что фактически в соответствии с законодательством ЕС на сегодняшний день согласие физического лица не является хотя бы одним из условий обработки биометрических данных. Более того, во многих случаях граждане не имеют возможности отказаться от предоставления и обработки их биометрических данных. Здесь хотелось бы отметить, что российское законодательство сегодня, напротив, оставляет за гражданами право на отказ от предоставления биометрических данных в некоторых случаях. В соответствии с Федеральным законом от 29 декабря 2022 г. № 572-ФЗ «отказ физического лица от прохождения идентификации и (или) аутентификации с использованием его биометрических персональных данных не может служить основанием для отказа ему в оказании государственной, муниципальной или иной услуги, выполнении государственных, муниципальных функций, продаже товаров, выполнении работ или отказа в приеме на обслуживание»[332].

4. Проблема отсутствия унифицированного правового регулирования на территории ЕС ввиду возможности государств-членов вводить на свое усмотрение дополнительные условия обработки биометрических данных или ограничения. Правила обработки биометрических данных должны подлежать строгому и понятному всем участникам отношений правовому регулированию. В праве ЕС не существует практики, в соответствии с которой, например, государства-члены могли бы принимать решения в части применения норм о правах человека: какие права и свободы уважать, а какие гарантии могут уступать реализации иных целей государства и общественности. Такой подход должен быть сформирован и по отношению к специальным (особо чувствительным) категориям персональных данных, таким как биометрические данные, генетические данные или данные о здоровье.

[332] Федеральный закон от 29 декабря 2022 г. № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» // СЗ РФ. 2023. № 1 (ч. I). Ст. 19.

Каждая такая категория персональных данных должна регулироваться отдельным единым актом ЕС, обладающим обязательной юридической силой для всех государств-членов и граждан ЕС и предусматривающим все правовые и содержательные особенности соответствующей категории данных.

Последнее десятилетие, в частности 2024 г., показало, что актуальность применения биометрических систем на основе технологий искусственного интеллекта и биометрических данных в целом только нарастает, в связи с чем в ЕС динамичнее стали приниматься акты, предусматривающие более конкретизированное прямое или частичное регулирование биометрических данных. Их положения, безусловно, основываются на общих требованиях обработки и защиты данных актов ЕС в области прав человека и персональных данных, однако сегментарный характер принятия таких норм не позволяет сформировать эталонное правовое регулирование сферы биометрических данных.

Напомним, что 2024 г. также характеризуется началом пути России к организации собственного миграционного контроля именно посредством использования биометрических данных иностранных граждан и созданием их цифровых профилей, что свидетельствует о положительной практике использования Россией опыта ЕС в миграционной сфере, который имеет успешное применение уже много лет.

В контексте России и существующих практических проблем в опыте ЕС, отдельно от упомянутых выше, отметим особую необходимость в заключении специальных соглашений между Россией и ЕС, регулирующих условия и правила обмена биометрическими данными граждан. Налаживание такого сотрудничества способно сделать взаимодействие правоохранительных органов обоих регионов более эффективным, а порядок двустороннего оформления виз как граждан России, так и граждан государств-членов ЕС для въезда/выезда на территории друг друга – более упрощенным и недискриминационным.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Нормативные правовые акты и иные официальные документы

1.1. Международно-правовые акты

1.1.1. Международные договоры

1. Конвенция о защите прав и достоинства человека в связи с применением достижений биологии и медицины: Конвенция о правах человека и биомедицине (СЕД No. 164). Открыта для подписания 4 апреля 1997 г. в г. Овьедо (Испания).

2. Конвенция о защите прав человека и основных свобод от 4 ноября 1950 г. // СЗ РФ. — 2001. — № 2. — Ст. 163.

3. Конвенция о защите физических лиц при автоматизированной обработке персональных данных (заключена в Страсбурге 28 января 1981 г.) // СЗ РФ. — 2014. — № 5. — Ст. 419.

4. Соглашение «О партнерстве и сотрудничестве, учреждающее партнерство между Российской Федерацией, с одной стороны, Европейскими сообществами и их государствами-членами, с другой стороны» (Agreement on partnership and cooperation establishing a partnership between the European Communities and their Member States, of one part, and the Russian Federation, of the other part) // OJ. — 28.11.1997. — L 327. — P. 1 ; СЗ РФ. — 1998. — № 16. — Ст. 1802.

5. Соглашение между Российской Федерацией и Европейским сообществом об упрощении выдачи виз гражданам Российской Федерации и Европейского союза (г. Сочи, 25 мая 2006 г.) // OJ. — 17.5.2007. — L 129. — P. 27–34 ; СЗ РФ. — 2007. — № 23. — Ст. 2694.

6. Соглашение между Российской Федерацией и Европейским сообществом о реадмиссии (подписано в г. Сочи 25 мая 2006 г.) // OJ. — 17.5.2007. — L 129. — P. 40–60 ; СЗ РФ. — 2007. — № 23. — Ст. 2693.

7. Соглашение о сотрудничестве между Российской Федерацией и Европолом (подписано в Риме 6 ноября 2003 г.) // Бюллетень международных договоров. — 2004. — № 3. — С. 58–62.

8. Agreement between the European Union and the Republic of Belarus on the facilitation of the issuance of visas // OJ. — 9.6.2020. — L 180. — P. 3–18.

9. Agreement between the European Union and the Republic of Peru on the short-stay visa waiver // OJ. — 24.3.2016. — L 78. — P. 4–10.

10. Convention between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands and the Republic of Austria on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration [Электронный ресурс] // Режим доступа: http://www.statewatch.org/media/documents/news/2005/aug/Prum-Convention.pdf.

11. Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community of 13 December 2007 [Электронный ресурс] // Режим доступа: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12007L%2FTXT.

1.1.2. Документы Организации Объединенных Наций

12. Всеобщая декларация о геноме человека и правах человека от 11 ноября 1997 г. Принята на XXIX сессии Генеральной конференции ООН по вопросам образования, науки и культуры [Электронный ресурс] // Режим доступа: https://www.un.org/ru/documents/decl_conv/declarations/human_genome.shtml.

13. Всеобщая декларация прав человека [Электронный ресурс] // Режим доступа: https://www.un.org/ru/documents/decl_conv/declarations/declhr.shtml.

14. Декларация о принципах международного права, касающихся дружественных отношений и сотрудничества между государствами в соответствии с Уставом Организации Объединенных Наций (принята 24 октября 1970 г. Резолюцией 2625 (XXV) на 1883-м пленарном заседании Генеральной Ассамблеи ООН) (Doc. A/RES/2625(XXV)).

15. Замечания общего порядка и общие рекомендации. Замечание общего порядка № 25 о правах детей в связи с цифровой средой. CRC/C/GC/25 [Электронный ресурс] // Режим доступа: https://www.refworld.org/ru/policy/concobservations/crc/2021/ru/146359.

16. Конвенция о правах ребенка (одобрена Генеральной Ассамблеей ООН 20 ноября 1989 г.) (вступила в силу для СССР 15 сентября 1990 г.) // Сборник международных договоров СССР. — 1993. — Вып. XLVI.

17. Резолюция «Использование возможностей безопасных, защищенных и надежных систем ИИ для устойчивого развития» [Электронный ресурс] // Режим доступа: https://ai.gov.ru/.

18. Резолюция, принятая Генеральной Ассамблеей 17 декабря 2018 г. по докладу Третьего комитета (A/73/589/Add.2), 73/179. Право на неприкосновенность частной жизни в цифровую эпоху [Электронный ресурс] // Режим доступа: https://www.un.org/ru.

19. Резолюция, принятая Генеральной Ассамблеей 18 декабря 2013 г. по докладу Третьего комитета (A/68/456/Add.2), 68/167. Право на неприкосновенность личной жизни в цифровой век [Электронный ресурс] // Режим доступа: https://www.un.org/ru.

20. Устав Организации Объединенных Наций (Сан-Франциско, 26 июня 1945 г.) [Электронный ресурс] // Официальный сайт ООН. — Режим доступа: https://www.un.org/ru/about-us/un-charter/full-text.

21. Addressing Security Concerns without Undermining Refugee Protection — UNHCR's Perspective [Электронный ресурс] // Режим доступа: https:// www.refworld.org/docid/5672aed34.html.

22. CCPR General Comment No. 15: The Position of Aliens under the Covenant Adopted at the Twenty-seventh session of the Human Rights Committee, on 11 April 1986 [Электронный ресурс] // Режим доступа: https://www.refworld.org/pdfid/45139acfc.pdf.

23. Letter dated 28 December 2018 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism

addressed to the President of the Security Council. S/2018/1177 [Электронный ресурс] // Режим доступа: https://documents.un.org/doc/undoc/gen/n19/009/63/pdf/n1900963.pdf.

24. Report of the United Nations High Commissioner for Human Rights, Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests, 2020 [Электронный ресурс] // Режим доступа: https://www.ohchr.org/en/press-releases/2020/09/un-human-rights-experts-belarus-must-stop-torturing-protesters-and-prevent?LangID=E&NewsID =26199.

25. Resolution 1373 (2001). Adopted by the Security Council at its 4385th meeting, on 28 September 2001 [Электронный ресурс] // Режим доступа: http://unscr.com/en/resolutions/doc/1373.

26. Resolution 2322 (2016). Adopted by the Security Council at its 7831st meeting, on 12 December 2016 [Электронный ресурс] // Режим доступа: http://unscr.com/en/resolutions/2322.

27. Resolution adopted by the General Assembly 60/288. The United Nations Global Counter-Terrorism Strategy [Электронный ресурс] // Режим доступа: https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/Terr%20ARES60288.pdf.

28. Resolution adopted by the General Assembly on 30 June 2021. The United Nations Global Counter-Terrorism Strategy: seventh review [Электронный ресурс] // Режим доступа: https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/A_RES_75_291_E.pdf.

29. Resolution on the use of biometrics in passports, identity cards and travel documents. 27th International Conference of Data Protection and Privacy Commissioners, Montreux, 2005 [Электронный ресурс] // Режим доступа: https://www.refworld.org/legal/resolution/icdppc/2005/en/42434.

1.1.3. Документы Совета Европы

30. Руководство по распознаванию лиц (T-PD (2020) 03rev4) (принято 28 января 2021 г. Консультативным комитетом Конвенции о защите физических

лиц при автоматизированной обработке персональных данных (Конвенция 108)) // Бюллетень Европейского Суда по правам человека. Российское издание. — 2021. — № 5 (227). — С. 124–133.

31. Committee of Ministers of the Council of Europe, Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector, adopted by the Committee of Ministers on 26 September 1973 at the 224th meeting of the Ministers' Deputies [Электронный ресурс] // Режим доступа: https://pace.coe.int/en/files/14546/html.

32. Committee of Ministers of the Council of Europe, Resolution (74) 29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector, adopted by the Committee of Ministers on 20 September 1974 at the 236th meeting of the Ministers' Deputies [Электронный ресурс] // Режим доступа: https://pace.coe.int/en/files/14546/html.

33. Committee on Bioethics, Opinion on the document of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD) entitled 'Modernisation of Convention 108: new proposals', DH-BIO (2012) 12 final, Restricted, 21.6.2012.

34. Council of Europe, Recommendation 509 (1968) on Human Rights and Modern Scientific and Technological Developments, adopted by the Assembly on 31st January 1968 (16th Sitting) [Электронный ресурс] // Режим доступа: https://pace.coe.int/en/files/14546/html.

1.1.4. Документы Европейского Союза

35. A29WP. Opinion 4/2007 on the concept of personal data (20 June 2007). 01248/07/EN WP 136.

36. A29WP. Working Document on Biometrics (2003) WP 80.

37. Charter of Fundamental Rights of the European Union (Strasbourg, December 12, 2007) (2016/C 202/02).

38. Charter of Fundamental Rights of the European Union // OJ. — 07.06.2016. — C 202. — P. 389–405.

39. COM (2003) 558 final, 24 September 2003.

40. COM (2006) 110 final, 10 March 2006.

41. Commission Decision of 22 September 2006 2006/648/EC laying down the technical specifications on the standards for biometric features related to the development of the Visa Information System (notified under document number C (2006) 3699) //OJ. — 27.9.2006. — L 267. — P. 41–43.

42. Commission Recommendation of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification (notified under document number C(2009) 3200)) // OJ. — 16.5.2009. — L 122. — P. 47–51.

43. Communication from the Commission to the European Parliament and the Council «Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition — two years of application of the General Data Protection Regulation», 24/06/2020 [Электронный ресурс] // Режим доступа: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52020DC0264.

44. Convention determining the state responsible for examining applications for asylum lodged in one of the Member States of the European Communities — Dublin Convention // OJ. — 19.8.1997. — C. 254. — P. 1–12.

45. Council Decision (EU) 2022/1500 of 9 September 2022 on the suspension in whole of the application of the Agreement between the European Community and the Russian Federation on the facilitation of the issuance of visas to the citizens of the European Union and the Russian Federation // OJ. — 9.9.2022. — L 2341. — P. 1–3.

46. Council Decision 2004/512/EC establishing the Visa Information System (VIS) // OJ. — 2004. — L 213/5.

47. Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime // OJ. — 6.8.2008. — L 210. — P. 1–11.

48. Council Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA // OJ. — 07.04.2009. — L 93. — P. 33.

49. Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States // OJ. — 07.04.2009. — L 93. — P. 23.

50. Council Regulation (EC) No. 1030/2002 of 13 June 2002 laying down a uniform format for residence permits for third-country nationals // OJ. — 2002. — L 157/1.

51. 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 // OJ. — 2004. — L 385/1.

52. Council Regulation (EC) No. 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention // OJ. 15.12.2000. L 316. P. 1–10.

53. Council Regulation (EC) No. 334/2002 of 18 February 2002 amending Regulation (EC) No. 1683/95 laying down a uniform format for visas // OJ. — 2002. — L 53/7.

54. Council Regulation (EC) No. 343/2003 of 18 February 2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national // OJ. — 25.2.2003. — L 50. — P. 1–10.

55. Directive (EU) 2016/680 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 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 // OJ. — 4.5.2016. — L 119. — P. 89–131.

56. 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 // OJ. — 23.11.1995. — L 281. — P. 31–50.

57. Doc. 10267/07 (Presse 125) [Электронный ресурс] // Режим доступа: https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/visa-information-system_en.

58. European Commission. Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts. 2021 [Электронный ресурс] // Режим доступа: https://eurlex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

59. European Parliament resolution of 15 September 2022 on human rights violations in the context of the forced deportation of Ukrainian civilians to and the forced adoption of Ukrainian children in Russia (2022/2825(RSP)) // OJ. — 5.4.2023. — C 125. — P. 67–71.

60. European Parliament, Use of smartphone data to manage COVID-19 must respect EU data protection rules. 2020 [Электронный ресурс] // Режим доступа: https://www.europarl.europa.eu/news/en/press-room/20200406IPR76604/use-of-smartphone-data-to-manage-covid-19-must-respect- eu-data-protection-rules.

61. Opinion of the European Committee of the Regions — A New Pact on Migration and Asylum. COR 2020/04843 // OJ. — 7.5.2021. — C 175. — P. 32–68.

62. Opinion of the European Data Protection Supervisor on the Proposal for a Regulation of the European Parliament and the Council amending the Common Consular Instructions on visas for diplomatic missions and consular posts in relation to the introduction of biometrics including provisions on the organisation of the reception and processing of visa applications (COM (2006) 269 final) — 2006/0088 (COD) // OJ. — 29.12.2006. — C 321. — P. 38–44.

63. Parliamentary question — E-002182/2021 for written answer E-002182/2021 to the Commission Rule 138 Sophia in 't Veld (Renew) [Электронный ресурс] // Режим доступа: https://www.europarl.europa.eu/doceo/document/E-9-2021-002182_EN.html#def2.

64. Presidency Conclusions, Thessaloniki European Council, 19–20 June 2003.

65. Proposal for a Regulation of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No. 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624. Brussels, 16.11.2016 COM(2016) 731 final 2016/0357(COD).

66. Proposal for a Regulation of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No. 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], for identifying an illegally staying thirdcountry national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes COM/2016/0272 final/2 — 2016/0132 (COD).

67. Proposal for a Regulation of the European Parliament and of the Council establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person COM/2016/0270 final — 2016/0133 (COD).

68. Proposal for a Regulation of the European Parliament and the Council on asylum and migration management and amending Council Directive concerning the status of third-country nationals who are long-term residents (COM(2020) 610 final).

69. Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108).

70. Recommendation 890 (1980) on the protection of personal data, Parliamentary Assembly of the Council of Europe, Documents 4472 and 4484 [Электронный ресурс] // Режим доступа: https://pace.coe.int/en/files/14546/html.

71. Recommendation No. R (97) 5 on the Protection of Medical Data. Feb. 13, 1997.

72. Regulation (EC) No. 444/2009 of the European Parliament and of the Council of 28 May 2009 amending Council Regulation (EC) No. 2252/2004 on standards

for security features and biometrics in passports and travel documents issued by Member States // OJ. — 6.6.2009. — L 142. — P. 1–4.

73. Regulation (EC) No. 767/2008 of the European Parliament and of the council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation) // OJ. — 13.08.2008. — L218. — P. 0060–0081.

74. Regulation (EC) No. 390/2009 of the European Parliament and of the Council of 23 April 2009 amending the Common Consular Instructions on visas for diplomatic missions and consular posts in relation to the introduction of biometrics including provisions on the organisation of the reception and processing of visa applications // OJ. — 28.5.2009. — L 131. — P. 1–10.

75. Regulation (EC) No. 810/2009 of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas (Visa Code) // OJ. — 15.9.2009. — L 243. — P. 1–58.

76. Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code) // OJ. — 23.3.2016. — L 77. — P. 1–52.

77. 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) // OJ. — 4.5.2016. — L 119. — P. 1–88.

78. Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA // OJ. — 24.5.2016. — L 135. — P. 53–114.

79. Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law

enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No. 767/2008 and (EU) No. 1077/2011 // OJ. — 9.12.2017. — L 327. — P. 20–82.

80. Regulation (EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and amending Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) No. 1077/2011 // OJ. — 21.11.2018. — L 295. — P. 99–137.

81. Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No. 1987/2006 // OJ. — 07.12.2018. — L 312. — P. 14–55.

82. Regulation (EU) 2019/1157 of the European Parliament and of the Council of 20 June 2019 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement // OJ. — 12.7.2019. — L 188. — P. 67–78.

83. Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726 // OJ. — 22.5.2019. — L 135. — P. 1–26.

84. Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA // OJ. — 22.5.2019. — L 135. — P. 27–84.

85. Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information

systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816 // OJ. — 22.5.2019. — L 135. — P. 85–135.

86. Regulation (EU) 2021/1151 of the European Parliament and of the Council of 7 July 2021 amending Regulations (EU) 2019/816 and (EU) 2019/818 as regards the establishment of the conditions for accessing other EU information systems for the purposes of the European Travel Information and Authorisation System // OJ. — 14.7.2021. — L 249. — P. 7–14.

87. Regulation (EU) 2024/1358 of the European Parliament and of the Council of 14 May 2024 on the establishment of 'Eurodac' for the comparison of biometric data in order to effectively apply Regulations (EU) 2024/1351 and (EU) 2024/1350 of the European Parliament and of the Council and Council Directive 2001/55/EC and to identify illegally staying third-country nationals and stateless persons and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, amending Regulations (EU) 2018/1240 and (EU) 2019/818 of the European Parliament and of the Council and repealing Regulation (EU) No 603/2013 of the European Parliament and of the Council // OJ. — 22.5.2024. — L 2024/1358.

88. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No. 300/2008, (EU) No. 167/2013, (EU) No. 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (text with EEA relevance) // OJ. — 12.7.2024. — L 2024/1689.

89. Regulation (EU) 2024/982 of the European Parliament and of the Council of 13 March 2024 on the automated search and exchange of data for police cooperation, and amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, (EU) No 2019/817 and (EU) 2019/818 of the European Parliament and of the Council (the Prüm II Regulation) // OJ. — 5.4.2024. — L 2024/982.

90. Regulation (EU) No. 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No. 767/2008 and (EU) No. 1077/2011 // OJ. — 9.12.2017. — L 327. — P. 20–82.

91. Regulation (EU) No. 604/2013 of the European Parliament and of the Council of 26 June 2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person // OJ. — 29.6.2013. — L 180. — P. 31–59.

92. Regulation (EU) No. 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No. 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast) // OJ. — 29.6.2013. — L 180. — P. 1–30.

93. Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816 // OJ. — 22.5.2019. — L 135.

94. The Schengen acquis — Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union,

the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders // OJ. — 22.09.2000. — L 239. — P. 0019–0062.

95. The Schengen acquis — Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders // OJ. — 22/09/2000. — L 239. — P. 0019–0062.

96. The terms of reference of their mission for 2012–2013, Committee on Bioethics (DH-BIO) Terms of Reference, DH-BIO/INFO (2012) 2.

97. Treaty on European Union // OJ. — 07.06.2016. — C 202. — P. 1–388.

98. Treaty on the Functioning of the European Union // OJ. — 07.06.2016. — C 202. — P. 1–388.

1.1.5. Документы Международной организации гражданской авиации

99. Документ ИКАО Doc 9303. Машиносчитываемые проездные документы. Часть 1: Машиносчитываемые паспорта. Том 1 : Паспорта с машиносчитываемыми данными, хранящимися в формате оптического распознавания знаков. Том 2 : Спецификация на электронные паспорта со средствами биометрической идентификации. — Изд. 6-е. — Монреаль : ИКАО, 2006.

1.1.6. Документы Международной организации по миграции

100. International Organization of Migration. IOM Data Protection Manual [Электронный ресурс] // Режим доступа: https://publications.iom.int/books/iom-data-protection-manual.

101. International Organization of Migration. IOM Data Protection Principles [Электронный ресурс] // Режим доступа: https://www.iom.int/sites/g/files/tmzbdl486/files/documents/2023-08/iom-dp-principles-en.pdf.

1.1.7. Документы Международной организации по стандартизации

102. ISO/IEC 2382-37 (n 24), Term 37.03.21, Definition of biometric sample as: ‘analog or digital representation of biometric characteristics prior to biometric feature extraction’.

1.1.8. Документы Организации экономического сотрудничества и развития

103. OECD Guidelines governing the protection of privacy and transborder flows of personal data [Электронный ресурс] // Режим доступа: https://web-archive.oecd.org/2013-09-06/247725-2013-oecd-privacy-guidelines.pdf.

104. Protecting privacy and data while using apps and biometrics. Organisation for Economic Co-operation and Development (OECD), Tech. Rep., 2020 [Электронный ресурс] // Режим доступа: https://www.oecd.org/coronavirus/policy-responses/tracking-and-tracing-covid-protecting-privacy-and-data-while-using-apps-and-biometrics-8f394636/.

1.2. Нормативные правовые акты и иные официальные документы государств — членов Европейского Союза

1.2.1 Бельгия

105. Act of 3 December 2017 establishing the Data Protection Authority (AH-2022-0020) [Электронный ресурс] // Режим доступа: https://www.autoriteprotectiondonnees.be/publications/opinion-on-preliminary-draft-law-amending-the-act-of-3-december-2017-establishing-the-data-protection-authority.pdf.

1.2.2. Германия

106. Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097), das zuletzt durch Artikel 10 des Gesetzes vom 23. Juni 2021 (BGBl. I. S. 1858; 2022 I 1045) geändert worden ist [Электронный ресурс] // Режим доступа: https://www.gesetze-im-internet.de/bdsg_2018/BJNR209710017.html.

107. Das Datenschutzgesetz des Landes Hessen 7. Oktober 1970.

1.2.3. Испания

108. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales [Электронный ресурс] // Boletín oficial del estado legislación consolidada. — 06.12.2018. — N. 294. — P. 119788–119857. Режим доступа: https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf.

1.2.4. Кипр

109. Law providing for the protection of natural persons with regard to the processing of personal data and for the free movement of such data [Электронный ресурс] // Режим доступа: https://www.dataguidance.com/legal-research/law-125i-2018-providing-protection-natural.

1.2.5. Польша

110. Act of 10 May 2018 on the Protection of Personal Data (the Data Protection Act) ; Act of 21 February 2019 on the amendments of some legal acts in connection with the implementation of the GDPR [Электронный ресурс] // Режим доступа: https://www.dataguidance.com/legal-research/act-10-may-2018-protection-personal-data.

1.2.6. Португалия

111. Lei nº 7/2009, de 12 de fevereiro [Электронный ресурс] // Режим доступа: https://diariodarepublica.pt/dr/detalhe/lei/7-2009-602073.

1.2.7. Словения

112. Personal Data Protection Act (Zakon o varstvu osebnih podatkov, ZVOP-1) [Электронный ресурс] // Режим доступа: https://rm.coe.int/16806af30c.

1.2.8. Франция

113. Act 78-17 on Data Processing, Data Files and Individual Liberties of 6 January 1978 (Data Protection Act) // BGBl. — 1978. — Nº 565.

114. LOI n° 2012-410 du 27 mars 2012 relative à la protection de l'identité // JORF. — N° 0075 du 28 mars 2012. — P. 5604, texte n° 2.

1.2.9. Швеция

115. The Data Act of 11 May 1973.

1.3. Нормативные правовые акты Российской Федерации

116. Федеральный закон от 30 декабря 2021 г. № 441-ФЗ «О внесении изменений в статью 15-3 Федерального закона “Об информации, информационных технологиях и о защите информации” и статьи 3 и 5 Федерального закона “О внесении изменений в отдельные законодательные акты Российской Федерации”» // СЗ РФ. 2022. № 1 (ч. I). Ст. 10.

117. Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» // СЗ РФ. 1995. № 33. Ст. 3349.

118. Федеральный закон от 7 февраля 2011 г. № 3-ФЗ «О полиции» // СЗ РФ. 2011. № 7. Ст. 900.

119. Федеральный закон от 29 декабря 2022 г. № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» // СЗ РФ. 2023. № 1 (ч. I). Ст. 19.

2. Материалы судебной практики

120. BVerfG, Urt. v. 16.01.1957 — 1 BvR 253/56 (Elfes) — E 6, 32 (35).

121. C-106/77, Amministrazione delle Finanze dello Stato v. Simmenthal SpA, ECR [1978] 629.

122. C-11/70, Handelsgesellschaft c. Einfuhr- und Vorratsstelle für Getreide und Futtermittel, 17 December 1970, Rec.

123. C-118/22, NG v. Direktor na Glavna direktsia «Natsionalna politsia» pri Ministerstvo na vatreshnite raboti — Sofia, Judgment of the Court (Grand Chamber) of 30 January 2024.

124. C-139/13, Judgment of the Court (Ninth Chamber) of 13 February 2014 — European Commission v. Kingdom of Belgium // OJ. — 29.3.2014. — C 93. — P. 18–19.

125. C-205/21, Ministerstvo na vatreshnite raboti (Enregistrement de données biométriques et génétiques par la police), Judgment of the Court (Fifth Chamber) of 26 January 2023.

126. C-29/69, Erich Stauder v. City of Ulm — Sozialamt, 12 November 1969.

127. C-293/12 and C-594/12, Digital Rights Ireland of 8 April 2014 [Электронный ресурс] // Режим доступа: https://curia.europa.eu/juris/liste.jsf?num=C-293/12.

128. C-6/64, Costa v. ENEL, ECR [1964] 585.

129. C-6/90 and C-9/90, Francovich and Bonifaci v. Italy, [1991].

130. C-61/22, Landeshauptstadt Wiesbaden: Judgment of the Court (Grand Chamber) of 21 March 2024 (request for a preliminary ruling from the Verwaltungsgericht Wiesbaden — Germany) — RL v. Landeshauptstadt Wiesbaden (Reference for a preliminary ruling — Regulation (EU) 2019/1157 — Strengthening the security of identity cards of EU citizens — Validity — Legal basis — Article 21(2) TFEU — Article 77(3) TFEU — Regulation (EU) 2019/1157 — Article 3(5) — Obligation for Member States to include two fingerprints in interoperable digital formats in the storage medium of identity cards — Article 7 of the Charter of Fundamental Rights of the European Union — Respect for private and family life — Article 8 of the Charter of Fundamental Rights — Protection of personal data — Regulation (EU) 2016/679 — Article 35 — Obligation to carry out a data protection impact assessment — Maintaining the effects for a certain time of a regulation which has been declared invalid) // OJ. — 21.5.2024. — C/2024/3129.

131. C-623/17, Privacy International v. Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service, Secret Intelligence Service, of 6 October 2020 [Электронный ресурс] // Режим доступа: https://gdprhub.eu/index.php?title=CJEU_-_C-623/17_-_Privacy_International_(BCD_case).

132. C-7/90, Criminal proceedings against Paul Vandevenne and others, [1991] ECR I, 4371.

133. Conseil Constitutionnel, Décision no. 2012-652 DC of 22 March 2012, no. 8. — ECLI:FR:CC:2012: 2012.652 DC.

134. Glukhin v. Russia. Application no. 11519/20, Judgment of 4 July 2023.

135. C-22/70, Commission v. Council (ERTA), ECR [1971] 263.

3. Специальная литература

3.1. Учебники, учебные пособия, монографии, статьи на русском языке

136. Абашидзе, А. Х. Правозащитная роль современного международного права в условиях инноваций и широкого применения нанотехнологий / А. Х. Абашидзе // Legal Concept. — 2012. — № 1.

137. Ануфриева, Л. П. Принципы в современном международном праве (некоторые вопросы понятия, природы, генезиса, сущности и содержания) / Л. П. Ануфриева // Московский журнал международного права. — 2021. — № 1.

138. Аппалонова, Н. А. Голосовая биометрия как система развития банковского бизнеса в России / Н. А. Аппалонова, А. В. Какорина // Вестник Университета управления «ТИСБИ». — 2018. — № 3. — С. 170–176.

139. Барковская, Е. Г. Исторические предпосылки и практические потребности интеграции биометрического и криминалистического знания / Е. Г. Барковская // Философия права. — 2010. — № 6.

140. Бекяшев, К. А. Мировое рыболовство: вопросы международного сотрудничества / К. А. Бекяшев, В. Д. Сапронов. — М., 1990.

141. Белая, О. В. Биометрические данные как средство идентификации и аутентификации человека: российский и международный опыт / О. В. Белая, Ю. А. Кицай // Право и практика. — 2020. — № 1.

142. Бирюков, П. Н. О «мягком праве» ЕС / П. Н. Бирюков // Актуальные проблемы современного международного права : материалы XIV Международного конгресса «Блищенковские чтения» : в 2 ч. Москва, 16 апреля 2016 г. Ч. I. — М. : Российский университет дружбы народов (РУДН), 2016. — С. 386.

143. Болл, Р. М. Руководство по биометрии / Р. М. Болл, Дж. Х. Коннел, Ш. Панканти, Н. К. Ратха, Э. У. Сеньор. — М. : Техносфера, 2007.

144. Васякина, Е. В. Правовое регулирование искусственного интеллекта в России и зарубежных странах: от этики к новой парадигме / Е. В. Васякина // Юридический мир. — 2023. — № 11.

145. Васякина, Е. В. Роль Всеобщей декларации прав человека в развитии международного права / Е. В. Васякина // Труды Оренбургского института (филиала) Московской государственной юридической академии. — 2018. — № 37. — С. 11–14.

146. Введение в право Европейского Союза : учеб. для студентов вузов / С. Ю. Кашкин, П. А. Калиниченко, А. О. Четвериков ; под ред. С. Ю. Кашкина. 3-е изд., перераб. и доп. — М. : Эксмо, 2010.

147. Войников, В. В. Право Европейского Союза в практике Европейского Суда по правам человека / В. В. Войников // Международное правосудие. — 2020. — № 1 (33).

148. Войников, В. В. Реформа законодательства Европейского Союза об убежище как ответ на миграционный кризис в Европе / В. В. Войников // Труды Института государства и права РАН. — 2017. — № 5 (63). — С. 149–169.

149. Волеводз, А. Г. Защита персональных данных в Европейском союзе: правовое регулирование и порядок взаимодействия с третьими странами /

А. Г. Волеводз // Библиотека криминалиста. Научный журнал. — 2018. — № 3 (38). — С. 303–312

150. Волеводз, А. Г. Удостоверяющие личность документы с биометрическими персональными данными: международные стандарты, иностранный опыт, отечественное правовое регулирование и его проблемы / А. Г. Волеводз // Ученые записки Санкт-Петербургского имени В.Б. Бобкова филиала Российской таможенной академии. — 2015. — № 1 (53).

151. Грнчарова Юст, Н. Реализация права на убежище в европейском союзе / Н. Грнчарова Юст // Вестник ОмГУ. Серия «Право». — 2015. — № 3 (44).

152. Гуляева, Е. Е. Роль международных организаций в противодействии биотерроризму / Е. Е. Гуляева // Евразийский юридический журнал. — 2023. — № 10 (185). — С. 34-37.

153. Гусенкова, А. А. Применение систем видеонаблюдения и автоматизированных систем биометрической идентификации человека при производстве портретных экспертиз и исследований (на примере аппаратно-программного комплекса «Безопасный город») / А. А. Гусенкова // Вестник Московского университета МВД России. — 2021. — № 6.

154. Двоеносова, Г. А. Биометрия как наука, метод и способ документирования / Г. А. Двоеносова, М. В. Двоеносова // Управление персоналом. — 2009. — № 11.

155. Дубов, А. Б. Правовые парадигмы регулирования исследований и разработок в области человеческого генома и их практического использования в России и за рубежом. Часть I / А. Б. Дубов, П. А. Калиниченко // Вестник Университета имени О.Е. Кутафина (МГЮА). — 2021. — № 7. — С. 61–69.

156. Дьяков, В. Г. Правовое обеспечение геномной безопасности в Европейском Союзе / В. Г. Дьяков, В. В. Ткачук // Международный правовой курьер. — 2020. — № 3–4 (39–40).

157. Европейское право : учебник и практикум для академического бакалавриата / А. И. Абдуллин [и др.] ; под ред. А. И. Абдуллина, Ю. С. Безбородова. — М. : Юрайт, 2018. — 238 с.

158. Иванов, А. И. Биометрическая идентификация личности по динамике подсознательных движений / А. И. Иванов. — Пенза : Изд-во Пенз. гос. ун-та, 2000. — 186 с.

159. Исполинов, А. С. Практика ЕСПЧ в отношении Европейского Союза: некоторые уроки для ЕврАзЭс / А. С. Исполинов // Журнал зарубежного законодательства и сравнительного правоведения. — 2012. — № 3.

160. Калиниченко, П. А. Глобальное и региональное регулирование исследований и разработок в области человеческого генома и их практического использования: особенности предмета и подходов / П. А. Калиниченко // Международный правовой курьер. — 2020. — № 3–4. — С. 20–25.

161. Калиниченко, П. А. Особенности правового регулирования геномных исследований на международном и европейском уровне / П. А. Калиниченко, М. В. Некотенева // Вестник Университета имени О.Е. Кутафина (МГЮА). — 2020. — № 4.

162. Калиниченко, П. А. Принципы прямого действия и верховенства: от права ЕС к праву ЕАЭС / П. А. Калиниченко // Центральная и Восточная Европа: между Евросоюзом и Евразийским экономическим союзом: перспективы соперничества и сотрудничества. — М. ; Люблин, 2019.

163. Калиниченко, П. А. Правовые основы регулирования отношений между Россией и Европейским Союзом : учебное пособие / П. А. Калиниченко. — М. : Университет имени О.Е. Кутафина, 2019.

164. Капустин, А. Я. Право Европейского Союза : учебник для вузов / А. Я. Капустин. — М. : Юрайт, 2019. — 387 с.

165. Карцхия, А. А. Тенденции развития правовых институтов под влиянием пандемии: российский и зарубежный опыт / А. А. Карцхия // Мониторинг правоприменения. — 2021. — № 1 (38).

166. Кашкин, С. Ю. В поисках концепции правового регулирования искусственного интеллекта: платформенные правовые модели / С. Ю. Кашкин, А. В. Алтухов // Вестник Университета имени О.Е. Кутафина (МГЮА). — 2020. — № 4. — С. 26–40.

167. Кашкин, С. Ю. Европейский союз: Основополагающие акты в редакции Лиссабонского договора с комментариями / С. Ю. Кашкин, А. О. Четвериков // СПС «КонсультантПлюс», 2007.

168. Кашкин, С. Ю. Интеграционное право как перспективное направление развития юридической науки и образования / С. Ю. Кашкин // Актуальные проблемы российского права. — 2014. — № 10. — С. 21–52.

169. Кашкин, С. Ю. Искусственный интеллект и робототехника: возможность вторжения в права человека и правовое регулирование этих процессов в ЕС и мире / С. Ю. Кашкин // Lex Russica. — 2019. — № 7 (152). — С. 151–159.

170. Кашкин, С. Ю. Право Европейского союза : учебник для вузов / С. Ю. Кашкин, П. А. Калиниченко, А. О. Четвериков ; под ред. С. Ю. Кашкина. 5-е изд., перераб. и доп. — М. : Юрайт, 2024.

171. Киселева, А. В. Механизмы предупреждения утечки персональных данных при чрезвычайной ситуации в области здравоохранения на примере пандемии коронавирусной инфекции COVID-19 в странах Европы и Азии / А. В. Киселева // Молодой ученый. — 2021. — № 21 (363). — С. 214–217.

172. Колодкин, Р. Л. Критика концепции «мягкого права» / Р. Л. Колодкин // Советское государство и право. — 1985. — № 12. — С. 95–99.

173. Колосов, А. В. Правовое регулирование оборота биометрических данных граждан в Европейском союзе / А. В. Колосов // Сибирский юридический вестник. — 2021. — № 3 (94). — С. 89–96.

174. Корнев, А. В. Информационное право в условиях цифровой трансформации российского права : монография / А. В. Корнев, О. В. Танимов. — М. : Проспект, 2022.

175. Корнев, А. В. Юридическая деятельность в цифровую эпоху: понятие, содержание, формы / А. В. Корнев // Актуальные проблемы российского права. — 2021. — Т. 16. — № 6.

176. Котляр, И. И. Права человека : учебное пособие / И. И. Котляр. — Минск : Право и экономика, 1996.

177. Кривогин, М. С. Особенности правового регулирования биометрических персональных данных / М. С. Кривогин // Право. Журнал Высшей школы экономики. — 2017. — № 2.

178. Кубитович, С. Н. ДНК как носитель информации неограниченного круга лиц / С. Н. Кубитович // Вестник экономической безопасности. — 2017. — № 4.

179. Кутафин, О. Е. Источники конституционного права Российской Федерации / О. Е. Кутафин. — М. : Юристъ, 2002.

180. Кутейников, Д. Л. Неприкосновенность частной жизни в условиях использования систем искусственного интеллекта для удаленной биометрической идентификации личности / Д. Л. Кутейников, О. А. Ижаев, Л. В. Алексеевич, С. С Зенин // Lex Russica. — 2022. — Т. 75. — № 2 (183).

181. Лукашук, И. И. Дипломатические переговоры и принимаемые на них акты / И. И. Лукашук. — М., 2007.

182. Лукашук, И. И. Нормы международного права в правовой системе России / И. И. Лукашук // Журнал российского права. — 2002. — № 3.

183. Магаммедов, М. А. Биометрические данные и банки / М. А. Магаммедов // Цифровая парадигма развития общества: взгляд из будущего : сборник научных трудов по итогам студенческой научно-практической конференции, Саратов, 26 апреля 2019 года / редколлегия: Н. С. Яшин [и др.]. — Саратов : Саратовский социально-экономический институт РЭУ имени Г. В. Плеханова, 2019. — С. 151.

184. Мальцева, Ю. В. Реформирование общей Европейской системы предоставления убежища / Ю. В. Мальцева // Современная Европа. — 2017. — № 4 (76). — С. 121–129.

185. Международное право : учебник / отв. ред. Л. А. Лазутин, Ю. С. Безбородов, М. А. Лихачев. — М. : Норма, 2023. — 656 с.

186. Мовчан, А. П. Кодификация и прогрессивное развитие международного права / А. П. Мовчан. — М., 1972.

187. Молчанов, Н. А. Доктрина информационной безопасности Российской Федерации (новелла законодательства) / Н. А. Молчанов, Е. К. Матевосова // Актуальные проблемы российского права. — 2017. — № 2 (75).

188. Набиев, Р. Ф. Бертильонаж: славное прошлое и возможные перспективы / Р. Ф. Набиев, Э. Э. Горяев // Ученые записки Казанского юридического института МВД России. — 2019. — Т. 4. — № 2 (8).

189. Наумов, В. Б. Персональные данные в соцсетях и социальных медиа: правовые проблемы защиты и использования / В. Б. Наумов // Закон. — 2012. — № 5. — С. 119–125.

190. Никитина, И. Э. Значение Прюмского договора в деле обеспечения обмена криминалистической информацией по уголовным делам в государствах — членах Европейского Союза / И. Э. Никитина, Т. И. Нетрусова, А. Ю. Никитина // Научный портал МВД России. — 2014. — № 4 (28). — С. 132–136.

191. Основы интеграционного права Европейского Союза и Евразийского экономического союза : учебник / отв. ред. Л. М. Энтин, М. Л. Энтин. — М. : Норма, Инфра-М, 2023. — 528 с.

192. Платонова, Н. И. Современный подход к пониманию персональных данных / Н. И. Платонова // Право и современные государства. — 2017. — № 5.

193. Попкова, А. Р. Правовой режим использования биометрических персональных данных при удаленной идентификации физических лиц банками / А. Р. Попкова // Молодой ученый. — 2020. — № 1 (291).

194. Потемкина, О. Ю. Европейский Союз в ожидании Пакта о миграции и убежище / О. Ю. Потемкина // Научно-аналитический вестник Института Европы РАН. — 2020. — № 4.

195. Право Европейского Союза : в 2 ч. : учебник и практикум для бакалавриата и магистратуры / А. Х. Абашидзе [и др.] ; под ред. А. Х. Абашидзе, А. О. Иншаковой. 2-е изд., перераб. и доп. — М. : Юрайт, 2019. — 293 с.

196. Правовые и этические аспекты, связанные с разработкой и применением систем искусственного интеллекта и робототехники: история, современное состояние и перспективы развития : монография / В. В. Архипов,

Г. Г. Камалова, Н. Б. Наумов, А. В. Незнамов, К. Ю. Никольская, Ю. В. Тытюк. — СПб., 2020. — 260 с

197. Рассолов, И. М. Правовое регулирование использования генетической информации в Евросоюзе / И. М. Рассолов, С. Г. Чубукова, И. В. Микурова // Аграрное и земельное право. — 2019. — № 7 (175).

198. Рассолов, И. М. Анализ возможного применения к регулированию отношений по поводу генетической информации институтов персональных данных, личной тайны, врачебной тайны / И. М. Рассолов, С. Г. Чубукова, И. В. Микурова // Lex russica. — 2020. — Т. 73. — № 4.

199. Рассолов, И. М. Интернет-право : учеб. пособие для студентов вузов / И. М. Рассолов. — М. : Юнити-Дана, Закон и право, 2012. — 143 с.

200. Рассолов, И. М. Биометрия в контексте персональных данных и генетической информации: правовые проблемы / И. М. Рассолов, С. Г. Чубукова, И. В. Микурова // Lex russica. — 2019. — № 1.

201. Семенова, Я. В. Формирование правового регулирования использования биометрических данных в Европейском Союзе / Я. В. Семенова // Евразийский юридический журнал. — 2022. — № 8.

202. Синюков, В. Н. Цифровое право и проблемы этапной трансформации российской правовой системы / В. Н. Синюков // Lex Russica. — 2019. — № 9 (154). — С. 9–18.

203. Смирнова, Я. В. Проблемы обеспечения права на охрану частной жизни при обработке биометрических данных в Европейском Союзе / Я. В. Смирнова // Актуальные проблемы российского права. — 2022. — № 10 (143). — С. 183–192.

204. Смирнова, Я. В. Особенности содержания понятия «биометрические данные» в праве Европейского Союза / Я. В. Смирнова // Вестник Университета имени О.Е. Кутафина (МГЮА). — 2021. — № 7.

205. Соколова, Н. А. Международно-правовые аспекты биобезопасности / Н. А. Соколова // Московский журнал международного права. — 2006. — № 1.

206. Степенко, В. Е. Биометрические персональные данные / В. Е. Степенко, А. Д. Богдановская // Евразийский Союз Ученых. — 2020. — № 4-10 (73). — С. 15–19.

207. Тункин, Г. И. Право и сила в международной системе / Г. И. Тункин. — М. : Междунар. отношения, 1983. — 199 с.

208. Федоров, В. Н. Организация Объединенных Наций, другие международные организации и их роль в XXI веке / В. Н. Федоров. — М. : Логос, 2007.

209. Фейсханов, И. Ф. Некоторые аспекты защиты биометрических персональных данных в информационных системах / И. Ф. Фейсханов, Л. Э. Арсланова // Российские регионы в фокусе перемен : сб. докладов XIV Междунар. конф. 2020. — Екатеринбург, 2020. — С. 241–243.

210. Черниченко, С. В. Теория международного права : в 2 т. / С. В. Черниченко. — Т. 1 : Современные теоретические проблемы. — М. : НИМП, 1999.

211. Четвериков, А. О. Правовой режим пересечения людьми внутренних и внешних границ государств — членов Европейского Союза : учебное пособие / А. О. Четвериков ; под ред. С. Ю. Кашкина. — М. : Волтерс Клувер, 2010. — 418 с.

212. Чуркина, Л. М. Конкуренция юрисдикций Европейского суда по правам человека и Суда Европейского Союза / Л. М. Чуркина // Право и практика. — 2023. — № 3.

213. Энтин, Л. М. Лиссабонский договор и реформа Европейского Союза / Л. М. Энтин. // Журнал российского права. — 2010. — № 3 (159).

214. Энтин, Л. М. Право Европейского Союза. Новый этап эволюции: 2009–2017 годы / Л. М. Энтин. — М. : Аксиом, 2009.

215. Энтин, М. Л. Взаимодействие судебных органов (на примере Суда Европейского союза и Европейского суда по правам человека) / М. Л. Энтин, Н. А. Цвейба // Московский журнал международного права. — 2023. — № 3. — С. 84–97.

216. Юмашев Ю. М. Региональная интеграция и международные отношения // Московский журнал международного права. — 2006. — № 1.

3.2. Учебники, учебные пособия, монографии, статьи и иные публикации на иностранном языке

217. Abbott, K. W. Hard and Soft Law in International Governance / K. W. Abbott, D. Snidal // International Organization. — 2000. — Vol. 54.

218. Ashbourn, J. Biometrics: Advanced Identity Verification: The Complete Guide / J. Ashbourn. — London : Springer-Verlag, 2000.

219. Azria, S. Facial Recognition: Current Situation and Challenges. Strasbourg, 13 November 2019 / S. Azria, F. Wickert [Электронный ресурс] // Режим доступа: https://rm.coe.int/t-pd-2019-05rev-facial-recognitionreport-003-/16809eadf1https://rm.coe.

220. Azria, S. Facial Recognition: Current Situation and Challenges. Strasbourg, 13 November 2019 / S. Azria, F. Wickert [Электронный ресурс] // Режим доступа: https://rm.coe.int/t-pd-2019-05rev-facial-recognitionreport-003-/16809eadf1https://rm.coe.

221. Bennett, C. Regulating Privacy: Data Protection and Public Policy in Europe and the United States / C. Bennett. Ithaca, NY : Cornell University Press, 1992. 288 p.

222. Bicskei, H. Violations of Human Rights in Digital Environments / H. Bicskei // Fiat Iustitia. — 2020. — Vol 14. — Issue 10. — P. 43–54.

223. Biometric Security / J. Hu, D. Chek Ling Ngo, A. Beng Jin Teoh (eds). — Newcastle upon Tyne, England : Cambridge Scholars Publishing, 2015.

224. Bodenheimer, E. Jurisprudence. The Philosophy and Method of Law / E. Bodenheimer. — Universal Law Publishing Co Ltd., 2005.

225. Buolamwini, J. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification / J. Buolamwini, T. Gebru [Электронный ресурс] // Proceedings of Machine Learning Research. — 2018. — Vol. 81. — P. 1–15. — Conference on Fairness, Accountability, and Transparency. — Режим доступа: http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

226. Chellappa, R. Advances in Video-Based Biometrics / R. Chellappa, P. Turaga // Advances in Computers. — 2011. — Vol. 83. — P. 183–203.

227. Coleman, N. From Gulf War to Gulf War — Years of Security Concern in Immigration and Asylum Policies at European Level // Terrorism and the Foreigner: A decade of tension around the rule of law in Europe / N. Coleman ; A. Baldaccini, E. Guild (eds). — P. 72–75.

228. Collignon, N. Le consentement aux empreintes génétiques en matière pénale / N. Collignon, O. Diamant-Berger // Médecine et droit. — 2000. — Nº 42.

229. Craig, P. The Evolution of EU Law / P. Craig, G. Burca. — Oxford University Press, 2011.

230. Dimitrova, D. Connecting the dots in the Area of Freedom, Security and Justice (AFSJ) — Part I / D. Dimitrova. — 2017.

231. Durner in: Grundgesetz Kommentar / begründet von T. Maunz, G. Dürig. Stand: 2010.

232. Fournier, N. A. Sex, Ancestral, and Pattern Type Variation of Fingerprint Minutiae: Forensic Perspective on Anthropological Dermatoglyphics / N. A. Fournier, A. H. Ross // American Journal of Physical Anthropology. — 2015. — Vol. 160 (4). — P. 625–632.

233. Gayrel, C. The principle of proportionality applied to biometrics in France: Review of ten years of CNIL's deliberations / C. Gayrel // Computer Law & Security Review. — 2016. — No. 32(3). — P. 450–461.

234. Gellman, R. Privacy and Biometric ID Systems: An Approach Using Fair Information Practices for Developing Countries. CGD Policy Paper 028 / R. Gellman. — Washington DC : Center for Global Development, 2013.

235. Goldsmith, L. French DPA Issues Robust Model Regulation for Biometric Access Controls in the Workplace / L. Goldsmith, M. Pepin [Электронный ресурс] // The National Law Review. — April 24. — 2019. — Vol. XIII. — No. 75. — Режим доступа: https://www.natlawreview.com/article/french-dpa-issues-robust-model-regulation-biometric-access-controls-workplace.

236. Gomez-Barrero, M. Biometrics in the Era of COVID-19: Challenges and Opportunities / M. Gomez-Barrero, P. Drozdowski, Ch. Rathgeb et al. — Jul. 2022 [Электронный ресурс] // Режим доступа: https://arxiv.org/pdf/2102.09258.pdf.

237. Gonçalves, M. E. Does the Centrality of Values in the Lisbon Treaty Promise More Than It Can Actually Offer? EU Biometrics Policy as a Case Study / M. E. Gonçalves, M. I. Gameiro // European Law Journal. — 2014. — Vol. 20 (1). — P. 21–33.

238. Grother, P. NISTIR 8280. Face Recognition Vendor Test (FRVT), Part 3 : Demographic Effects / P. Grother, M. Ngan, K. Hanaoka ; National Institute of Standards and Technology (NIST), U.S. Department of Commerce. — December 2019 [Электронный ресурс] // Режим доступа: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

239. Hillenberg, H. A Fresh Look at Soft Law / H. Hillenberg // European Journal of International Law. — 1999. — No. 10. — P. 499–515.

240. Jasserand, C. Legal Nature of Biometric Data: From 'Generic' Personal Data to Sensitive Data / C. Jasserand // European Data Protection Law Review. — Vol. 2 (2016). — Issue 3. — P. 297–311

241. Jefferson, R. B. Biometrics: Privacy, Progress and Government / R. B. Jefferson. — New York : Nova Science Publishers, Inc., 2010.

242. Jefferson, R. B. Biometrics: Privacy, Progress and Government / R. B. Jefferson. — New York : Nova Science Publishers, Inc., 2010.

243. Kindt, E. J. Having Yes, Using No? About the New Legal Regime for Biometric Data / E. J. Kindt // Computer Law & Security Review. — 2018. — Vol. 34. — No. 3. — P. 523–538.

244. Kindt, E. Privacy and Data Protection Issues of Biometric Applications: A Comparative Analysis / E. Kindt. — Springer, 2013.

245. Kotschy, W. Article 2, Directive 95/46/EC / W. Kotschy // Concise of European IT law / A. Büllesbach, S. J. H. Gijrath, Y. Poullet, J. E. J. Prins (eds). — Kluwer Law International, 2010.

246. Liu, N. Y. Bio-Privacy: Privacy Regulations and the Challenge of Biometrics / N. Y. Liu. — N.Y., 2012.

247. López-Lapuente, L. Spain / L. López-Lapuente // The Privacy, Data Protection and Cybersecurity Law Review. — London : Law Business Research Ltd., 2022. — P. 372–386.

248. Mordini, E. Second Generation Biometrics: The Ethical, Legal and Social Context / E. Mordini. — N.Y., 2012.

249. Newbold, R. Newbold's Biometric Dictionary for Military and Industry / R. Newbold. 2nd ed. — NY : Authorhouse, 2008. — 236 pp.

250. Peers, S. EU Justice and Home Affairs Law / S. Peers. — 2nd ed. — Oxford University Press, 2006.

251. Quinn, P. The Difficulty of Defining Sensitive Data — The Concept of Sensitive Data in the EU Data Protection Framework / P. Quinn // German Law Journal. — 2021. — No. 22 (8). — P. 1583–1612.

252. Riedl, M. Biometric Borders and Minors' Rights. A critical analysis of European Migration Management under the new Eurodac Regulation / M. Riedl. — Submission date: 03.07.2024 [Электронный ресурс] // Режим доступа: https://docs.yandex.ru/docs/view?tm=1727616757&tld=ru&lang=en&name=Riedl_BA_BMS.pdf&text=Biometric%20Borders%20and%20Minors'%20Rights&url=https%3A%2F%2Fessay.utwente.nl%2F101676%2F1%2FRiedl_BA_BMS.pdf&lr=10715&mime=pdf&l10n=ru&sign=26c6450ac7a2a7c2a500059c6634e28b&keyno=0&nosw=1&serpParams=tm%3D1727616757%26tld%3Dru%26lang%3Den%26name%3DRiedl_BA_BMS.pdf%26text%3DBiometric%2BBorders%2Band%2BMinors%25E2%2580%2599%2BRights%26url%3Dhttps%253A%2F%2Fessay.utwente.nl%2F101676%2F1%2FRiedl_BA_BMS.pdf%26lr%3D10715%26mime%3Dpdf%26l10n%3Dru%26sign%3D26c6450ac7a2a7c2a500059c6634e28b%26keyno%3D0%26nosw%3D1.

253. Robilant A. di. Genealogies of Soft Law / A. di Robilant // The American Journal of Comparative Law. — 2006. — Vol. 54.

254. Rowe, E. Regulating Facial Recognition Technology in the Private Sector / E. Rowe // Stanford Technology Law Review. — 2021. — Vol. 24 (1).

255. Schmidt-Bleibtreu, B. Kommentar zum Grundgesetz / B. Schmidt-Bleibtreu, H. Hofmann, A. Hopfauf. — 11. Aufl. — 2007.

256. Shelton, D. Normative Hierarchy in International Law / D. Shelton // American Journal of International Law. — 2006. — April. — Vol. 100. — No. 2.

257. Shelton, D. Normative Hierarchy in International Law / D. Shelton // American Journal of International Law. — 2006. — April. — Vol. 100. — No. 2.

258. Smith, M. The ethical application of biometric facial recognition technology / M. Smith, S. Miller // Ai & Society. — 2022. — Vol. 37 (1). — P. 167–175.

259. Sperry, B. P. Genetic Fingerprints and National Security / B. P. Sperry, M. Allyse, R. R. Sharp // American Journal of Bioethics. — 2017. — Vol. 17 (5). — P. 1–3.

260. Vavoula N. The Establishment of ECRIS-TCN. In Immigration and Privacy in the Law of the European Union (Chapter 7) / N. Vavoula. — Leiden, The Netherlands : Brill, 2022.

261. Waldmann Agarwal, M. A. Biometric Information — A Brave New World of Regulatory Compliance / M. A. Waldmann Agarwal, A. J. Fleisher. — Morrison Foerster, 2017.

262. Whitson, S. Kuwait: New counterterror law sets mandatory DNA testing / S. Whitson. — Human Rights Watch, 2015.

3.3. Диссертации и авторефераты диссертаций

263. Велижанина, М. Ю. «Мягкое право»: его сущность и роль в регулировании международных отношений : дис. … канд. юрид. наук : 12.00.10 / Велижанина Марина Юрьевна. — М., 2007.

264. Вельдер, И. А. Система правовой защиты персональных данных в Европейском Союзе : дис. ... канд. юрид. наук : 12.00.10 / Илья Александрович Вельдер. — Казань, 2006. — 143 с.

265. Вельдер, И. А. Система правовой защиты персональных данных в Европейском Союзе : автореф. дис. ... канд. юрид. наук : 12.00.10 / Илья Александрович Вельдер. — Казань, 2006.

266. Галяшина, Е. И. Теоретические и прикладные основы судебной фоноскопической экспертизы : дис. … докт. юрид. наук : 12.00.09 / Галяшина Елена Игоревна. — Воронеж, 2002. — 478 с.

267. Галяшина, Е. И. Теоретические и прикладные основы судебной фоноскопической экспертизы : автореф. дис. ... докт. юрид. наук : 12.00.09 / Галяшина Елена Игоревна. — Воронеж, 2002.

268. Калиниченко, П. А. Правовое регулирование отношений между Россией и Европейским Союзом : дис. … докт. юрид. наук : 12.00.10 / Калиниченко Пауль Алексеевич. — М., 2011.

269. Просветова, О. Б. Защита персональных данных : дис. ... канд. юрид. наук : 05.13.19 / Просветова Ольга Борисовна. — Воронеж, 2005.

270. Четвериков, А. О. Правовое регулирование либерализации трансграничных отношений : опыт Европейского Союза : дис. ... докт. юрид. наук : 12.00.10 / Четвериков Артем Олегович. — М., 2010. — 518 с.

271. Шадрин, С. А. Правовое регулирование защиты персональных данных в Европейском союзе: генезис и перспективы развития : автореф. дис. ... канд. юрид. наук: 12.00.10 / Шадрин Станислав Александрович. — Казань, 2019. — 35 с.