Правоведение

УДК 342.7

В.В. Архипов, В.Б. Наумов

ТЕОРЕТИКО-ПРАВОВЫЕ ВОПРОСЫ ОХРАНЫ ПРАВ ЧЕЛОВЕКА ПРИ ИСПОЛЬЗОВАНИИ БИОМЕТРИЧЕСКИХ ДАННЫХ СИСТЕМАМИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: ЕВРОПЕЙСКИЙ ОПЫТ[1]

В статье рассматриваются теоретические вопросы формирования правовых механизмов охраны прав человека, включая право на неприкосновенность частной жизни, в современных условиях цифровой трансформации. В работе на основе методов сравнительного правоведения исследованы правовые риски цифровизации в аспекте использования биометрических данных программными решениями и устройствами на базе технологии искусственного интеллекта. В результате проведенного исследования для повышения экономической эффективности технологий при одновременном обеспечении прав граждан с учетом растущего потенциала высоко персонализированного манипулирования и иных рисков технологии обработки биометрических персональных данных авторы приходят к выводам о значительных вызовах для права. Это усиливает значение выработки основных этических и правовых принципов в области искусственного интеллекта и формирования законодательной базы в сфере искусственного интеллекта.

Ключевые слова: теория государства и права, теоретические основы цифровизации, права человека, неприкосновенность частной жизни, правовые риски, сравнительно-правовое исследование, цифровые технологии, цифровая трансформация, идентификация субъектов, биометрические данные, искусственный интеллект.

DOI: 10.35634/2412-9593-2022-32-1-109-118

Современные условия цифровизации оказывают трансформирующее влияние на все сферы жизни общества, государства и человека, одновременно меняя не только понимание многих концептов права, но и сами правовые ценности. Вместе с тем указанное развитие не носит и не может носить линейный характер. Предлагаемые цифровые технологии и результаты их использования, имея высокую социально-экономическую эффективность и востребованность, подвергаются оценке научным сообществом в части пределов их применения с учетом соблюдения общепризнанных прав и свобод человека. При этом права человека, с одной стороны, сами эволюционируют под воздействием всеобщей цифровой трансформации, что сегодня отмечается и исследуется учеными и специалистами. С другой стороны, права и свободы человека образуют содержание пределов вмешательства цифровых технологий в частную жизнь лица. Особенно явно такая дихотомия проявляется при разработке, внедрении и применении систем искусственного интеллекта и робототехнике, использующих при своем функционировании такие чувствительные данные, как биометрические персональные данные. Указанное требует осмысления как с позиции теории права, так и отраслевых наук, важное место среди которых в предметном исследовании занимают положения международного, гражданского, административного и информационного права.

Учитывая незначительный опыт правового регулирования рассматриваемых вопросов в России и иных юрисдикциях, полагаем, что исследование теоретических вопросов охраны прав человека при использования биометрических данных системами искусственного интеллекта целесообразно основывать на методах сравнительного правоведения. Следует отметить, что исследования взаимосвязанных вопросов проводились, включая эволюцию прав человека в условиях цифровой трансформации, внедрения искусственного интеллекта [1-4 и др.], правовой охраны биометрических данных [5; 6 и др.], научных работ вопросов правовой охраны прав человека при использовании биометрических данных программных решений и устройств на базе искусственного интеллекта все еще достаточно немного [7]. В связи с этим для совершенствования российского законодательства, регулирующего применение цифровых технологий, необходимо провести сравнительно-правовое исследование теоретических ас-

[1] Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-29-16015 «Комплексное исследование правовых и этических аспектов, связанных с разработкой и применением систем искусственного интеллекта и робототехники».

пектов влияния на право человека использовать биометрические данные при разработке и применении систем искусственного интеллекта и устройств на базе данной технологии.

Научный интерес в части использования биометрических персональных данных представляет зарубежный и особенно европейский опыт правового регулирования. В этом контексте европейский опыт отличает системность в части следования основным ценностным посылкам, которая в том числе отражается в результатах деятельности CAHAI, о которых будет сказано далее. При этом, вполне закономерно, что исходная ценностная парадигма, лежащая в основе европейского подхода, выражена в Европейской Конвенции о защите прав человека и основных свобод (далее – ЕКПЧ) [8], и конкретно в ст. 8 ЕКПЧ, согласно ч. 1 которой «каждый имеет право на уважение его личной и семейной жизни, его жилища и корреспонденции» (при этом ч. 2 данной статьи ограничивает возможности вмешательства публичных властей в осуществление этого права). Будучи сформулированной в период, когда правовое регулирование отношений по поводу обработки персональных данных, тем более биометрических и тем более с применением технологий искусственного интеллекта, еще не составляло часть актуальной политико-правовой повестки, положения данной статьи в настоящее время толкуются расширительно – они распространяются и на систему соответствующих правоотношений в цифровой среде. Для практики Европейского суда по правам человека характерно рассмотрение спорных вопросов, связанных с процессами обработки биометрических персональных данных именно в свете данной статьи [9]. Еще одним источником, который следует упомянуть в данном контексте, является Хартия Европейского союза об основных правах [10]. Данная Хартия (также в ст. 8) прямо ориентирована на защиту персональных данных, причем в ее тексте используется именно аутентичный термин «персональные данные» (“personal data”). Конкретно указывается, что каждый имеет право на защиту относящихся к нему или к ней персональных данных, что такие данные должны обрабатываться справедливо для определенных целей на основе согласия или иного установленного законом основания, причем каждый имеет право доступа к собранным данным и их исправлениям, а соблюдение данных требований должно контролироваться независимым органом власти.

Для европейских стран и стран СНГ, включая Россию, основы модели защиты персональных данных (которую условно можно охарактеризовать как «европейскую» с учетом приводимого основного источника) были заложены в Конвенции о защите физических лиц при автоматизированной обработке персональных данных [11], редакция которой была обновлена в 2018 г. Государства-члены Конвенции обязаны имплементировать положения в национальное право [12], примером чего и является Федеральный закон «О персональных данных». В то же время данный закон является и примером того, что на национальном уровне возможны значительные вариации в деталях регулирования отношений по поводу персональных данных, в первую очередь относящихся к различным особым видам, в том числе к биометрическим персональным данным. Собственно говоря, именно обилие различий, возникающих на уровне имплементации положений указанной Конвенции, выступило одним из главных обстоятельств, которые обусловили принятие Общего регламента о защите персональных данных в Европейском Союзе, о котором пойдет речь далее. Кроме того, говоря о европейской модели защиты персональных данных как она реализована в Европейском Союзе, нельзя обойти вниманием и Директиву 2002/58/ЕС от 12.07.2002 «Об обработке персональных данных и защите информации о частной жизни в сфере электронных коммуникаций» [13]. Данной Директивой установлены отдельные специальные требования, действующие при обработке персональных данных для целей электронной коммерции. В перспективе данный акт должен быть заменен на более актуальный Регламент [14].

Рассматривая европейское регулирование в сфере использования биометрии и учитывая тренды цифровизации нельзя не упомянуть проект Регламента о гармонизации регулирования искусственного интеллекта и внесения изменений в ряд нормативно-правовых актов Европейского союза [15]. Предполагается, что этот Регламент станет актом, обеспечивающим общую нормативную основу для отношений по поводу применения технологий искусственного интеллекта, подобно тому, как Общий регламент о защите персональных данных поспособствовал гармонизации правил, касающихся обработки персональных данных. В числе целей документа было закрепление конкретных правил защиты физических лиц при использовании искусственного интеллекта для удаленной биометрической идентификации (в том числе в режиме реального времени в общедоступных местах). Полагаем, что с логикой общей направленности подобных изменений можно было бы согласиться, поскольку, как минимум, в отличие от непосредственной (против удаленной) идентификации в отложенном режиме (против режима реального времени), противоположный способ, действительно, по очевидным при-

чинам предполагает более высокий риск для нарушения прав человека – хотя бы потому, что отсутствует возможность быстро и непосредственно выразить возражения против определенных аспектов процедуры. В то же время сам проект Регламента был подвергнут критике, однако основанием для такой критики как раз и выступил указанный вид идентификации [16]. Отметим, что данное обстоятельство в целом наглядно иллюстрирует различие в подходах к идентификации посредством биометрических данных (что невозможно сделать в современных условиях без использования технологий искусственного интеллекта) в рамках европейской модели, как она реализована в Европейском Союзе и в других странах, которые допускают определенный отход от такой модели (в то же время критическое отношение к удаленной биометрической идентификации с использованием искусственного интеллекта, как известно, сохраняется и в США, для которых в общем не характерно следование общей европейской модели защиты персональных данных, что можно считать достаточно примечательным обстоятельством).

Критический подход к использованию биометрических персональных данных для целей удаленной идентификации (как и для других чувствительных целей) определяется самой природой этих данных и связанными с ними повышенными рисками для прав человека. Среди прочего, такие риски выражаются в том обстоятельстве, что биометрические данные в большинстве случаев принципиально нельзя изменить (или же их нельзя изменить способом, который был бы «пропорциональным» по отношению к рискам). Именно этот факт прямо или косвенно отражается в известных определениях биометрических персональных данных. Полагаем, что в сравнительно-правовом аспекте будет уместно обратиться к позиции, отраженной в документе 4/2007 «О концепции персональных данных» рабочей группы по защите данных (Data Protection Working Party) [17]. Как следует из указанного подхода, биометрические данные должны пониматься как «биологические свойства, физиологические характеристики, черты характера, привычки, когда эти свойства/действия являются уникальными для конкретного субъекта и которые можно эмпирически наблюдать, даже если измерение показателей может носить вероятностный характер. К типичным примерам биометрических данных относятся отпечатки пальцев, сетчатка глаза, структура лица, голос, геометрия руки, рисунок вен или даже некоторые глубоко укоренившиеся навыки или другие поведенческие характеристики (например, рукописная подпись, манера нажатия клавиш, особая походка или манера речи и т. д.)». Рабочая группа подчеркнула двойственность биометрических персональных данных – это и информация о конкретном лице, и определенная характеристика той связи, которая существует между соответствующей информацией и конкретным субъектом. В этом контексте актуальным также является вопрос о правовой природе биоматериалов, которые также, как кажется на первый взгляд, имеют двойственную природу, выступая либо в качестве своего рода вещи-носителя информации, либо в качестве специфического феномена, в котором качества материального носителя вроде бы могут быть и неотделимы от информации как таковой (как бы абсурдно это ни звучало с точки зрения здравого смысла, такая постановка вопроса возможна в качестве предварительной гипотезы в рассуждении с использованием метода, собственно говоря, *reductio ad absurdum*). Исследуя эту проблему, рабочая группа заняла позицию, согласно которой те же образцы тканей человека – это все же носители информации, однако сама информация, разумеется, является персональными данными.

Основным актом, устанавливающим общие, унифицированные правила в части обработки всех категорий персональных данных, на уровне Европейского Союза (точнее, Европейской экономической зоны) является Общий регламент о защите персональных данных (далее – «GDPR») [18], который заменил действующую с 1995 г. Директиву 95/46/ЕС «О защите прав физических лиц применительно к обработке персональных данных и о свободном движении таких данных» [19]. GDPR определяет основные положения, касающиеся обработки персональных данных, которые включают в себя, среди прочего, общие положения, включая определения, принципы обработки персональных данных (в значительной степени совпадающие с установленным российским законодательством), права субъектов данных, отдельные правила, касающиеся в том числе обязанностей контролера и обработчика данных, экспорта данных, роли надзорных органов и пр. Большинство из этих положений применимы и к биометрическим персональным данным, и к тем случаям, когда биометрические персональные данные используются для целей идентификации с использованием технологий искусственного интеллекта. Причина проста – законодательство о персональных данных в рамках европейской модели технически нейтрально (по большей части, хотя и ориентировано, прежде всего, на то, что в российской правовой системе называется автоматизированной обработкой персональных данных), а

значит одни и те же принципы и правила должны применяться как в случаях использования технологий искусственного интеллекта, так и в иных случаях. Это не отменяет того факта, что в национальных законодательстве и практике отдельных государств Европы могут быть различные специфические региональные правила, касающиеся использования искусственного интеллекта как в целом, так и конкретно в области обработки биометрических персональных данных, но общие положения GDPR при этом все равно являются принципиальными. Особенное значение имеет само нормативное определение биометрических персональных данных. Как следует из ст. 4 (14) GDPR, под биометрическими данными понимаются персональные данные, возникающие в результате особой технической обработки данных о физических, физиологических или поведенческих характеристиках физического лица, предусматривающих или подтверждающих его уникальную идентификацию. Это уже отличает определение, данное GDPR, от известных определений, в том числе от российского: так, в последнем отсутствует указание на «поведенческие характеристики» и на «уникальность идентификации». Этим, однако, особые общие правила, релевантные контексту исследования, не ограничиваются. Среди прочего, GDPR устанавливает специальные требования на тот случай, если происходит масштабная обработки специальных категорий данных (включая биометрические данные), когда используются новые технологии либо при высоком риске для прав и свобод физических лиц. Как следует из ст. 35 GDPR, контролер данных (то есть оператор персональных данных, если использовать аналогичное понятие из российского законодательства) должен оценить воздействие на защиту данных, проведя анализ процессов и целей их обработки, оценив соблюдение принципа пропорциональности, риски нарушения прав субъектов данных и т.п.

При этом в контексте данного рассуждения необходимо подчеркнуть закономерность, которая отражается на уровне нормативно-правового регулирования многих юрисдикций (включая собственно Европейский Союз и Великобританию): исследуемый предмет регулирования подразумевает соединение двух изначально отдельных направлений нормативного регулирования – отношений по поводу обработки персональных данных и отношений по поводу применения технологий искусственного интеллекта. Таким образом, при анализе соответствующих примеров необходимо учитывать эту практическую двойственность. При этом данное обстоятельство уже учитывается в ряде проектов, соответствующих нормативных актов, что приводит к интеграции подходов. Так, в частности, в проекте «Регламента Европейского Парламента и Совета, устанавливающего согласованные правила по искусственному интеллекту (Акт об искусственном интеллекте) и вносящем изменения в некоторые законодательные акты Союза» [20], собственно вводится понятие «системы удаленной биометрической идентификации» (remote biometric identification system), причем этот термин используется для описания «системы искусственного интеллекта, предназначенной для идентификации физических лиц на расстоянии путем сравнения биометрических данных человека с биометрическими данными, содержащимися в справочной базе данных, и без предварительного знания о том, будет ли определенное лицо присутствовать в определенном месте, и может ли оно быть идентифицировано, независимо от конкретной технологии, процессов или типов используемых биометрических данных». Подчеркнем две составляющих этого понятия – «удаленная система биометрической идентификации в режиме реального времени» (real time remote biometric identification system) и «удаленная система последующей биометрической идентификации» (post-remote biometric identification system). Значение этих понятий не выходит за рамки устоявшегося словоупотребления, а на уровне данного акта предлагается ввести общий запрет на применение первого вида систем в общественных местах для целей правоприменения, кроме случаев получения прямого и конкретного разрешения от судебного органа или от независимого административного органа государства-члена ЕС. В то же время, в силу особенностей европейского подхода, судьба удаленной биометрической идентификации в странах Европейской экономической зоны все же пока остается неопределенной.

Отмеченные сомнения определяются предсказуемой ценностной позицией. Так, например, в совместной позиции Европейского инспектора по защите данных и Европейского совета по защите данных 5/2021 по поводу проекта Постановления Европейского Парламента и Совета, устанавливающего гармонизированные правила об искусственном интеллекте (Закон об искусственном интеллекте) [21], отмечаются возникающие в связи с массовым сбором данных угрозы демократическому режиму и правам человека. Позиция призывает к «общему запрету на любое использование искусственного интеллекта для автоматизированного распознавания человеческих черт в общедоступных местах – например, лиц, а также походки, отпечатков пальцев, ДНК, голоса, манеры нажатия клавиш

и других биометрических или поведенческих сигналов – в любом контексте». Среди дополнительных предложений отмечается введение запрета на использование систем искусственного интеллекта, если посредством обработки биометрических данных система классифицирует людей по таким категориям как раса, гендер, политические или сексуальные предпочтения (независимо от того, используется ли система частными компаниями или государственными органами). Также высказывается идея ввести запрет на использование систем искусственного интеллекта, научная обоснованность деятельности которых не доказана или противоречит основным ценностям Европейского Союза. Среди прочего это подразумевает запрет и на «биометрическую категоризацию» субъектов.

Как видно, особое внимание уделяется вопросам возможной дискриминации при использовании биометрической идентификации. Так, в частности, в Резолюции Европейского парламента от 06.10.2021 «Об искусственном интеллекте в уголовном праве и его использовании полицией и судебными органами в уголовных делах» (2020/2016(INI)) [22] указано, что значительное число систем, построенных на алгоритмах, при идентификации допускают ошибки, связанные с идентификацией субъектов, относящихся к различным меньшинствам, непропорционально часто, при том, что граждане не только не должны страдать от подобных ошибок, но и в принципе иметь возможность не подвергаться процедурам идентификации, кроме случаев, когда законом не установлено изъятие из этого правила для убедительных и законных публичных интересов (п.9). Кроме того, Парламент призывает к постоянному запрету использования автоматизированного анализа или же распознавания человека в публично доступных местах по другим специфическим особенностям, в число которых входит: походка, отпечатки пальцев, ДНК, голос и другие биометрические и поведенческие особенности (п.26). Также предлагается ввести мораторий на внедрение систем распознавания лиц в правоохранительных целях. Исключение должны составлять случаи использования таких систем только для целей идентификации жертвы преступления. Такая ситуация должна сохраняться, пока не будут разработаны соответствующие стандарты, которые будут признаны полностью соответствующим целям защиты прав граждан, результаты использования систем не будут предвзятыми и дискриминационными, а правовая база обеспечит надлежащие гарантии против злоупотреблений и строгий демократический контроль за их использованием. В дополнение к этому необходимо представить наличие эмпирических доказательств необходимости и пропорциональности внедрения таких систем перед тем, как начать их использование (п.27).

Проблематика распознавания лиц с использованием технологий искусственного интеллекта является предметом не только теоретико-правовой дискуссии, но и обсуждения практиков и представителей бизнеса. Так, использованию искусственного интеллекта в системах идентификации лиц было посвящено исследование Института Алана Тюринга [23]. В нем отмечаются риски при использовании искусственного интеллекта для сбора и обработки информации об онлайн и офлайн-активности посредством интеллектуального анализа веб-сайтов, социальных сетей или иных данных. Данные технологии могут быть угрозой для реализации гражданских прав и свобод. Также отдельное беспокойство они вызывают в отношении создания фейковых видео- и аудио-подделок (deepfake) и фальшивых аккаунтов.

Переходя к российскому регулированию в данной области, следует отметить, что положения законодательства о защите персональных данных были разработаны до начала активного внедрения современных технологий обработки данных. Анализируя динамику распространения среди населения мобильных и иных устройств, можно прийти к выводу о сравнительно широком распространении таких устройств только в последние десять лет. До 2010 г. такие устройства в повседневном доступе вне профессиональной сферы имелись у очень незначительной части населения. Сравнительно недавно основная масса граждан считала компьютерные программы, позволяющие изменять голос, способными синтезировать правдоподобное изображение, а также интеллектуально общаться с пользователем делом будущего. Для многих подобные перспективы звучали футуристично. В указанных условиях нормы, законодательно устанавливающие правила обращения с биометрическими данными и регламентирующие применение биометрии и принятые в 2006 г., были сформулированы достаточно обобщенно, не учитывают современные технологические возможности и требуют совершенствования с учетом достижений цифровизации в России и в мире.

Особенностью обработки биометрических данных является высокая эффективность алгоритмов при доступности значительной вычислительной мощности цифровых устройств, а также объемов памяти для аккумулирования и оперирования данными. Вместе с тем применение высокотехнологич-

ных устройств и современных программных средств, повышая эффективность обработки биометрических и иных данных, также актуализирует вопросы защиты информации и минимизации рисков. Нормы действующего законодательства в настоящее время не учитывают всей специфики обеспечения информационной безопасности в процессе хранения и обработки такой категории персональных данных, как биометрические. Указанное происходит в условиях постоянного противоборствования в информационной сфере между корпорациями и государствами. Указанное усиливается в применении технологии искусственного интеллекта, включая нейросети, используемые для решения нелинейных задач. Применение нейросетей предполагает функционирование системы на базе сложной, динамически формируемой модели, которая часто позволяет интерпретировать процесс в конструкция законодательства о персональных данных.

Г.Г. Камалова также отмечала и неточность нормы-дефиниции биометрических персональных данных [6] и с ее доводами, полагаем, можно согласиться. В современной российской формулировке определения биометрических персональных данных явно недостаточно поведенческих признаков. В этом аспекте представляется целесообразным заимствование зарубежного опыта, рассмотренного выше. Вместе с тем нередко определение, закрепленное в ч. 1 ст. 11 Закона о персональных данных [24], рассматривается как удовлетворяющее требованиям правоприменительной практики. Вместе с тем положения законодательства, регламентирующего обработку биометрических данных, в настоящее время не учитывают применение современных цифровых технологий, включая технологии искусственного интеллекта, больших данных, виртуальной и дополненной реальности, интернета вещей и технологий обработки геномной информации.

Представление биометрических данных и иной информации о человеке в виде программного кода, обработка такого кода и его анализ посредством разделения на части множеством программ и устройств, позволяет ставить вопрос о том являются ли отдельные наборы кодов биометрическими данными. Полагаем, что во многих случаях ответ будет отрицательным. Следовательно, с позиции буквы закона компьютерная программа нередко будет обрабатывать код, а не биометрические данные. И в лучшем случае пользователь технологии искусственного интеллекта для защиты своих данных сможет руководствоваться лишь общими нормами, устанавливающими требования к обработке персональных данных. Возможность применения специальных норм, направленных на биометрические данные, может оказаться дискуссионной. В связи с этим представляется целесообразным дальнейшее развитие законодательства в сфере охраны биометрических данных с учетом необходимости обеспечения высокого уровня защиты прав субъектов персональных данных в процессе разработки и использования технологии искусственного интеллекта.

Кроме того, правоприменительная практика в сфере искусственного интеллекта при обработке биометрических данных осложняется неопределенностью правонарушителя. Действительно, определение состава объективной и субъективной стороны правонарушения происходит в условиях необходимости учета применяемых моделей, алгоритмов и совокупности цифровых устройств. Разделение процессов, одновременная параллельная обработка данных, как было указано выше, влечет ситуацию, когда каждое отдельно взятое устройство с формальной позиции не обрабатывало биометрические данные. При этом указанная проблема для теоретико-правового исследования юридической ответственности в сфере современных цифровых технологий является универсальной и характерна для всего массива автоматических и автоматизированных действий, а не только систем искусственного интеллекта и киберфизических систем.

Особенностью использования технологии нейросетей для обработки биометрических персональных данных является сложность «понимания» процесса принятия решений искусственной интеллектуальной системой. Формируемые при этом записи не позволяют в полной мере воссоздать процесс в целях его анализа и установления необходимых причинно-следственных связей. Указанное обстоятельство существенно затрудняет реализацию норм юридической ответственности. При этом отметим, что обеспечение регистрации и учета всех действий, совершаемых в информационной системе, является одним из требований в области безопасности обработки персональных данных (п. 8 ч. 2 ст. 19 Закона о персональных данных). В связи с этим полагаем: необходимо совершенствование законодательства в данной сфере с учетом возможных рисков, что особо значимо в сфере привлечения к административной и уголовной ответственности.

В информационные системы целесообразно включать постоянно функционирующую подсистему, фиксирующую данные об условиях работы системы и всех ее операциях. Доступ к этой инфор-

мации должен предоставляться лицам, несущим ответственность за действия и надлежащее функционирование информационной системы, а также уполномоченным государственным органом в установленном порядке, что позволит устанавливать причинно-следственные связи между функционированием искусственного интеллекта и причиненным вредом. При этом сформировать примерное понимание сложности процедуры принятия решений нейросетью можно на основе образцовой модели действий нейросети по классификации двух видов объектов, различающихся по цвету, представленной в общем доступе [25]. Указанная модель демонстрирует, что распознавание образов, включая образы человека, на основе этой технологии является действием на динамически формирующейся модели и требует больших вложений для минимизации рисков принятия неадекватных (ложных) решений. Это свидетельствует о необходимости выработки дополнительных правовых механизмов обеспечения прав граждан при применении нейросетей в таких чувствительных областях, как деятельность правоохранительных органов и судебных органов.

Таким образом, можно сделать вывод, что использование технологии искусственного интеллекта при обработке биометрических данных, включая идентификацию, сопряжено со значительными рисками, для минимизации которых может, среди прочего, рассматриваться возможность использования только государственных ресурсов для обеспечения процесса идентификации, либо лицензионный контроль над лицами, которые оказывают услуги государству. Кроме того, есть особое мнение специалиста в этой области, например Комиссара по защите персональных данных в ООН, согласно которому использование искусственного интеллекта для биометрической идентификации должно быть в целом запрещено в полном объеме [26].

Одно из последних актуальных исследований в отношении использования технологий искусственного интеллекта в бизнесе, проведенное юридической фирмой Dentons в 2021 г. [27], также говорит о том, что круг решений, принимаемых искусственным интеллектом, должен быть ограничен. Например, принятие судебных решений, поскольку такое решение требует наличие эмоционального интеллекта и этических соображений. Среди других рисков указывается на излишнюю рациональность искусственного интеллекта, которая не должна противопоставляться социальным нормам и правам человека, поэтому работа над безопасностью ИИ должна идти как со стороны государства, так и со стороны бизнеса. В исследовании указывается, что использование этих технологий – это альтернативная экономическая стоимость к улучшению качества жизни трудящихся людей. Перед бизнесом и государством встает выбор между обучением рабочей силы, чтобы люди освоили новые навыки и сбором данных, чтобы технологии искусственного интеллекта работали корректно, при этом отмечается подход различных стран с предоставлением данных для машинного обучения. В то время как одни страны делают данные общедоступными и легкодоступными, другие страны отдают предпочтение защите частной жизни граждан. Также выделяются запретные практики для технологий ИИ, такие как: социальный скоринг, удаленная биометрическая идентификация физических лиц в общедоступных местах, использование технологий для определения эмоций человека, классификация людей с помощью искусственного интеллекта по биометрическим данным в кластеры в соответствии с этнической принадлежностью, полу, политической или сексуальной ориентации или другим признакам, которые могут привести к дискриминации. Важно, что среди других проблем использования искусственного интеллекта исследователи и опрошенные ими респонденты выделяют недостаток прозрачности принятия решений с помощью технологий искусственного интеллекта (проблема «черного ящика»).

Таким образом, исследование показывает актуальность рассматриваемой проблематики не только для Российской Федерации, но и для всего мира. В то же время технологии обработки биометрических персональных данных развиваются и в перспективе ожидается значительное усложнение юридической проблематики. Во многом такие прогнозы связаны с развитием технологий искусственного интеллекта и соответствующих этому вызовов для права. Это усиливает значение выработки основных этических и правовых принципов в области искусственного интеллекта в целях повышения экономической эффективности технологий при одновременном обеспечении прав граждан. При этом помимо вторжения в частную жизнь человека и возрастающих возможностей высоко персонализированного манипулирования, отслеживание граждан может иметь серьезные негативные последствия для осуществления прав человека, которые необходимо учитывать на протяжении всего жизненного цикла системы искусственного интеллекта. Не случайно в стратегии развития искусственного интеллекта, принятой во Франции [28], отмечено, что «на данном этапе подотчетность систем, функционирующих на основе машинного обучения, представляет собой настоящий научный вызов, который создает конфликт между потребно-

стью в объяснениях и интересами в повышении эффективности. Хотя некоторые модели машинного обучения легче поддаются объяснению, чем другие (системы, основанные на правилах, простые деревья решений и байесовские сети), в настоящее время их производительность, как правило, не соответствует производительности алгоритмов глубокого обучения».

В связи с этим должны быть выработаны общие принципы регулирования отношений, связанных с применением технологий искусственного интеллекта и робототехники, а также сформирована база, обеспечивающая гарантии для прав граждан, включая случаи обработки генетических данных и персональных данных. В России основные тренды регулирования отражены в Национальной стратегии развития искусственного интеллекта на период до 2030 г. [29] и Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 г., утв. Распоряжением Правительства РФ от 19.08.2020 № 2129-р [30]. В контексте настоящего исследования важно отметить и то, что подходы, известные российскому регулированию на данном (начальном) этапе, по большей части соответствуют и европейскому, практически-ориентированные доктринальные основы которого были заложены на уровне комплексного исследования (“feasibility study”) Комитета [Совета Европы] ad hoc по искусственному интеллекту (“CAHAI”) [31]. В частности, в разделе 7.1 данного исследования содержатся практические предложения, которые можно обобщенно соотнести с рядом принципов, многие из которых имеют прямое соответствие с теми, что установлены на уровне российских нормативных правовых актов. К числу данных общих принципов применения систем искусственного интеллекта, которые также должны закономерно применяться и в отношениях, связанных с использованием биометрических персональных данных для целей удаленной идентификации, относятся принципы идентификации систем искусственного интеллекта, свободы взаимодействия с искусственным интеллектом, проектируемого соответствия закону и проектируемой безопасности, недискриминации, прозрачности и объяснимости систем искусственного интеллекта, защиты неприкосновенности частной жизни, правления права и надлежащей процедуры. Будущее исследований и практики в области обработки биометрических персональных данных неразрывно связано с вопросами принятия решений на основе алгоритмов (то есть с использованием искусственного интеллекта). Указанное усиливает значимость дальнейших теоретико-правовых исследований в данной области.

СПИСОК ЛИТЕРАТУРЫ

1. Камалова Г.Г. Теоретико-правовые аспекты эволюции прав человека в условиях цифровизации и внедрения технологии искусственного интеллекта // Вестн. Удм. ун-та. Сер. Экономика и право. 2021. Т. 31, вып. 4. С. 662-668.
2. Кашкин С.Ю., Покровский А.В. Искусственный интеллект, робототехника и защита прав человека в Европейском Союзе // Вестн. Университета имени О.Е. Кутафина (МГЮА). 2019. № 4 (56). С. 64-90.
3. Минбалеев А.В. Проблемы социальной эффективности и защиты прав человека при использовании искусственного интеллекта в рамках социального скоринга // Вестн. Южно-Уральского гос. ун-та. Серия: Право. 2020. Т. 20, № 2. С. 96-101.
4. 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.
5. Брызгин А.А., Минбалеев А.В. Правовой режим биометрических персональных данных // Вестн. УрФО. Безопасность в информационной сфере. 2012. № 2 (4). С. 35-41.
6. Камалова Г.Г. Биометрические персональные данные: определение и сущность // Информационное право. 2016. № 3. С. 8-12.
7. Архипов В.В., Наумов В.Б. Искусственный интеллект и автономные устройства в контексте права: о разработке первого в России закона о робототехнике // Труды СПИИРАН. 2017. № 6 (55). С. 46-62.
8. Конвенция о защите прав человека и основных свобод. Заключена в г. Риме 04.11.1950 (с изм. от 24.06.2013) // СЗ РФ. 2001. № 2. Ст. 163.
9. P.N. v. Germany App No 74440/17 (ECtHR 11 June 2020) // European Court of Human Rights. URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-202758%22]} (дата обращения: 10.11.2021).
10. Хартия Европейского союза об основных правах. Принята в г. Страсбурге 12.12.2007 // СПС «Консультант Плюс».
11. Конвенции о защите физических лиц при автоматизированной обработке персональных данных. URL: http://www.pravo.gov.ru, 11.10.2013.
12. Научно-практический постатейный комментарий к Федеральному закону «О персональных данных» / А.И. Савельев. М.: Статут, 2017. 468 с.

13. Директива Европейского парламента и Совета Европейского Союза № 2002/58/ЕС от 12 июля 2002 г. (с изм. и доп. от 25.11.2009) «Об обработке персональных данных и защите информации о частной жизни в сфере электронных коммуникаций» // СПС «Консультант Плюс».
14. Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC // European Union Law. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010 (дата обращения: 10.11.2021).
15. 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 com/2021/206 final // An official website of the European Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206 (дата обращения: 10.11.2021).
16. EDPB & EDPS call for ban on use of AI for automated recognition of human features in publicly accessible spaces, and some other uses of AI that can lead to unfair discrimination // European Data Protection Board. URL: https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-human-features-publicly-accessible_en (дата обращения: 10.11.2021).
17. Opinion Nº 4/2007 WP 136 (20.06.2007) // European Commission. URL: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm (дата обращения: 10.11.2021).
18. О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных): регламент Европейского парламента и Совета Европейского Союза. № 2016/679. 27.04.2016 // СПС «Консультант Плюс».
19. Директива 95/46/ЕС «О защите прав физических лиц применительно к обработке персональных данных и о свободном движении таких данных» // СПС «Консультант Плюс».
20. 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 com/2021/206 final // An official website of the European Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206 (дата обращения: 10.11.2021).
21. EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) // European Data Protection Board. URL: https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en (дата обращения: 10.11.2021).
22. European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI)) // European Parliament. URL: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.html (дата обращения: 10.11.2021).
23. Artificial intelligence, human rights, democracy, and the rule of law // Council of Europe. URL: https://rm.coe.int/primer-en-new-cover-pages-coe-english-compressed-2754-7186-0228-v-1/1680a2fd4a (дата обращения: 10.11.2021).
24. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 02.07.2021) «О персональных данных» // СЗ РФ. 2006. № 31 (1 ч.). Ст. 3451.
25. Доступная модель нейросети для визуализации понимания работы нейросетей / A Neural Network Playground // URL: https://playground.tensorflow.org/ (дата обращения: 10.11.2021).
26. Urgent action needed over artificial intelligence risks to human right // Сайт ООН. URL https://news.un.org/en/story/2021/09/1099972?utm_source=UN+News+-+Newsletter&utm_campaign=4b590eb8aa- (дата обращения: 10.11.2021).
27. Dentons Artificial Intelligence Guide 2022: The AI journey-opening eyes to opportunity and risk // Dentons – AI: Global Solutions HUB. URL: https://insights.dentons.com/344/23400/uploads/final---embargoed-until-10-jan---ai-guide-2022---brand-67749-v15.pdf?intIaContactId=1ITDENBjckU3rTR0WQXZrQ%3d%3d&intExternalSystemId=8 (дата обращения: 21.12.2021).
28. For a Meaningful Artificial Intelligence: Towards a French and European Strategy // European Commission. URL: https://knowledge4policy.ec.europa.eu/publication/meaningful-artificial-intelligence-towards-french-european-strategy_en (дата обращения: 10.11.2021).
29. Указ Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года») // URL: http://www.pravo.gov.ru, (дата обращения: 10.11.2021).
30. Распоряжение Правительства РФ от 19.08.2020 № 2129-р «Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года» // URL: http://www.pravo.gov.ru, 26.08.2020.
31. Feasibility Study. Ad Hoc Committee on Artificial Intelligence (CAHAI)". 2020. *Council of Europe*. https://rm.coe.int/cahai-2020-23-final-eng-feasibility-study-/1680a0c6da (дата обращения: 10.11.2021).

Поступила в редакцию 14.01.2022

Архипов Владислав Владимирович, доктор юридических наук, доцент,
заведующий кафедрой теории и истории государства и права
ФГБОУ ВО «Санкт-Петербургский государственный университет»
199106, Россия, Санкт-Петербург, 22-я линия В.О., 7

Наумов Виктор Борисович, доктор юридических наук, главный научный сотрудник
сектора информационного права и международной информационной безопасности
ФГБУН «Институт государства и права Российской академии наук»
119019, Россия, г. Москва, ул. Знаменка, 10
E-mail: nau@russianlaw.net

V.V. Arkhipov, V.B. Naumov

THEORETICAL AND LEGAL ISSUES OF PROTECTION OF HUMAN RIGHTS WHEN USING BIOMETRIC DATA ARTIFICIAL INTELLIGENCE SYSTEMS: EUROPEAN EXPERIENCE

The article discusses the theoretical issues of the formation of legal mechanisms for the protection of human rights, including the right to privacy, in the modern conditions of digital transformation. Based on the methods of comparative law, the paper investigates the legal risks of digitalization in terms of the use of biometric data by software solutions and devices based on artificial intelligence technology. As a result of the study, in order to increase the economic efficiency of technologies while ensuring the rights of citizens, taking into account the growing potential for highly personalized manipulation and other risks of biometric personal data processing technology, the authors come to conclusions about significant challenges for the law. This reinforces the importance of developing basic ethical and legal principles in the field of artificial intelligence and the formation of a legislative framework in the field of artificial intelligence.

Keywords: theory of state and law, theoretical foundations of digitalization, human rights, privacy, legal risks, comparative legal research, digital technologies, digital transformation, identification of subjects, biometric data, artificial intelligence.

Received 14.01.2022

Arkhipov V.V., Doctor of Law, Associate Professor,
Head of the Department of Theory and History of State and Law
Saint Petersburg State University
22nd line V.O., 7, St. Petersburg, Russia, 199106

Naumov V.B., Doctor of Law, Chief Researcher
in Sector of Information Law and International Information Security
Institute of State and Law of the Russian Academy of Sciences
Znamenka st., 10, Moscow, Russia, 119019
E-mail: nau@russianlaw.net