А.Ю. Ястребова,
доктор юридических наук, доцент,
профессор кафедры международного права,
Дипломатическая академия МИД России
e-mail: allayastrebova@mail.ru
A.Yu. Yastrebova,
Doctor of Law, Associate Professor,
Professor of the Department of International Law,
Diplomatic Academy of the Ministry of Foreign Affairs of Russia

И.О. Анисимов,
кандидат юридических наук, заместитель декана,
доцент кафедры международного права,
Дипломатическая академия МИД России
e-mail: i-anisimov@mail.ru

I.O. Anisimov,
PhD in Law, Deputy Dean,
Associate Professor, Department of International Law,
Diplomatic Academy of the Ministry of Foreign Affairs of Russia
e-mail: i-anisimov@mail.ru

ОСУЩЕСТВЛЕНИЕ ПРАВА ЧЕЛОВЕКА НА ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ: ОТДЕЛЬНЫЕ МЕЖДУНАРОДНО-ПРАВОВЫЕ АСПЕКТЫ, ОПЫТ РОССИИ И СНГ

IMPLEMENTATION OF THE HUMAN RIGHT TO PROTECTION OF PERSONAL DATA: PARTICULAR INTERNATIONAL LEGAL ASPECTS, THE EXPERIENCE OF RUSSIA AND THE CIS

Аннотация. В статье рассматриваются отдельные аспекты международно-правовой защиты персональных данных и ее особенности на универсальном, региональном и национальном правовом уровне. Проанализирован термин «персональные данные» и право индивида на защиту персональных данных в контексте универсальных стандартов прав человека. Отдельно представлены правовые основы защиты персональных данных в рамках Визовой информационной системы государств-членов ЕС. Изучены формы персональных данных и особенности идентификации для передвижения граждан третьих стран в Шенгенском пространстве. Рассмотрены формы правовой защиты персональных данных, закрепленные в российском законодательстве и праве СНГ.

Ключевые слова: право, цифровые технологии, защита персональных данных, международно-правовая защита права на частную жизнь, нормативные акты ЕС, Визовая информационная система, Шенгенское пространство, право СНГ, законодательство Российской Федерации.

Abstract. The article provides certain aspects of the international legal protection of personal data and its features at the universal, regional and national legal level. The term "personal data" and the right of an individual to the protection of personal data in the context of universal human rights standards are analyzed. Separately, the legal framework for the protection of personal data within the framework of the Visa Information System of the EU Member States is presented. The forms of personal data and identification features for the movement of citizens of third countries in the Schengen area are studied. The forms of legal protection of personal data, enshrined in Russian legislation and CIS law, are considered.

Keywords: law, digital technologies, protection of personal data, international legal protection of the right to privacy, EU regulations, Visa information system, Schengen area, CIS law, legislation of the Russian Federation.

Введение

Международно-правовые аспекты защиты персональных данных человека связаны с двумя направлениями сотрудничества государств: содержанием права на частную жизнь и обеспечением безопасного обмена цифровой информацией в рамках глобализации технологий ее передачи и использования. Защита персональных данных должна осуществляться также государственными органами и юридическими лицами на национальном уровне. Сегодня мы можем говорить о тенденции цифровизации всех основных сфер жизнедеятельности человечества [25. С. 262].

С одной стороны, реализация определенных форм общественных отношений в информационно-технологическом пространстве выступает позитивным фактором. Так, упрощение коммуникации, взаимодействие субъектов правоотношений по предоставлению товаров и услуг стимулируют социальную и экономическую сферу деятельности государств. Одновременно эти процессы обусловили обмен и накопление персональных данных физических лиц. С другой стороны, развитие информационных технологий может опережать установление системы государственного контроля за защитой таких данных [26. С. 41]. Существует широкий перечень угроз, связанных с технической стороной гарантий защиты персональных данных физических лиц: произвольная или организованная утечка данных, нарушение целостности информационных систем, взлом информационных баз, содержащих персональный контент.

Защита персональных данных на универсальном международно-правовом уровне и в рамках Совета Европы

Как известно, право на защиту персональных данных определяется общим правом человека на частную жизнь. Данное право остается не регламентированным в международно-правовых актах универсального уровня. Ст. 12 Всеобщей декларации прав человека 1948 г. включает запрет произвольного вмешательства в личную и семейную жизнь, посягательств на неприкосновенность жилища, тайну корреспонденции, честь и репутацию индивида; при этом каждый человек имеет право на защиту закона от подобных

действий [1]. Персональные данные человека априори входят в понятие «личная и семейная жизнь» как информация о его генетических, культурных и социальных особенностях. В свою очередь, защита сведений о местоположении индивида может косвенно обеспечивать неприкосновенность жилища. Корреспонденция индивида содержит информацию, которая относится к персональным данным, поэтому ее неприкосновенность связана с их защитой. Стоит также отметить закрепление подобных запретов в ст. 17 Международного пакта о гражданских и политических правах 1966 г. [2]. Так же, как и в содержании Всеобщей декларации прав человека 1948 г., право человека на частную жизнь дополнено в ч. 2 правом на защиту закона от таких вмешательств или посягательств. Пакт, как и любой международный договор, имеет целью установить определенные международно-правовые обязательства государств-участников.

Нужно указать, что право индивида на защиту персональных данных в той или иной форме закреплено в ряде универсальных международных договоров, определяющих правовой статус отдельных уязвимых категорий людей. Так, ч. 1 ст. 8 Факультативного протокола к Конвенции о правах ребенка, касающегося торговли детьми, детской проституции и детской порнографии 2000 г., содержит требование принятия государствами-участниками надлежащих мер для защиты прав и интересов детей-жертв в частности, их частной жизни и личности, с целью избегать нежелательного распространения информации, которая могла бы привести к установлению их личности [3]. Указанные нормы конфиденциальности должны обеспечивать ресоциализацию детей, пострадавших от вовлечения в такую деятельность. Ч. 2 ст. 22 Конвенции о правах инвалидов 2006 г. устанавливает, что «государства-участники охраняют конфиденциальность сведений о личности, состоянии здоровья и реабилитации инвалидов наравне с другими» [4]. Представляется, что в условиях цифровизации социальной сферы только создание и поддержание системы защиты персональных данных может обеспечивать особые права и потребности таких лиц. Они, вне всякого сомнения, относятся к сфере частной жизни и

личной безопасности индивидов. С.Ю. Кашкин и А.В. Покровский ставят вопрос о негативном влиянии технологических инноваций на эффективность защиты персональных данных и указывают, что «применение технологий искусственного интеллекта позволяет открыто вмешиваться в частную жизнь, сводя на нет это недавно завоеванное людьми право» [28. С. 75]. Необходимо поддерживать международно-правовую защиту персональных данных и совершенствовать ее в соответствии с развитием современных достижений цифровизации.

Представляется, что наиболее детально международно-правовые аспекты современного права на защиту персональных данных регламентированы на региональном уровне. Так, учредительные договоры Европейского Союза включают право каждого индивида на защиту его персональных данных (ч. 1 ст. 16 Договора о функционировании ЕС (ДФЕС) в редакции Лиссабонского договора 2007 г.) [16]. Установление правил, относящихся к защите персональных данных физических лиц и свободе их перемещения, возложено на Европейский Парламент, Европейский Совет и государства-члены ЕС (ч. 2 ст. 16 ДФЕС). Хартия об основных правах (составная часть Лиссабонского договора о ЕС 2007 г.), помимо прямого закрепления права на защиту персональных данных, содержит требования к государствам-членам о добропорядочных и целевых условиях их обработки при наличии согласия заинтересованного лица или других правомерных оснований, установленных законом (ч. 2 ст. 8) [8]. Здесь же установлено право каждого человека на доступ к собранным в отношении его данных и устранение в них ошибок, причем соблюдение таких правил находится под контролем независимых органов (ч. 3 ст.8).

П.А. Калиниченко и М.В. Некотенева также определяют необходимость защиты персональных данных при осуществлении исследований генома человека и замечают, что с целью обеспечения безопасности геномной информации «ряд актов вторичного права ЕС <…> регулирует отношения, связанные с защитой прав личности при сборе, хранении и обработке персональных данных» [27. С. 75].

Стокгольмская программа «Открытая и безопасная Европа, которая служит своим гражданам и защищает их» от 4 мая 2010 г. указывает в качестве цели ЕС обеспечение «стратегии для защиты данных в рамках Союза и в его отношениях с другими странами» (п. 2.5) [9]. Европейский Союз должен предусмотреть и регламентировать условия, при которых вмешательство публичных властей в осуществление права на персональные данные выступает оправданным, и применять принципы их защиты в частной сфере.

Регламент Европейского Парламента и Совета ЕС № 679/2016 от 27 апреля 2016 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных устанавливает определение персональных данных как любой информации, относящейся к физическому лицу, с помощью которой такое лицо могло бы быть идентифицировано прямо или косвенно, в частности, посредством таких критериев, как имя, идентификационный номер, сведения о местоположении, идентификатор в режиме онлайн или через один или несколько признаков, характерных для физической, психологической, генетической, умственной, экономической, культурной или социальной идентичности указанного физического лица (ч. 1 ст. 4) [10].

Российские правоведы отмечают, что эффективность защиты персональных данных требует не только гармонизации принципов такой защиты, но «и в определенной степени средств их применения в столь быстро меняющейся и высоко технологической области» и условий трансграничной передачи указанных данных [29. С. 122]. Как известно, Российская Федерация присоединилась к Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных 1981 г. в ноябре 2001 г. Исполнение правовых обязательств по указанному договору и использование международно-правовых стандартов защиты приватности частично нашли свое закрепление в Федеральном законе от 27 июля 2006 г. № 152-ФЗ «О персональных данных» [18].

Согласно Конвенции, персональные данные представляют собой любую информацию об определенном или определяемом физическом лице (п. «а» ст. 2)

[11]. В Федеральном законе уточняется, что лицо при этом может быть определенным или определяемым как прямо, так и косвенно (ч. 1 ст. 3) [18]. Данный закон учитывает современные тенденции идентификации физических лиц, определяет понятие биометрических персональных данных как сведений, устанавливающих физиологические и биологические особенности человека, на основании которых выясняется его личность, и основные принципы их обработки оператором (ст. 11). Трансграничная передача персональных данных связывается с участием государств в Конвенции Совета Европы 1981 г. и наличием адекватной системы защиты прав их субъектов (ст. 12). М.Ю. Авдеев указывает, что общей целью Федерального закона № 152-ФЗ является «обеспечение защиты прав и свобод человека при обработке персональной информации о нем, в том числе защиты прав на неприкосновенность частой жизни, личную и семейную тайну» и его действие предполагает «постепенное формирование правовой культуры защиты персональных данных» [23. С. 222-223.].

Республика Молдова также является участником Конвенции Совета Европы 1981 г. При ее ратификации были сделаны оговорки, в соответствии с которыми Конвенция не будет применяться в отношении обработки персональных данных физических лиц, предназначенных исключительно для личных и семейных нужд (с условием, что они не нарушают права субъектов персональных данных[1]), а также в отношении обработки персональных данных, относящихся к информации, являющейся государственной тайной [21].

В то же время было заявлено, что положения Конвенции будут применяться, в том числе, и в отношении персональных данных, которые не подвергаются автоматизированной обработке. В качестве компетентного органа по выполнению положений Конвенции Совета Европы был назначен Национальный центр по защите персональных данных.

[1] Под субъектом персональных данных понимается физическое лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных.

В 2011 г. был принят Закон Республики Молдова «О защите персональных данных» [22]. Целью закона является «обеспечение защиты основных прав и свобод физического лица при обработке его персональных данных, в особенности права на неприкосновенность интимной, семейной и частной жизни» (ст. 1).

Данным законом регулируются правоотношения, возникающие при обработке персональных данных полностью или частично автоматизированными средствами, а также при обработке средствами, отличными от автоматизированных, персональных данных, составляющих часть системы учета или предназначенных для введения в такую систему. В соответствии со ст. 3 Закона, персональные данные определяются как «любая информация, связанная с идентифицированным или идентифицируемым физическим лицом (субъектом персональных данных)».

Закон Республики Армения «О защите персональных данных» 2015 г.[2] определяет персональные данные как «любое сведение, относящееся к физическому лицу, которое позволяет или может позволить впрямую или косвенно идентифицировать личность» [20]. Закон регулирует порядок и условия государственного контроля над обработкой персональных данных органами государственного управления или местного самоуправления, государственными или общинными учреждениями или организациями, юридическими или физическими лицами. Установленные законом средства обработки и регулирования защиты персональных данных обусловлены имплементацией положений Конвенции Совета Европы и директивы Европейского парламента и Совета Европейского Союза 95-46-ЕС от 24-го октября 1995 года «О защите физических лиц при обработке персональных данных» [24].

[2] Республика Армения ратифицировала Конвенцию о защите физических лиц при автоматизированной обработке персональных данных 1981 г. 9 мая 2012 г.

Подводя итог, можно сделать вывод о том, что в национальном законодательстве государств-участников Конвенции Совета Европы понятие «персональных данных» является фактически идентичным.

Персональные данные физических лиц обладают уникальной значимостью, позволяют точно идентифицировать личность человека и должны быть объектом особой защиты. Вышеприведенный Регламент ЕС № 679/2016 устанавливает ряд мер по защите персональных данных. Е.В. Постникова справедливо замечает, что Регламент «создает единое правовое регулирование ЕС в сфере защиты персональных данных, которое должно усилить право на защиту данных и сделать так, чтобы люди доверяли структурам, которым они сообщают свои данные» [30. С. 244]. Данным правовым актом государства-члены ЕС закрепляют перечень основополагающих принципов, необходимых к соблюдению при обработке персональных данных физических лиц, который включает требования:

- законной, беспристрастной и прозрачной обработки данных;
- целевого ограничения, согласно которому обработка данных должна происходить исключительно в установленных целях, о которых индивид был проинформирован;
- минимизации данных, согласно которому к обработке привлекаются только такие данные, которые действительно необходимы для указанных целей;
- точности, означающей, что персональные данные должны быть актуальными и любые неточности подлежат как можно более скорому исправлению;
- ограничения по хранению, что обеспечивает необходимость удаления данных сразу после того, как цели обработки были достигнуты и дальнейшее хранение данных более нецелесообразно;
- конфиденциальности и целостности, согласно которым персональные данные должны обрабатываться безопасным способом, без утечек и иного несанкционированного доступа.

Указанные принципы обеспечиваются положениями Регламента, дающего широкий список прав и обязанностей как субъектам, предоставляющим свои персональные данные организации или иному лицу, управомоченному осуществлять их обработку («субъект данных»), и организациям, определяющим цели и способы обработки («контролеры») [32. С. 96-97].

Е.В. Постникова также указывает, что «одним из инструментов повышения эффективности единого внутреннего рынка выступает защита персональных данных, которая, в свою очередь, является неотъемлемой частью пространства правосудия и основных прав человека» [30. С. 234].

Регламент ЕС № 679/2016 выступает правовой основой для ряда других актов ЕС, например, Регламента Европейского Парламента и Европейского Совета № 1725/2018 от 23 октября 2018 г. о защите физических лиц при обработке персональных данных институтами, органами, ведомствами и агентствами и о свободном обращении таких данных, а также об отмене Регламента № 45/2001 и Решения № 1247/2002/ЕС [12]. В содержании Регламента № 1725 приведен более широкий перечень правовых определений. В частности, ст. 3 вводит термины «оперативные персональные данные» (персональные данные, обработанные государственными органами стран-членов ЕС) и «пользователь» (физическое лицо, оперирующее в пределах распределенной сети или оборудования, подконтрольного органам государства-члена ЕС). Ст. 52 Регламента № 1725 учреждает Европейский надзорный орган по защите данных (European Data Protection Supervisor). Раздел 3 гл. 4 Регламента № 1725 предусматривает обязательство органов государств-членов ЕС обеспечивать безопасность своих электронных сетей; защиту информации, переданной, полученной и обработанной с помощью терминального оборудования, относящегося к сайтам и мобильным приложениям; запрет использования информации о пользователях в маркетинговых целях. Регламент включает нормы, обеспечивающие создание технических условий для поддержания безопасности персональных данных и их обработки.

Правовые основы защиты персональных данных в Визовой информационной системе, установленной правом ЕС

Самостоятельной частью права ЕС в сфере регламентации защиты персональных данных выступает содержание Визового кодекса в редакции Регламента № 1155/2019 Европейского Парламента и Совета ЕС от 20 июня 2019 г. об изменении Регламента ЕС № 810/2009, устанавливающего Кодекс Сообщества о визах [13]. Им регламентировано включение персональных данных граждан третьих стран, въезжающих на территорию государств-членов ЕС, в Визовую информационную систему (VIS/ВИС). Данная база представляет собой систему информационного обмена данными о краткосрочных визах граждан третьих стран для государств, входящих в Шенгенское пространство. ВИС складывается из центральной базы данных, национальных интерфейсов и коммуникационной структуры, соединяющей эти элементы. Благодаря использованию ВИС компетентные органы государств-участников Шенгенских соглашений могут обобщать данные об обработке визовых заявлений, получении или отказе в выдаче виз.

ВИС также предполагает наличие автоматизированной дактилоскопической системы идентификации лиц, где сохраняются отпечатки пальцев заявителей и обеспечивается технически возможность установления их совпадений при повторном обращении. Лица, прибывающие в Шенгенское пространство, идентифицируются пограничными службами государств-членов. ВИС сопряжена с национальными визовыми системами государств-участников.

Назначение и функции ВИС определяются Регламентом Европейского Парламента и Совета ЕС № 767/2008 от 9 июля 2008 г. в отношении системы ВИС и обмена между государствами-членами данными в отношении краткосрочных виз (Регламент по ВИС) [14]. Данный правовой акт сейчас уточнен дополнениями и поправками, предусмотренными Регламентом № 2021/1134 от 7 июля 2021 г., где само наименование документа расширено «обменом между государствами-членами данными в отношении краткосрочных виз, долгосрочных виз и видов на жительство» [17]. Правовые основы

использования ВИС уполномоченными властями предполагают применение принципа недискриминации заявителей и держателей Шенгенской визы для указанных типов пребывания по таким основаниям, как пол, расовое, этническое или социальное происхождение, генетические особенности, языковая принадлежность, вероисповедание или убеждения, политические взгляды, принадлежность к национальному меньшинству, собственность, место рождения, наличие инвалидности, возраст и сексуальная ориентация. Включение сведений в ВИС осуществляется с учетом уважения человеческого достоинства и основных прав, включая право на частную жизнь и защиту персональных данных (ч. 2 ст. 7 Регламента 2021/1134). Это позволяет говорить об основах организации ВИС с указанием на специальные (отраслевые) принципы международного права прав человека и фундаментальное право человека на защиту частной жизни.

В содержание ВИС поочередно вносятся сведения о подаче визового заявления, его рассмотрении, выдаче визы, остановки в рассмотрении заявления, отказе в выдаче визы, ее аннулировании или продлении. ВИЗ взаимодействует с другими базами данных, такими, как Шенгенская информационная система (SIS), Европейская система информации о поездках и авторизации (ETIAS), Интерполом и Европолом, резервной компьютерной сетью Бюро SIRENE, Европейской дактилоскопической системой (Eurodac).

В качестве биометрических идентификаторов ходатайствующих о Шенгенской визе лиц Регламентом № 1155/2019 установлены фотография и десять отпечатков пальцев заявителя в цифровой форме (ст. 12). Решением Совета ЕС в 2021 г. фотографии для виз должны выполняться при подаче ходатайства; требования дактилоскопии распространены на детей в возрасте с 6 лет; при рассмотрении ходатайств могут проводиться дополнительные проверки биографических данных заявителей. В базы ВИС включается также, помимо информации о краткосрочных визах, сведения о долгосрочных визах и видах на жительство, которые подразумевают свободное передвижение граждан третьих стран в общем пространстве ЕС [15].

Доступ к ВИС обеспечен только для уполномоченного персонала государств-членов, назначенного должным образом для выполнения своих функций; персональные данные заявителей поступают в нее только на законной основе и собираются законными средствами (ч. 1 ст. 29 Регламента 2021/1134). Каждый заявитель имеет право получить информацию о своих личных сведениях, которые сохранены в ВИС (ч. 1 ст. 38 Регламента). Он также вправе требовать исправления неправильных сведений о себе и удаления незаконно полученных персональных данных (ч. 2 ст. 38). Тем не менее, если ходатайство было принято, и решение по предоставлению Шенгенской визы отрицательное, информация о заявителе остается в ВИС.

Целями организации ВИС определены, в частности:

1) облегчение визовых процедур;

2) упрощение контроля на внешних границах ЕС и на территории государств-членов;

3) обеспечение надлежащей идентификации физических лиц;

4) поддержание правил, установленных Шенгенской информационной системой;

5) предупреждения угроз для национальной безопасности государств-членов ЕС и преступности (ч. 1 ст. 2 Регламента 2021/1134).

Национальным властям государства, ответственного за выдачу визы, разрешено использование персональных данных заявителя, таких, как информация о его статусе, целях въезда, типе въездного документа и т.д., для ведения отчетности и статистики. Каждое государство-член обязано обеспечивать безопасность личных сведений, которое оно получает из базы ВИС и не допускать индивидуальной идентификации при их использовании (ч. 1 ст. 45а Регламента 2021/1134).

Таким образом, сбор и обработка персональных данных граждан третьих стран в унифицированных информационных базах ЕС сложились как региональный правовой инструмент идентификации и визового контроля таких лиц. ВИС обеспечивает постоянный доступ государств-членов ЕС и стран,

входящих в Шенгенское пространство, к детальной персонификации заявителей. Представляется, что она подлежит использованию с учетом обязанностей указанных государств по реальному обеспечению права человека на частную жизнь и защиту персональных данных и гарантий конфиденциальности личной информации в цифровой среде. В нынешних условиях приостановки действия Соглашения между Российской Федерацией и Европейским сообществом об упрощении выдачи виз гражданам Российской Федерации и Европейского союза 2006 г., произошедшей по инициативе Европейской комиссии и отдельных государств-членов ЕС, неоправданного усложнения процедур приема и рассмотрения визовых заявлений российских граждан, повышения требований к списку предоставляемых ими документов затруднительным будет представить перспективы международно-правового сотрудничества по защите персональных данных на этом уровне.

Защита персональных данных в праве СНГ и Российской Федерации

Нужно отметить, что в рамках СНГ действует ряд собственных международно-правовых актов в области защиты персональных данных. Так, например, в 1999 г. на Межпарламентской Ассамблее государств-участников СНГ был принят Модельный закон «О персональных данных» (далее Модельный закон), который стал основой для унификации законодательства государств-участников. Ст. 2 Модельного закона содержит ряд системных определений [5]. Так, под персональными данными понимается «информация (зафиксированная на материальном носителе) о конкретном человеке, которая отождествлена или может быть отождествлена с ним». Модельный закон относит к персональным данным:

- биографические и опознавательные данные;

- личные характеристики;

- сведения о семейном, социальном положении, образовании, профессии, служебном и финансовом положении, состоянии здоровья и прочие.

Кроме того, в ст. 2 дается определение таким понятиям, как *сбор персональных данных*, *передача персональных данных*, а также *трансграничная*

передача персональных данных, под которой понимается передача держателем персональных данных этих данных держателям, которые находятся под юрисдикцией другого государства.

Ст. 3 Модельного закона определяет общие принципы правового регулирования персональных данных. К таким принципам, в частности, относятся следующие:

- персональные данные должны быть получены и обработаны законным образом на основании действующего законодательства;

- персональные данные включаются в базы персональных данных на основании свободного согласия субъекта, выраженного в письменной форме;

- персональные данные должны накапливаться для точно определенных и законных целей, не использоваться в противоречии с этими целями и не быть избыточными по отношению к ним;

- персональные данные, предоставляемые держателем, должны быть точными и в случае необходимости обновляться;

- персональные данные должны храниться не дольше, чем этого требует цель, для которой они накапливаются, и подлежать уничтожению по достижении этой цели или при миновании надобности;

- должны приниматься меры для охраны персональных данных, исключающие случайное или несанкционированное разрушение или случайную их утрату, а равно несанкционированный доступ к ним, изменение, блокирование или передачу данных;

- не допускается объединение баз персональных данных, собранных держателями в разных целях, для автоматизированной обработки информации;

- для лиц, занимающих высшие государственные должности, и кандидатов на эти должности национальным законодательством может быть установлен специальный правовой режим для их персональных данных, обеспечивающий открытость только общественно значимых данных.

Ст. 4 устанавливает правовой режим персональных данных, под которым понимается «нормативно установленные правила, определяющие условия

доступа, хранения, уточнения, передачи, блокирования, обезличивания и уничтожения персональных данных». Необходимо отметить, что персональные данные, находящиеся в ведении держателя, по умолчанию относятся к конфиденциальной информации, кроме специально предусмотренных случав.

Особое внимание в анализируемой статье уделено защите персональных данных умершего лица. В частности устанавливается, что с момента смерти субъекта персональных данных правовой режим персональных данных подлежит замене на режим архивного хранения или иной правовой режим, предусмотренный национальным законодательством. Предусмотрено, что защита персональных данных умершего лица может осуществляться другими лицами, в том числе наследниками, в порядке, предусмотренном национальным законодательством о защите чести, достоинства, деловой репутации, личной и семейной тайн.

Модельный закон определяет порядок трансграничной передачи персональных данных. Ст. 10 предусматривает, что трансграничная передача персональных данных не может запрещаться или ставиться под специальный контроль, за исключением случаев, создающих угрозу национальной безопасности, и при необеспечении адекватного уровня защиты персональных данных. На государстве лежит обязанность по обеспечению законных мер защиты, находящихся на его территории или передаваемых через его территорию персональных данных, исключающих их искажение и несанкционированное использование.

Ч 4. ст. 10 устанавливает, что передача персональных данных в страны, не обеспечивающие адекватный уровень защиты этих данных, может иметь место при условии:

- явно выраженного согласия субъекта персональных данных на эту передачу;

- необходимости передачи персональных данных для заключения и (или) исполнения договора между субъектом и держателем персональных данных

либо между держателем и третьей стороной в интересах субъекта персональных данных;

- если передача необходима для защиты жизненно важных интересов субъекта персональных данных;

- если персональные данные содержатся в общедоступной базе персональных данных.

Необходимо отметить, что за двадцать с лишим лет с момента принятия Модельного закона в развитии информационно-коммуникационных технологий произошли серьёзные изменения.

Исследователи отмечают, что «радикально трансформировались технологии обработки данных, в том числе персональных» [31. С. 45]. В связи с этим настала необходимость пересмотреть законодательство государств-участников СНГ. 29 ноября 2018 г. Межпарламентская Ассамблея СНГ приняла новую редакцию Модельного закона «О персональных данных» [6].

Как отмечается, цель новой редакции - «гармонизация национального законодательства государств-участников СНГ в части оборота и защиты персональных данных предложением общих ориентиров с учетом актуальных тенденций в этой области и новых подходов к определению роли персональных данных в повседневной жизни» [31. С. 46].

В новой редакции модельного закона скорректировано определение персональных данных. Теперь под ними понимается информационные данные о личности, то есть информация, которая позволяет прямо или косвенно определить физическое лицо (субъекта персональных данных) или может быть отождествлена с ним [6]. Кроме того, введены в оборот различные категории персональных данных - *анкетные персональные данные*, *служебные персональные данные* и *биометрические персональные данные*.

Определены специальные категории персональных данных, к числу специальных относятся:

- персональные данные (в том числе служебные), собираемые в рамках

законной деятельности, связанной с защитой государственной тайны, работой правоохранительных органов, органов государственной власти (органов местного самоуправления), охраной здоровья граждан, обеспечением обороны и безопасности государства;

- персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъекта персональных данных.

Положения о трансграничной передаче данных были дополнены новацией, согласно которой на оператора персональных данных возложена обязанность убедиться в том, что иностранным государством, куда планируется передача указанных данных, обеспечивается адекватная защита прав субъектов персональных данных.

Еще одним международно-правовым актом в сфере защиты персональных данных в рамках СНГ стало Соглашение о взаимной правовой помощи по административным вопросам в сфере обмена персональными данными (далее Соглашение 2020 г.) [7]. В нем также дается определение «персональных данных», под которыми понимается любая информация, прямо или косвенно относящаяся к физическому лицу, уже идентифицированному либо которое может быть идентифицировано.

Исходя из специфики сферы действия Соглашения 2020 г., ст. 3. конкретизирует типы персональных данных, которые могут являться предметом запроса об оказании правовой помощи, к которым относятся информация по:

- наличию/отсутствию гражданства;

- наличию документов, дающих право на постоянное или временное пребывание (проживание) на территориях государств-участников Соглашения;

- постановке на миграционный учет или регистрации по месту жительства (месту пребывания) граждан государств-участников Соглашения, граждан третьих государств и лиц без гражданства;

- выдаче виз, дающих право на въезд на территории государств-участников Соглашения;

- недвижимому имуществу, зарегистрированному на имя субъекта персональных данных на территориях государств-участников Соглашения;

- обязательствам имущественного характера, имеющимся у субъекта персональных данных на территориях государств-участников Соглашения;

- привлечению субъекта персональных данных к уголовной или административной ответственности на территориях государств-участников Соглашения;

- документам, удостоверяющим личность.

Необходимо отметить, что рассмотренные международно-правовые акты оказывают серьезное влияние на унификацию и совершенствование национального законодательства государств-участников СНГ, в частности России.

Так, с 1 сентября 2022 г. в содержание Федерального закона № 152-ФЗ «О персональных данных» были внесены существенные изменения [19]. Теперь операторы должны уведомлять Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее - Роскомнадзор) о начале или осуществлении любой обработки персональных данных, за исключением случаев, когда данные обрабатываются в целях защиты безопасности государства и общественного порядка, транспортной безопасности, или если оператор обрабатывает данные исключительно без средств автоматизации. Сроки предоставления информации Роскомнадзору были сокращены с 30 календарных до 10 рабочих дней.

В Законе теперь определены обязанности оператора в случае компрометации персональных данных. Так, у оператора есть 24 часа с момента происшествия, чтобы сообщить в Роскомнадзор:

- об инциденте;

- его предполагаемой причине и вреде, причиненном субъектам данных;

- мерах по устранению последствий инцидента;

- представителе компании, который уполномочен взаимодействовать с Роскомнадзором по вопросам, связанным с происшествием.

Кроме того, оператор обязан в течении 72 часов с момента инцидента провести внутреннее расследование и сообщить в Роскомнадзор о его результатах, а также о виновниках (при наличии). Оператор обязан взаимодействовать с госсистемой обнаружения компьютерных атак (ГосСОПКА), в том числе направлять сообщения об утечке данных. Механизм взаимодействия определит ФСБ.

Скорректирован порядок обработки данных по требованию физлица. У оператора есть 10 рабочих дней с момента получения требования физлица, чтобы прекратить обработку данных о нем или обеспечить прекращение обработки (если ее ведет другое лицо). Срок можно продлить в пределах 5 рабочих дней на основании мотивированного уведомления.

Положения Закона были распространены на иностранные компании и физлиц, которые используют данные российских физлиц. Если компания передала данные иностранной организации для обработки, ответственность перед физлицом несут обе организации.

Также закон внес изменения в правила трансграничной передачи персональных данных. Новый порядок будет применяться с 1 марта 2023 г., но операторов, которые уже сейчас передают данные за границу, закон обязал направить в Роскомнадзор уведомление о трансграничной передаче до этой даты через Портал персональных данных Роскомнадзора или в письменном виде. Такое усиление защиты трансграничной передачи персональных данных связано, прежде всего, с обеспечением национальной безопасности государства.

Заключение

Понятие персональных данных является очень схожим по своей юридической формулировке как на региональном международно-правовом уровне, так и в законодательстве государств-участников. В самом обобщенном виде они представляет собой любую информацию, прямо или косвенно относящуюся к идентифицируемому физическому лицу.

Систематизация защиты персональных данных представляет собой особую правовую потребность в связи с тем, что постоянно расширяется сфера использования указанных данных в деятельности государств и юридических лиц. Следовательно, для каждой вновь обозначенного направления развития информационных технологий должны применятся общие стандарты защиты права человека на частную жизнь и право на идентификацию.

Необходимо отметить, что принятие новых международно-правовых актов на уровне СНГ в сфере защиты персональных данных направлено не только на унификацию и гармонизацию государств-участников, но и на совершенствование существующего национального законодательства. Изменения, внесенные в Федеральный закон Российской Федерации № 152-ФЗ «О персональных данных», отражают общую тенденцию ужесточения контроля за любыми операциями, проводимыми операторами с персональными данными субъекта. Особое внимание как на региональном, так и национальном уровне уделяется контролю за трансграничной передачей персональных данных.

Литература

1. Всеобщая декларация прав человека [Текст]: принята Резолюцией 217 А (III) Генеральной Ассамблеи Организации Объединенных Наций от 10 декабря 1948 г. // Российская газета. – 1995. – № 67.

2. Международный пакт о гражданских и политических правах [Текст]: принят Резолюцией 2200 А (XXI)Генеральной Ассамблеи Организации Объединенных Наций от 16 декабря 1966 г. // Бюллетень Верховного Суда Российской Федерации. – 1994. – № 12.

3. Факультативный протокол к Конвенции о правах ребенка, касающийся торговли детьми, детской проституции и детской порнографии, от 25 мая 2000 г. // СЗ РФ от 17.02.2014. № 7. Ст. 633.

4. Конвенция о правах инвалидов от 13 декабря 2006 г. // СЗ РФ от 11.02.2013. № 6.Ст. 468.

5. Модельный закон СНГ «О персональных данных» от 16 октября 1999 г. [Электронный ресурс]. – URL: https://docs.cntd.ru/document/901818602 (дата обращения: 18.09.2022).

6. Модельный закон СНГ «О персональных данных» (новая редакция): от 29 ноября 2018 г. [Электронный ресурс]. URL: http://www.parliament.am/library/modelayin%20orenqner/370.pdf (дата обращения:18.09.2022)

7. Соглашение о взаимной правовой помощи по административным вопросам в сфере обмена персональными данными от 18 декабря 2020 г. [Электронный ресурс]. – URL: https://rppa.ru/npa/sng27_18.12.2020 (дата обращения: 18.09.2022).

8. Charter of fundamental rights of European Union (2000/C364/01). [Электронный ресурс]. – URL:https://www.europarl.europa.eu/charter/pdf/text_en.pdf (дата обращения: 10.11.2021).

9. The Stockholm Programme: An open and secure Europe serving and protecting citizens (2010/C115/01). [Электронный ресурс]. – URL: https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:115:0001:0038:EN:PDF (дата обращения: 18.09.2022).

10. 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). [Электронный ресурс]. – URL:https://eurlex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679&qid=1626789259064 (дата обращения: 18.09.2022).

11. Конвенция о защите физических лиц при автоматизированной обработке персональных данных, 28января 1981 г. [Электронный ресурс]. – URL: http://www.consultant.ru/document/cons_doc_LAW_121499/ (дата обращения: 18.09.2022).

12. Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance.) [Электронный ресурс]. – URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1725&from=EN (дата обращения: 18.09.2022).

13. Regulation (EU) 2019/1155 of the European Parliament and of the Council of 20 June 2019 amending Regulation (EC) No 810/2009 establishing a Community Code on Visas (Visa Code). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R1155&from=EN [Электронный ресурс]. – URL: (дата обращения: 18.09.2022).

14. 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).URL: https://eur-lex.europa.eu/eli/reg/2008/767/oj [Электронный ресурс]. – URL: (дата обращения: 18.09.2022).

15. Position of the Council at first reading with a view to the adoption of a Regulation of the European Parliament and of the Council amending Regulations (EC) No 767/2008, (EC) No 810/2009, (EU) 2016/399, (EU) 2017/2226, (EU)2018/1240, (EU) 2018/1860, (EU) 2018/1861, (EU) 2019/817 and (EU) 2019/1896 of the European Parliament and of the Council and repealing Council Decisions 2004/512/EC and 2008/633/JHA, for the purpose of reforming the Visa Information System. Adopted by the Council on 27 May 2021. [Электронный ресурс]. – URL:https://data.consilium.europa.eu/doc/document/ST-5950-2021-REV-1/en/pdf (дата обращения: 18.09.2022).

16. Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community(2007/C306/01). [Электронный ресурс]. –

URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12007L%2FTXT (дата обращения: 18.09.2022).

17. Regulation (EU) 2021/1134 of the European Parliament and of the Council of 7 July 2021 amending Regulations (EC) No 767/2008, (EC) No 810/2009, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1860, (EU) 2018/1861, (EU) 2019/817 and (EU) 2019/1896 of the European Parliament and of the Council and repealing Council Decisions 2004/512/EC and 2008/633/JHA, for the purpose of reforming the Visa Information System. Official Journal of European Union. 13 July 2021. L 248/11.

18. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» [Электронный ресурс]. – URL:https://base.garant.ru/12148567/ (дата обращения: 18.09.2022).

19. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций. Информация об изменениях в законодательстве о персональных данных с 1 сентября 2022 г. [Электронный ресурс]. – URL: http://www.consultant.ru/ (дата обращения: 18.09.2022).

20. Закон Республики Армения от 13 июня 2015 года №ЗР-49 «О защите персональных данных».[Электронный ресурс]. – URL: http://base.spinform.ru/show_doc.fwx?rgn=78183 (дата обращения: 18.09.2022).

21. Закон Республики Молдова в сфере информационной безопасности. Часть 2: Персональные данные, личная и семейная тайна. [Электронный ресурс]. – URL: https://digital.report/zakonodatelstvo-moldovy-infobezopasnost-2/ (дата обращения: 18.09.2022).

22. Закон Республики Молдова «О защите персональных данных» от 8 июля 2011 года №133. [Электронный ресурс]. – URL: http://base.spinform.ru/show_doc.fwx?rgn=51097 (дата обращения: 18.09.2022).

23. Авдеев М.Ю. Право на неприкосновенность частной жизни: конституционно-правовой аспект // Право и жизнь. — 2012. — № 173. — С. 220-228.

24. Акобян М. Обзор законодательства Республики Армения в сфере информационной безопасности — Часть 1: Общий обзор. [Электронный ресурс]. – URL: https://digital.report/zakonodatelstvo-armenii-informatsionnaya-bezopasnost/ (дата обращения: дата обращения: 18.09.2022).

25. Данельян А.А. Международно-правовое регулирование киберпространства // Образование и право. —2020. — № 1. — С. 261-269. DOI 10.24411/2076-1503-2020-10140

26. Котляров М.В. Контролируя неконтролируемое: стратегия Российского государства в Интернете //Вестник Пермского университета. Серия «Политология». — 2017. — № 3. — С. 41-56.

27. 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. 68-78. https://doi.org/10.17803/2311-5998.2020.68.4.068-078

28. Кашкин С.Ю., Покровский А.В. Искусственный интеллект, робототехника и защита прав человека в европейском союзе // Вестник университета имени О.Е. Кутафина (МГЮА). — 2019. — № 4. — 64-90. https://doi.org/10.17803/2311-5998.2019.56.4.064-090

29. Полякова Т.А., Химченко А.И. Актуальные организационно-правовые вопросы трансграничной передачи персональных данных // Право: журнал Высшей школы экономики. — 2013. — № 1. — С. 113-122.

30. Постникова Е.В. Некоторые аспекты правового регулирования защиты персональных данных в рамках внутреннего рынка Европейского союза // Право: журнал Высшей школы экономики. — 2018. — № 1. — С. 234-254.

31. Твердынин М.М., Парфентьев У.У. Анализ законодательства государств-участников СНГ о персональных данных в аспекте их контроля субъектом персональных данных // Диалог: политика, право, экономика. – 2019. - №2 (13). - С. 38-48.

32. Ястребова А.Ю., Анисимов И.О., Акчурин Т.Ф., Горелик И.Б. Право человека на защиту персональных данных: международно-правовые основы,

примеры их имплементации в законодательстве государств, особенности регламентации в праве ЕС и национальном праве США Международно-правовой курьер. 2021. № 7. С. 93-106.