УДК 349

БИОМЕТРИЧЕСКИЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ И ДИПФЕЙКИ: ПРАВОВОЙ АСПЕКТ

АБЛАМЕЙКО М.С.,
доцент кафедры конституционного права юридического факультета Белорусского государственного университета, кандидат юридических наук, доцент
m.ablameyko@mail.ru

ШАКЕЛЬ Н.В.,
старший юрист
ООО «Степановский, Папакуль и партнеры. Юридические услуги», кандидат юридических наук, доцент
n.shakel@spplaw.by

В статье рассмотрены примеры применения новых технологий, в том числе искусственного интеллекта, в государственном и частном секторах. Имеющиеся сегодня новые вызовы сопряжены со сложно просчитываемыми рисками, в том числе в сфере информационных отношений, что продемонстрировано на примере дипфейков, основанных на использовании биометрических персональных данных и искусственного интеллекта. Анализ действующего законодательства, а также подходов к регулированию в других странах позволяет сделать вывод о необходимости принятия комплексных мер по регулированию данной сферы.

Ключевые слова: биометрические персональные данные, дипфейк, искусственный интеллект, цифровизация, правоприменение.

ВВЕДЕНИЕ

Повсеместное применение информационных технологий привело к глобальной цифровизации всех сфер жизнедеятельности общества, в том числе открытости данных. Увеличение объема информации, ее обмена, использования и преобразования привело к возникновению новых вызовов и угроз как для общества в целом, так и для личности. Сегодня особого внимания в этой связи требует использование биометрических персональных

Библиографическая ссылка:
Абламейко, М. С. Биометрические персональные данные и дипфейки: правовой аспект / М. С. Абламейко, Н. В. Шакель // Право.by. – 2024. – № 3 (89). – С. 79–87.

данных (БПД), особенно если в отношении них применяются технологии искусственного интеллекта (ИИ), что позволяет создать, например, дипфейки. БПД, характеризуя биологические и физиологические особенности человека, остаются неизменными на протяжении жизни и позволяют с большой долей вероятности отнести такую информацию к идентифицируемому объекту. По этой причине они требуют особого внимания.

Актуальность и новизна настоящей статьи связана с тем, что она посвящена изучению правовых аспектов использования биометрии в современном мире, в том числе при применении дипфейков. Отметим, что вопросы защиты персональных данных в целом рассматривались в работах Н.В.Валюшко-Орса [1], В.Д.Ипатова [2], И.В.Насоновой [3], Н.А.Савановича [4] и др. Юридические аспекты использования биометрических персональных данных изучали Ю.А.Никитин [5], Н.И.Платонова [6], А.А.Юхник [7] и иные авторы. Кроме того, имеются публикации, в основном в зарубежных источниках, относительно правовых аспектов использования дипфейков (М.Б.Добробаба [8], В.Милославская [9] и др.). Тем не менее многие работы были опубликованы до момента вступления в силу Закона Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных» (далее – Закон о ПД), более того, в целом возможно констатировать, что вопросы использования биометрии и в особенности дипфейков на данный момент не получили достаточного внимания в отечественной юридической литературе. В этой связи целью проведенного в настоящей статье исследования является комплексный анализ правовых аспектов использования БПД, а также выработка предложений, направленных на защиту прав и интересов личности при использовании биометрии, в том числе дипфейков.

ОСНОВНАЯ ЧАСТЬ

Понятие и основные характеристики биометрических персональных данных

Заинтересованность в эффективной и быстрой идентификации лиц имеется в различных сферах деятельности. Так, работа правоохранительных органов непосредственно связана с поиском идентификаций преступников. Интересно отметить, что одним из основоположников системы идентификации таких лиц по численным данным антропометрических параметров и их совокупным пропорциям является французский ученый А.Бертильон. По его мнению, для составления антропометрического портрета личности нужно всего 15 критериев, среди которых: окружность, длина и ширина головы; ширина лба; расстояние между скуловыми костями; длина и ширина правого уха и другие линейные параметры тела [10, с. 79]. Как отмечают исследователи, изначально биометрия использовалась только для судебной идентификации [5]. Сегодня же БПД широко используются и в повседневной жизни. В качестве примеров можно привести использование технологии Face ID в мобильных телефонах, сбор информации о человеке в социальных сетях посредством изображения, распознавание лиц в общественных местах и др. Следует констатировать, что ко многим таким технологиям представители общества относятся положительно, при этом не всегда учитывая особенности их функционирования. Как справедливо отмечает В.Д.Ипатов, имеется определенное «непонимание ценности и значения персональных данных самими гражданами, которые все чаще делают доступной личную информацию в глобальной компьютерной сети Интернет, не учитывая потенциальные риски» [2, с. 26]. Со стороны операторов, напротив, наблюдается стремление аргументировать, что определенные сведения не являются персональными данными

NB *Комплексное правовое регулирование биометрических персональных данных необходимо в том числе для противодействия дипфейкам.*

(для того чтобы не применять положения Закона о ПД к своей деятельности) [4, с. 41], или же обосновать, что обрабатываемые ими персональные данные являются «обычными», а не биометрическими (что существенно снижает уровень предъявляемых к такой обработке требований по защите информации).

С учетом изложенного рассмотрим характеристики БПД и подходы к определению данного понятия.

К особенностям биометрических данных в юридической литературе относят то, что такие данные присущи физическому лицу, целью их сбора и использования является идентификация человека, а полученные в результате сбора данные считаются фиксированными [5; 6, с. 23]. Также выделяют специальные признаки, которые отражают непосредственно сущность биометрии:

1) универсальность. Данный признак означает, что идентификация производится чаще всего по универсальным характеристикам, которые есть у каждого индивида (при этом у конкретной личности такие характеристики имеют свои особенности или могут отсутствовать);

2) уникальность (т.е. даже при определенной схожести определенных характеристик, позволяющих объединить их в особую группу, сохраняется их уникальность, что позволяет проводить различия между лицами);

3) постоянство (изменчивость). С одной стороны, внешность человека (относительный размер, степень четкости и различимость конкретных отличительных черт) может меняться. Вместе с тем имеются признаки, которые остаются стабильными и неизменными на протяжении длительного периода времени и используются при идентификации [7, с. 84; 11].

Идентифицирующими признаками, обладающими высокой степенью репрезентативности, которые составляют основу для сопоставлений в цифровом формате, являются биометрические маркеры. Они характеризуются измеримостью (данные собираются, оцифровываются и хранятся в рамках системы), эффективностью функционирования (данные должны быть достоверными, точными, быстрыми в обработке и надежными как на начальном, так и на последующих этапах технологического процесса), уязвимостью [12].

С технической точки зрения в биометрических идентификаторах используются статические, основанные на физиологических характеристиках человека (радужная оболочка глаз, капилляры сетчатки глаз, тепловое изображение лица), и динамические (почерк, голос) методы [13, с. 225].

В Республике Беларусь БПД отнесены к категории так называемых специальных персональных данных. Согласно определению, закрепленному в Законе о ПД, БПД представляют собой информацию, характеризующую физиологические и биологические особенности человека, которая используется для его уникальной идентификации (отпечатки пальцев рук, ладоней, радужная оболочка глаза, характеристики лица и его изображение и др.).

Таким образом, отечественный законодатель отнес к БПД не только физиологические, но и биологические особенности человека. Считаем целесообразным разграничить данные понятия. Так, например, в России, где также выделяются физиологические и биологические особенности человека применительно к БПД, предлагалось следующее разграничение: «К биометрическим персональным данным относятся физиологические данные (дактилоскопические данные, радужная оболочка глаз, анализы ДНК, рост, вес и другие), а также иные физиологические или биологические характеристики человека, в том числе изображение человека (фотография и видеозапись), которые позволяют установить его личность и используются оператором для установления субъекта» [14].

Как отмечает И.В.Насонова, специальные персональные данные выделяются из общих персональных данных на основании признака предметности, и при этом БПД относятся к специфической категории специальных персональных данных [3, с. 338].

Проблемы отнесения тех или иных идентифицирующих человека признаков к БПД остаются нерешенными. Определение, которое закреплено в Законе о ПД, на практике воспринимается достаточно неоднозначно, так как не в полной мере понятно, какие признаки относятся к физиологическим,

а какие – к биологическим. Кроме того, имеется смешение «обычных» изображений и изображений, которые относятся к БПД. Это обусловлено тем, что в определении не указан такой признак биометрии, как наличие автоматизации соответствующего процесса для уникальной идентификации субъекта персональных данных. Полагаем, что для решения данного вопроса как первый этап необходима подготовка разъяснений Национального центра защиты персональных данных (НЦЗПД). В последующем в Законе о ПД следует скорректировать понятие «биометрические персональные данные», чтобы исключить различные толкования данного термина.

Значение данных предложений обусловлено расширяющимися сферами применения биометрии в государственном и частном секторах. Так, если говорить о распознавании изображений, то оно осуществляется сегодня по двум основным направлениям: распознавание лиц в рамках реализации государственных функций (для целей обеспечения национальной и общественной безопасности); реализация распознавания лиц и их дальнейшее использование частными организациями и лицами.

К первой группе можно отнести:

- создание единых биометрических систем на национальном уровне (пример – Единая биометрическая система (Россия) – цифровая платформа, которая позволяет гражданину проходить удаленную идентификацию по биометрическим образцам для получения услуг);
- выдачу биометрических документов (паспортов), удостоверяющих личность;
- применение систем мониторинга общественной безопасности (пример – республиканская система мониторинга общественной безопасности (Беларусь), элементом которой является распознавание лиц с камер видеонаблюдения, что позволяет обнаружить и идентифицировать человека в потоке, в режиме реального времени [15]);
- обеспечение безопасности границ.

Ко второй группе относятся сервисы, позволяющие частным компаниям идентифицировать пользователей, посетителей, клиентов и даже работников. Так, расширяется использование биометрии в банковской сфере для оказания финансовых услуг.

Право на изображение и дипфейки

В рамках данного исследования считаем необходимым обратить внимание на правовые аспекты использования изображения лица человека в биометрических системах, в том числе при создании дипфейков. По нашему мнению, именно использование изображения вызывает наибольшие проблемы в условиях развития цифровизации, так как существенно затрагивает приватность человека, его цифровые права.

Право на изображение как таковое в настоящее время прямо не определено в законодательстве Беларуси. Отметим, что, по мнению Конституционного Суда, гражданское законодательство определяет правовые механизмы осуществления и защиты нематериальных благ, в том числе внешнего облика гражданина как нематериального блага и права на изображение гражданина. Конкретное изображение гражданина, зафиксированное на материальном носителе, должно охраняться нормами гражданского законодательства с установлением способов такой охраны и определением режима использования изображения гражданина другими лицами [16]. Вместе с тем в Гражданском кодексе Республики Беларусь отсутствуют положения, регламентирующие вопрос о том, что является изображением человека, в каких случаях необходимо согласие на его использование (в том числе на автоматизированную обработку с использованием средств биометрии).

В литературе под дипфейками обычно понимают методику компьютерной генерации изображения, основанной на искусственном интеллекте и использующейся для соединения и наложения существующих изображений и видеороликов на исходные изображения или видеоролики [17, с. 381], а также сам продукт, итоговый результат, полученный в ходе процесса генерации ИИ и представленный в виде аудио- или видеоизображения [18, с. 1]. Таким образом, дипфейки являются технологией, в рамках которой появляется возможность «подмены лиц» с помощью технологий ИИ.

Такие технологии могут применяться в том числе в целях нанесения вреда национальной безопасности: например, фальсификация заявлений глав государств, подделка выступления главы министерства экономики о возможном экономическом кризисе или руководства системой здравоохранения о несуществующем опасном заболевании могут вызвать общественный резонанс, панику и иные негативные реакции со стороны общества.

Как демонстрируют примеры из зарубежной практики, сегодня многие частные компании на постоянной основе используют дипфейки в своей деятельности. Известен пример, когда при производстве рекламных роликов, которое осуществлялось российской компанией без получения каких-либо согласий, использовались дипфейки известных лиц. Интересно отметить, что такие ролики были признаны охраняемым объектом авторского права. Как следует из материалов соответствующего судебного спора, первая компания создала по заказу второй ролик, использовав в нем с помощью дипфейк-технологий изображение зарубежного актера К.Ривза. Третья компания использовала ролик в своих целях, так как в числе прочего полагала, что в подобной ситуации авторское право не возникает. Против нее был подан иск о нарушении авторского права, который был выигран правообладателем [9].

Отдельного внимания заслуживает сфера культуры как наиболее подверженная применению дипфейков, в том числе при искусственном омоложении или старении актеров, синхронизации движений губ при дубляже перевода или «доснятии» фильма после внезапной смерти или прекращения участия в съемках актера [8, с. 114]. Вместе с тем когда в фильме может появиться давно умерший актер, который мог не желать принимать участие в той или иной роли в силу различных соображений (религиозных, эстетических и иных), такие действия уже не в полной мере соответствуют подходу, основанному на правах человека. Подчеркнем в этой связи, что в отличие от многих юрисдикций в Республике Беларусь права субъекта персональных данных, в том числе в части права требовать прекращения обработки его персональных данных, могут быть реализованы и после его смерти указанными в законе лицами.

Использование дипфейк-технологий зачастую осуществляется и частными лицами. Многочисленны случаи создания ими роликов, на которых изображение третьих лиц применено для создания неприемлемого контента, в том числе порнографического характера, высказывания не соответствующих действительности фактов и осуществления иных действий, нарушающих законодательство. В таких ситуациях не всегда возможно говорить о нарушении Закона о ПД, так как его действие не распространяется на случаи обработки, не связанные с профессиональной или предпринимательской деятельностью. Применению подлежат общие положения о защите информации и частной жизни. Так, в соответствии с Законом Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации» сбор, обработка, хранение, предоставление, распространение информации о частной жизни физического лица, а также пользование ею и обработка персональных данных осуществляются с согласия данного физического лица, если иное не установлено законодательными актами. Таким образом, если дипфейк или сам процесс его создания (например, использованная для дипфейка фотография была снята в приватной обстановке без ведома лица) затрагивают частную жизнь лица, то это также будет нарушением требований регуляторики.

Проблемой, которая требует внимания, является сложность установления нарушителя (создателя дипфейка), так как большая часть таких роликов размещается в сети Интернет анонимными пользователями. Удаление соответствующих материалов также является затруднительным. Большинство вебсайтов имеют механизмы удаления контента, нарушающего авторские права. Однако в данном случае права создателя дипфейка как автора не нарушены. Не всегда имеются основания однозначно говорить, что дипфейки нарушают и права на неприкосновенность частной жизни: поскольку данные видео не показывают реальную жизнь человека, его частная жизнь не раскрывается третьим

лицам. Возможным выходом в этой связи представляется разрешение рассматриваемой ситуации через корректировку законодательства о персональных данных.

Законодательство в сфере защиты персональных данных и дипфейки

При определении подходов о регулировании БПД на национальном уровне правительствам необходимо решать вопросы, связанные с защитой лиц, идентифицируемых такими системами, добиваясь, чтобы сбор, хранение и иная обработка таких данных велись в соответствии с международными стандартами в области прав человека о неприкосновенности частной жизни.

Руководствуясь основополагающим принципом минимизации обработки персональных данных, такие данные, как биометрические, следует собирать и хранить лишь в тех случаях, когда это одновременно и необходимо, и целесообразно.

Правовым основанием обработки БПД по общему правилу является согласие. Случаи, когда обработка таких данных возможна без согласия, установлены в ст. 8 Закона о ПД. Как и для других видов специальных персональных данных, обработка биометрии не допускается на основании договора, заключенного (заключаемого) с физическим лицом, а также путем подачи оператору документа (заявления, требования и др.).

Вместе с тем проведенный нами анализ демонстрирует специфику обработки БПД в качестве специальных, особенно в ситуациях, когда соответствующие данные применяются для создания дипфейков. Это требует отражения в законодательстве.

С учетом сложности технологий и процессов, используемых при работе систем, обрабатывающих БПД, установлены дополнительные требования к обеспечению информационной безопасности в данной сфере. При обработке БПД необходимо использовать имеющие надлежащий уровень защиты сертифицированные средства защиты информации. В настоящее время меры по защите информации, в том числе БПД, основаны на положениях Указа Президента Республики Беларусь от 16 апреля 2013 г. № 196 «О некоторых мерах по совершенствованию защиты информации», а также приказа Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449». Вместе с тем меры, которые должны приниматься лицами, использующими биометрические технологии, не имеют градации в зависимости от конкретных обстоятельств, условий и объема используемых данных. Установление дифференцированных требований в зависимости от особенностей использования позволит далее развивать сферу использования биометрии, обеспечивая при этом защиту соответствующей информации.

Для решения проблем, связанных с использованием дипфейков, могут быть применены разные меры. Так, в России в 2023 году рассматривался (но не был принят) законопроект о введении в Уголовный кодекс Российской Федерации (УК РФ) новой статьи, устанавливающей ответственность за незаконное создание или распространение информации о людях без их согласия с помощью ИИ, который подменяет лицо и голос [19; 20, с. 82]. В целях борьбы с порнографическими дипфейками предлагалось также внести соответствующие изменения в ст. 137 и ст. 242 УК РФ [21, с. 73].

В целом с учетом проведенного анализа можно сделать вывод о том, что к решению вопроса регулирования БПД следует подходить комплексно. Поскольку использование информационных технологий для подделки изображения и голоса других лиц не только нарушает личные неимущественные права физических лиц, но и потенциально влечет отрицательные социальные последствия, включая угрозу национальной безопасности и публичным интересам, считаем целесообразным дополнить Гражданский кодекс Республики Беларусь отдельной статьей, регулирующей право на изображение, в том числе с учетом применения технологий ИИ. В целях защиты интересов граждан в данной статье следует установить однозначный запрет юридическим и физическим лицам осуществлять посягательство на изображения физических лиц, в том числе посредством осуществления несанкционированных

действий с ними с использованием информационно-коммуникационных технологий (применение технологий ИИ, дипфейки и т.п.). Следует учитывать, что создатели дипфейков действуют исходя из различных побуждений (стремления получить экономическую выгоду, нанести моральный вред и причинить страдания, желания повлиять на политические процессы путем воздействия на имидж того или иного лица и даже желания создать юмористический или образовательный контент). В этой связи является вторичным установление причины таких действий, наличия или отсутствия вины.

В рамках Закона о ПД в целях повышения информированности граждан о том, что такое биометрия и какие могут быть последствия ее применения, а также решения иных поставленных в настоящей статье вопросов предлагается:

• выделить отдельные основания для обработки БПД путем введения в Закон о ПД ст. 8^1 «Обработка биометрических персональных данных», в которой определить, что обработка таких данных должна осуществляться на основании согласия, с уведомлением субъекта персональных данных об имеющихся рисках обработки его данных, а также с информированием о том, используются ли при обработке системы ИИ, осуществляется ли трансграничная передача персональных данных;

• ввести обязательную маркировку сгенерированных ИИ материалов;

• определить в качестве необходимых мер защиты при использовании БПД применение сертифицированных средств защиты с их градацией в зависимости от цели и способа использования биометрии;

• к числу правовых оснований обработки БПД (не требующих согласия) отнести договор с субъектом персональных данных (например, если лицо дает право использовать свое изображение для генерации рекламных роликов или создания фильма), а также разрешение НЦЗПД (такое разрешение сейчас может быть получено для трансграничной передачи персональных данных, вместе с тем полагаем возможным подобный механизм распространить и на обработку биометрии).

Для реализации вышеупомянутых мер следует предусмотреть административную и уголовную ответственность сторон путем внесения изменений в соответствующие кодексы.

ЗАКЛЮЧЕНИЕ

Широкое использование биометрии оправдано, так как позволяет обеспечить эффективность решения достаточно сложных задач, в том числе по контролю доступа в помещения, требующие дополнительных мер защиты, или же созданию дипфейков, в том числе требуемых для сферы культуры. В связи с масштабным распространением и применением технологий ИИ все более актуальным становится вопрос защиты БПД. Человек не всегда придает большое внимание распространению сведений о себе, не в полной мере осознает возможные последствия в том числе при размещении своих фотографий в сети Интернет. Необходимо повышение осведомленности о рисках применения биометрических технологий. В современных условиях наука должна содействовать исследованию проблем развития и использования систем ИИ, предлагая сбалансированные решения, как содействующие распространению новых технологий, так и обеспечивающие их надежность и безопасность. Применение технологий ИИ не должно привести к нарушению или ущемлению интересов личности и обрушению морально-нравственных норм, сформированных человечеством.

Необходимо определение правовых правил и норм использования БПД в различных сферах, с учетом широкого их применения как государственным, так и частным сектором, в том числе физическими лицами индивидуально. В этой связи считаем целесообразным рассматривать комплексный подход к решению данного вопроса путем внесения изменений в Гражданский кодекс Республики Беларусь, законодательство о защите персональных данных, Кодекс Республики Беларусь об административных правонарушениях и Уголовный кодекс Республики Беларусь (путем определения «права на изображение» в гражданском законодательстве, внесения в Закон о ПД ст. 8^1 «Обработка биометрических персональных данных», а также определения мер ответственности за нарушение установленных законодательством норм).

СПИСОК ЦИТИРОВАННЫХ ИСТОЧНИКОВ

1. Валюшко-Орса, Н. В. Сущностно-содержательные аспекты персональных данных в Республике Беларусь / Н. В. Валюшко-Орса // Журн. Белорус. гос. ун-та. Право. – 2017. – № 2. – С. 17–23.

2. Ипатов, В. Д. Совершенствование законодательства о персональных данных / В. Д. Ипатов // Информационные технологии и право : Правовая информатизация – 2018 : сб. материалов VI Междунар. науч.-практ. конф., Минск, 17 мая 2018 г. / Нац. центр правовой информ. Респ. Беларусь ; под общ. ред. Е. И. Коваленко. – Минск : Нац. центр правовой информ. Респ. Беларусь, 2018. – С. 26–30.

3. Насонова, И. В. Защита персональных данных в Республике Беларусь: понятие, условия и субъекты / И. В. Насонова // Право в современном белорусском обществе : сб. науч. тр. / редкол.: Н. А. Карпович (гл. ред.) [и др.]. – Минск : ООО «Колорград», 2022. – С. 334–343.

4. Саванович, Н. А. Дефиниция персональных данных в Законе Республики Беларусь «О защите персональных данных» и проблемы ее применения / Н. А. Саванович // Юстиция Беларуси. – 2022. – № 6. – С. 41–44.

5. Никитин, Ю. А. Биометрические персональные данные и особенности правового регулирования использования биометрических документов [Электронный ресурс] / Ю. А. Никитин // ЭТАЛОН-ONLINE. – Режим доступа: https://etalonline.by/novosti/mnenie/biometricheskie-personalnye-dannye/. – Дата доступа: 11.03.2024.

6. Платонова, Н. И. Современные правовые подходы к пониманию биометрических данных / Н. И. Платонова // Информационное право. – 2018. – № 1. – С. 22–26.

7. Юхник, А. А. Биометрические персональные данные как специальный вид персональных данных в законодательстве Республики Беларусь / А. А. Юхник // Труд. Профсоюзы. Общество = Labour. Trade Unions. Society : ежекварт. науч.-практ. журнал / Федерация профсоюзов Беларуси, Междунар. ун-т «МИТСО». – 2017. – № 4. – С. 80–85.

8. Добробаба, М. Б. Дипфейки как угроза правам человека / М. Б. Добробаба // Lex russica. – 2022. – № 11 (192). – С. 112–118.

9. Милославская, В. Правовые проблемы использования технологии Deepfake [Электронный ресурс] / В. Милославская // Закон.ру. – Режим доступа: https://zakon.ru/blog/2024/04/19/pravovye_problemy_ispolzovaniya_tehnologii_deepfake. – Дата доступа: 12.04.2024.

10. Набиев, Р. Ф. Бертильонаж: славное прошлое и возможные перспективы / Р. Ф. Набиев, Э. Э. Горяев // Ученые записки Казан. юрид. ин-та МВД России. – 2019. – № 2 (8). – С. 77–82.

11. Jain, A. K. Biometrics: Personal Identification in Networked Society / R. Bolle, S. Pankanti // Norwell, Mass. : Kluwer Academic Publisher, 1999. – 411 p.

12. Сборник практических рекомендаций Организации Объединенных Наций по ответственному использованию биометрических данных и обмену ими в рамках борьбы с терроризмом [Электронный ресурс] // ООН. – Режим доступа: https://www.unodc.org/pdf/terrorism/Compendium-Biometrics/_.pdf. – Дата доступа: 15.04.2024.

13. Ворона, В. А. Биометрические технологии идентификации в системах контроля и управления доступом / В. А. Ворона, В. О. Костенко // Computational nanotechnology. – 2016. – № 3. – С. 224–241.

14. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций разъясняет вопросы отнесения фото- и видеоизображения, дактилоскопических данных и иной информации к биометрическим персональным данным и особенности их обработки [Электронный ресурс] // Роскомнадзор. – Режим доступа: https://25.rkn.gov.ru/news/news54167.htm. – Дата доступа: 15.01.2024.

15. МВД – о программной платформе мониторинга общественной безопасности [Электронный ресурс] // Национальный правовой Интернет-портал Республики Беларусь. – Режим доступа: https://pravo.by/novosti/obshchestvenno-politicheskie-i-v-oblasti-prava/2022/december/72426/. – Дата доступа: 11.04.2024.

16. О правовом регулировании в гражданском законодательстве использования и охраны изображения гражданина [Электронный ресурс] : решение Конституц. Суда Респ. Беларусь, 30 окт. 2018 г., № Р-1145/2018 // Национальный правовой Интернет-портал Республики Беларусь. – Режим доступа: https://pravo.by/document/?guid=12551&p0=K91801145. – Дата доступа: 15.04.2024.

17. Иванов, В. Г. Deepfakes: перспективы применения в политике и угрозы для личности и национальной безопасности / В. Г. Иванов, Я. Р. Игнатовский // Вестн. Рос. ун-та дружбы народов. Сер. Государственное и муниципальное управление. – 2020. – Т. 7, № 4. – С. 379–386.

18. Sloot B., van der. Deepfakes: regulatory challenges for the synthetic society / B. van der Sloot, Y. Wagensveld // Computer law and Security review. – 2022. – Vol. 46. – P. 1–15.

19. В правительстве не поддержали законопроект об уголовной ответственности за дипфейки [Электронный ресурс] // ТАСС. – 2023. – Режим доступа: https://tass.ru/obschestvo/17922853. – Дата доступа: 18.04.2024.

20. Ситник, В. Перспективы установления уголовной ответственности за преступления, совершенные с использованием технологии дипфейк / В. Ситник // Урал. журн. правовых исследований. – 2022. – № 3 (20). – С. 76–83.

21. Архипцев, И. Н. Порнографический дипфейк: вымысел или виртуальная реальность? / И. Н. Архипцев [и др.] // Социально-политические науки. – 2021. – Т. 11, № 1. – С. 69–74.

Рецензент: Михалёва Т.Н.,
ведущий научный сотрудник Национального центра законодательства и правовых исследований Республики Беларусь, кандидат юридических наук, доцент

Актуальность и корректность цитирования (использования) нормативных правовых актов Республики Беларусь проверены автором посредством ИПС «ЭТАЛОН» (ИПС «ЭТАЛОН-ONLINE») на дату поступления статьи в редакцию 20.05.2024.

ABLAMEYKO M.S., SHAKEL N.V.

Biometric personal data and deepfakes: legal aspect

The article discusses examples of the application of new technologies, including artificial intelligence, in the public and private sectors. New challenges available today are associated with difficult to calculate risks, including in the sphere of information relations, as demonstrated by the example of deepfakes based on the use of biometric personal data and artificial intelligence. The analysis of the current legislation, as well as approaches to regulation in other countries allows us to conclude that it is necessary to take comprehensive measures to regulate this area.

Keywords: biometric personal data, deepfake, artificial intelligence, digitalization, law enforcement.