ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БИОМЕТРИЧЕСКИХ ТЕХНОЛОГИЙ

Калашникова А.В., Калашникова К.В.

Научный руководитель: Инюшкин А.А.

Россия, г. Самара,
Самарский национальный исследовательский университет
имени академика С.П. Королева

Аннотация. *В статье рассматривается проблема правового регулирования технологии распознавания лиц с точки зрения информационной безопасности. Проанализировано существующее законодательство и предложены меры по соблюдению биометрической конфиденциальности.*

Ключевые слова: *биометрия, персональные данные, конфиденциальность, безопасность, технология распознавания лиц.*

В современном мире в системы видеонаблюдения активно внедряются алгоритмы распознавания, которые в режиме реального времени распознают лицо, походку, радужную оболочку глаза в видеопотоке, сверяют с данными, находящимися в базе данных, и уведомляют оператора такой системы при обнаружении совпадений. Данные алгоритмы предназначены для решения задач безопасности государства и бизнеса, так как система искусственного интеллекта способна за доли секунд обнаружить преступника и отследить маршруты его передвижений.

Технология распознавания лиц основана на использовании «биометрии» (то есть индивидуальных физических характеристик) для цифрового отображения «геометрии» лица человека. Эти измерения затем используются для создания математической формулы, известной как «шаблон лица» или «подпись лица». Этот сохраненный шаблон, или подпись, затем используется для сравнения физической структуры лица человека, чтобы подтвердить его личность или однозначно идентифицировать этого человека.

Быстрое развитие науки способствовало распространению данной технологии, которая продолжает внедряться в новые области общественной и частной жизни. Популяризация технологии способствует расширению возможностей использования, таких как: контроль доступа к объектам и системам, выявление нарушителей, анализ поведения покупателей, идентификация в банковской сфере, учет рабочего времени сотрудников, оплата товаров и услуг, использование лица при проходе на стадионы, вокзалы, аэропорты, внедрение в системы «Умный город», доступ к экзаменам.

Согласно Федеральному закону №152 «О персональных данных» такие данные, как лицо человека, радужная оболочка глаза, отпечаток пальца, голос, походка, почерк и др., являются биометрическими персональными данными, поскольку относятся к физиологическим данным, а также к иным физиологиче-

ским или биологическим характеристикам человека, в том числе изображение человека (фотография и видеозапись), которые позволяют установить его личность и используются оператором для установления личности субъекта [1]. Таким образом, биометрические данные являются особым видом персональных данных, и поэтому для них должен быть установлен специальный правовой режим и регулирование.

Благодаря тому, что биометрические данные являются постоянными, они позволяют в любой момент идентифицировать заинтересованное лицо по присущим только ему биологическим особенностям. Причина использования биометрических данных в качестве идентификаторов заключается именно в том, что они уникальны и неизменны с течением времени. Однако если эту технологию не регулировать, ее можно будет использовать способами, которые могут поставить под угрозу конфиденциальность информации. В отличие от пароля, биометрические индивидуальные характеристики непросто уничтожить или изменить. Поэтому утечка биометрических данных может иметь ощутимые последствия для заинтересованного лица: он больше не сможет использовать скомпрометированные биометрические данные, а также впоследствии надежно себя идентифицировать. Так как любые биометрические данные являются мощным уникальным идентификатором, то возможно объединение личной информации из разных источников в подробный личный профиль субъекта данных без его согласия, что является явным вторжением в частную жизнь и подрывает личный контроль человека над использованием информации. Философские основы права на неприкосновенность частной жизни предполагают, что потеря этого элемента контроля приводит к потере конфиденциальности. Более того, неспособность контролировать информацию, относящуюся к нам, также имеет негативные коннотации для степени автономии, достоинства и уважения, оказываемых нам как личностям.

В этой связи биометрическая обработка данных не является безобидным явлением, и требует особого правового регулирования на каждом этапе процесса обработки биометрической информации, и при его правильной разработке могла бы стать средством повышения конфиденциальности. Именно поэтому законодатель должен предусмотреть усиленный контроль процедуры оборота подобной информации. Приведем некоторые существующие законодательные меры по этому вопросу:

1. В США не существует единого Федерального закона, регулирующего сбор и использование персональных данных в целом или биометрических данных. Вместо этого каждый штат сам регулирует данный вопрос. Так, например, в 2008 году Иллинойс принял «Biometric Information Privacy Act» (BIPA) [5], который защищает от незаконного сбора и хранения биометрической информации. Согласно BIPA, частное лицо не может собирать или хранить данные шаблона лица без предварительного уведомления, получения письменного согласия и раскрытия определенной информации.

2. В Евросоюзе с 2018 года принято положение в законодательстве «General Data Protection Regulation» (GDPR) [4] о защите данных и конфиденциальности, которое защищает все биометрические данные человека (в том

числе фотографии) от использования и обработки в любых целях, за исключением оказания медицинской помощи или угрозы национальной безопасности. Принципы GDPR также выходят за пределы Европы, и это можно видеть по тому, что в других странах начинают появляться новые законы о конфиденциальности биометрических данных.

3. В России обработка биометрических персональных данных осуществляется в соответствии со статьей 19 Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных» [2]. Кроме того, согласно Федеральному закону № 482-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» государственные органы, банки и иные организации в предусмотренных законом случаях могут проводить удаленную идентификацию физических лиц, основанную на использовании их биометрических персональных данных [3].

4. В Китае в настоящее время отсутствует единая правовая основа для защиты биометрических данных и их конфиденциальности, связанная с технологией распознавания лиц. Однако несмотря на это, в КНР режим защиты данных содержит множество принципов и требований, установленных различными законами и постановлениями. Китай предпринимает различные законодательные попытки установить нормы защиты личной информации аналогично GDPR. Рассматривается проект закона «О персональных данных», в котором биометрические персональные данные рассматриваются как персональные данные наравне с расовой, этнической, религиозной, медицинской, финансовой и личной информацией.

Растущее использование технологий, в частности, систем биометрической идентификации не привело к принятию соответствующего законодательства. В связи с этим необходимо принять законодательство о биометрической конфиденциальности, которое расширит требования к уведомлениям, согласию и безопасности, подобным BIPA. Возможно наложить дополнительные требования, такие, как обязательное тестирование перед развертыванием и периодическое обучение сотрудников, а также разрешение тестирования этой технологии третьим лицом. В то же время необходимо сделать биометрическую идентификацию одним из основных направлений общенационального регулирования, которое установило бы единые требования по всей стране в отношении использования технологий. Также необходимо принять дополнительные законы, регулирующие использование технологии распознавания лиц коммерческими предприятиями.

Организации, использующие технологии распознавания лиц сегодня, или компании, планирующие использовать эту технологию в будущем, особенно те, которые используют данные технологии в целях безопасности и наблюдения, даже если в настоящее время не попадают под действие какого-либо закона, не должны ждать принятия новых законов. Вместо этого им следует принять меры по соблюдению биометрической конфиденциальности уже сейчас.

Предложим меры, которые компании могут предпринять, чтобы эффективно использовать технологию распознавания лиц в соответствии с юридическими обязательствами:

- разработка политики конфиденциальности. Разработка общедоступной подробной политики конфиденциальности для системы распознавания лиц, которая включает в себя цели, для которых собираются данные. Такая политика конфиденциальности должна содержать информацию о том, как компания собирается хранить и уничтожать данные, и срок хранения таких данных;

- письменное уведомление. До момента сбора любых данных предоставить письменное уведомление, которое проинформирует человека о том, что его данные будут собираться, использоваться, храниться или обрабатываться компанией с указанием срока хранения до уничтожения;

- письменное разрешение. Необходимо получить письменное разрешение от лиц, у которых будут собраны данные. Биометрические данные впоследствии будут собраны и использованы компанией в рамках принятой политики конфиденциальности. Кроме того, необходимо предусмотреть факт отказа человека от сбора его данных. Безопасность хранимых данных. Необходимо принять как организационные, так и технические меры по защите данных для недопущения атак на базы данных и/или несанкционированной передачи третьим лицам.

Однако использование только законодательных и организационных мер будет недостаточно. Необходимо также использовать технические решения. Биометрические данные должны быть не просто записаны в обычной базе данных, но это должна быть целая биометрическая система, включающая в себя различные алгоритмы перевода таких данных в некоторый специфический вид – биометрические шаблоны. В таких биометрических системах биометрические шаблоны представляют собой цифровые изображения, созданные с помощью сложных алгоритмов. Например, голосовой биометрический шаблон не содержит звука и не является «звуковым» файлом, а используемые шаблоны для распознавания лиц не содержат изображений лиц в их обычном понимании. На самом деле это серия случайных, бессмысленных числовых цифр. Более того, при правильной реализации он не может быть преобразован обратно в исходную звуковую или графическую форму. Это будет справедливо для любого правильно сконструированного шаблона. Другими словами, если шаблон попал в руки злоумышленника, он ничего не может с ним сделать. Это в равной степени применимо независимо от того, зашифрован шаблон или нет: однако в хорошей биометрической системе всегда применяется шифрование.

Таким образом, даже если злоумышленник получит биометрический шаблон некоторого лица, это не приведет к компрометации биометрических данных, так как используется надежная сертифицированная система защиты биометрических данных.

Библиографический список

1. Разъяснения Роскомнадзора о вопросах отнесения фото- и видеоизображения, дактилоскопических данных и иной информации к биометрическим персональным данным и особенности их обработки [Электронный ресурс].

URL: http://www.consultant.ru/law/hotdocs/28108.html/ (дата обращения 03.11.2020).

2. Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных» [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения 16.10.2020).

3. Федеральный закон от 31.12.2017 N 482-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_286744/ (дата обращения 16.10.2020).

4. General Data Protection Regulation (GDPR) Compliance Guidelines [Электронный ресурс] URL: https://gdpr-info.eu. Дата обращения: 13.10.2020.

5. Illinois General Assembly [Электронный ресурс]. URL: https://ilga.gov (дата обращения: 28.09.2020).

BIOMETRIC SECURITY

Kalashnikova A.V., Kalashnikova X.V.

Scientific adviser: Inyushkin A.A.

Samara National Research University, Samara, Russia

Abstract. *The article examines the problem of legal regulation of face recognition technology from the point of view of information security. The existing legislation was analyzed and measures to ensure biometric confidentiality were proposed.*

Keywords: *biometrics, personal data, confidentiality, security, face recognition technology.*