УДК 343.9

Чуваткин Борис Юрьевич
Студент Института юстиции,
Уральский государственный юридический университет
Научный руководитель – Бахтеев Д. В., кандидат юридических наук
(г. Екатеринбург, Российская Федерация)
ch-boris97@mail.ru

ПРИМЕНЕНИЕ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ В БИОМЕТРИЧЕСКИХ СИСТЕМАХ ИДЕНТИФИКАЦИИ ЛИЦА ЧЕЛОВЕКА*

Аннотация: В работе рассматриваются понятия персональные данные и автоматизированная обработка персональных данных. Определяются типы персональных данных, закреплённых в национальных правопорядках европейских государств и в правопорядке Российской Федерации. Определяется понятие и особенности биометрических персональных данных в законодательстве Российской Федерации. Оговариваются изменения законодательства в работе с биометрическими персональными данными в России. Анализируется возможность использования в правоохранительной деятельности интеллектуальных биометрических систем идентификации лица человека.

Ключевые слова: восприятие лица человека, интеллектуальные системы, биометрические системы распознавания лица человека, категории персональных данных, биометрические персональные данные, особенности биометрических персональных данных, оператор.

В настоящее время биометрические технологии всё плотнее входят в жизнь каждого человека. Это связано с тем, что произошёл прорыв в области компьютерного обучения. Многие страны-члены Совета Европы, в том числе и Россия, ратифицировали на своей территории Конвенцию № 108 «О защите физических лиц при автоматизированной обработке персональных данных»[1].

* Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований в рамках научного проекта 18-29-16001\18 «Комплексное исследование правовых, криминалистических и этических аспектов, связанных с разработкой и функционированием систем искусственного интеллекта».

[1] Конвенция о защите физических лиц при автоматизированной обработке персональных данных (вместе с Поправками к Конвенции о защите физических лиц при автоматизированной обработке персональных данных (СДСЕ N 108), позволяющими присоединение европейских сообществ, принятыми Комитетом Министров в Страсбурге 15.06.1999) // Собрание законодательства. 03.02.2014. N 5. Ст. 419.

Данная конвенция подразделяет персональные данные на обычные и специальные персональные данные. Многие национальные правовые системы восприняли такое деление персональных данных, в то же время появляются и исключения из общего правила. Некоторые страны, такие как Россия, Словения и Италия, ввели особое правовое регулирование для биометрических персональных данных. Выделение ряда дополнительных типов персональных данных является рациональным, так как позволяет учесть особенности, характерные для данного типа сведений, что позволяет уменьшить возможность угрозы нарушения субъективных прав лиц при обработке персональных данных.

Понятие биометрических персональных данных в России закреплено в статье 11 Федерального закона «О персональных данных»[1]. Биометрические персональные данные – это сведения, характеризующие физиологические и биологические особенности человека, позволяющие оператору идентифицировать личность человека. Биометрическими персональными данными на основании данного закона являются: отпечатки пальцев и кистей рук, венозный рисунок кистей рук, сетчатка глаза, радужная оболочка глаза, геометрия лица человека, образцы голоса, ДНК субъекта персональных данных и иные биометрические характеристики человека, по которым возможно его идентифицировать. Список не является исчерпывающим, к примеру, существуют разработки по идентификации человека по походке. Обработка биометрических персональных данных разрешается при наличии согласия субъекта персональных данных, либо без согласия субъекта биометрических персональных данных в случаях, предусмотренных ч. 2 ст.11 данного закона, к примеру, при расследовании преступлений. В рамках европейского союза можно говорить о схожем, но более подробном нормативном закреплении использования персональных данных для предотвращения, расследования, обнаружения или преследования уголовных преступлений, закреплённом директивой N 2016/680[2].

Современный период времени требует использования современных криминалистических методов для расследования преступлений. Сущностные характеристики биометрических данных и компьютерная обработка биометрических персональных данных даёт возможность использовать эти инструменты для расследования преступлений. Основными особенностями,

[1] О персональных данных: Федеральный закон от 27.07.2006 N 152-ФЗ // Российская газета. 2006. 29 июля.

[2] О защите физических лиц при обработке персональных данных компетентными органами в целях предотвращения, расследования, выявления или уголовного преследования преступлений или исполнения уголовных наказаний, о свободном обращении таких данных, а также об отмене Рамочного Решения 2008/977/ПВД Совета ЕС: Директива N 2016/680 Европейского парламента и Совета Европейского Союза (Принята в г. Брюсселе 27.04.2016) // Official Journal of the European Union N L 119. 04.05.2016. P. 89. URL: http://eur-lex.europa.eu/.

позволяющими использовать биометрические данные в компьютерной обработке становятся:

1) Уникальность биометрических характеристик каждого человека. Например, человеческая ДНК, отпечаток пальца, геометрические характеристики лица человека присущи одному конкретному человеку, что позволяет осуществить его идентификацию.

2) Распространённость биометрических характеристик. Биометрические данные являются повсеместно распространёнными, что предусматривает возможность их сбора, накопления и обработки, что позволяет создать широкую базу данных для криминалистической идентификации.

3) Относительная устойчивость биометрических характеристик. В большинстве своём биометрические характеристики являются неизменяемыми, что позволяет получить верный результат идентификации на протяжении большого количества времени.

4) Возможность классифицировать биометрические характеристики. В ряде программ для автоматической обработки биометрических персональных данных используются алгоритмы выявления определённых особенностей, которые в дальнейшем записываются в базу в виде кода.

Л. Я. Драпкин, как и многие криминалисты, понимал важность идентификации человека для раскрытия и расследования преступлений. Использование портрета преступника: психологического, словесного и (или) фотокомбинированного позволяет успешно раскрывать и расследовать преступления[1]. Причиной этого является когнитивное восприятие лица человека, которое занимает одну из важнейших ролей в процессе социальной коммуникации. Сначала человек определяет физические характеристики лица другого человека, в дальнейшем происходит сравнение с характеристиками лиц, отразившимися в памяти отражающего субъекта, и после этого мозг человека даёт результат, знакомо ли лицо человека отражающему субъекту, либо нет. Учёными установлено, что за каждый из этапов распознавания лица человека отвечает определённый участок мозга, к примеру, когда человек видит чьё-то лицо, активизируется латеральная височно-затылочная (веретенообразная) извилина, которая с возрастом увеличивается в размерах за счёт роста миелиновых оболочек аксонов, для того чтобы распознавать большее количество лиц[2]. Данный биологический механизм когнитивного

[1] Драпкин Л. Я., Долинин В. Н., Шуклин А. Е. Использование криминалистического портрета преступника в расследовании серийных убийств // Электронное приложение к Российскому юридическому журналу. 2017. № 4. С. 93–101.

[2] Gomez J., Barnett M. A., Natu V. Microstructural proliferation in human cortex is coupled with the development of face processing // Science. 2017. Vol. 355. Issue 6320. URL: https://science.sciencemag.org/content/355/6320/68 (дата обращения 15.10.2019).

восприятия долгое время помогал правоохранительным органам расследовать и раскрывать преступления, но наука и техника не стоят на месте, появляются новые возможности воспроизведения биологических механизмов человека в технических и информационных областях знаний.

Новым витком развития идентификации лица человека выступают биометрические системы идентификации лица человека и интеллектуальные биометрические системы идентификации лица человека. Данные системы стараются воспроизводить этапы распознавания лица человека: производят считывание лица человека, заносят информацию по биометрическим характеристикам лица в сформированную базу, проводят сравнивание данных и выводят результат о идентификации лица с лицом, внесённым в базу или об отсутствии схожей информации.

Ранее интерес к использованию биометрических данных в идентификации лица человека в криминалистике был связан с введением биометрических паспортов в Российской Федерации[1], основным биометрическим параметром которых является изображение лица его владельца. В 2017 году был принят Федеральный закон № 482-ФЗ от 31 декабря 2017 г. «О внесении изменений в отдельные законодательные акты Российской Федерации»[2], названный в общем виде законом о биометрической идентификации. Данный закон закрепил создание единой биометрической системы, используемой в банковской деятельности, для того чтобы каждый пользовать мог удалённо воспользоваться банковскими услугами. Оператором данной системы является «Ростелеком», банки, хоть и собирают биометрические персональные данные, не имеют доступа к ним. При подключении систем банковского обслуживания к системе проверки биометрических данных при запросе получения услуги, банк видит лишь процент совпадения биометрических характеристик лица. Единая биометрическая система использует для идентификации два типа биометрических данных: изображение человека и его голос.

Введение единой биометрической системы может открыть новые возможность для развития криминалистической отрасли биометрической идентификации. Ведь именно в криминалистике чаще всего используются биометрические персональные данные человека, примером чего является проведение дактилоскопической экспертизы, габитоскопической экспертизы, фоноскопической экспертизы и многих других. В правоохранительной деятельности повсеместно распространена работа с отпечатками пальцев на

[1] Егоров Е. Е. О возможности использования правоохранительными органами биометрического метода распознавания лица // Информационная безопасность регионов. 2011. № 2. С. 113–117.

[2] О внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 31.12.2017 N 482-ФЗ // Российская газета. 2018. 9 января.

базе системы «Папилон». В то же время вводимая единая биометрическая система может быть интересна для сотрудников правоохранительных органов, так как сможет позволить сформировать широкую базу лиц, не только совершивших преступление и пропавших без вести, но и всех граждан, проживающих или находившихся на территории РФ. В правовом плане получение доступа правоохранительных органов к такой базе будет законно на основании ч. 2 ст. 11 ФЗ «О персональных данных».

Интерес для деятельности по расследованию преступлений представляет биометрическая идентификация лица человека. Для распознавания лица человека используются разные методы разработки программного обеспечения. Одним из методов является использование локальных алгоритмов, которые выделяют отдельные части лица человека, к примеру, подбородок, рот, нос и т. д. Другим способом является использование глобальных алгоритмов, где программа работает со всем лицом. Также существуют и смешанные алгоритмы, в которых используются и глобальные и локальные алгоритмы. При разработке биометрических систем в настоящее время часто используют нейросетевой метод разработки. В биометрических системах распознавания лица человека в большинстве случаев используются свёрточные нейронные сети. Свёрточная нейронная сеть, входящая в технологии глубокого обучения, первоначально разрабатывалась Яном Лекуном для распознавания образов. Свёрточная нейронная сеть обрабатывает полученные фотографии лиц с помощью биометрического алгоритма и переводит фотографию в массив точек, которые в дальнейшем преобразуются с помощью математического алгоритма (к примеру: SIFT, SURF, HOG) в массив чисел (дескриптор), на основании чего получается файл с последовательностью определённых чисел, который записывается в базу данных. В дальнейшем при обработке другой фотографии свёрточная нейронная сеть получает набор чисел (дескриптор) и сравнивает данный набор с наборами уже имеющимися в базе и выводит оператору результат о наличии либо отсутствии совпадений. Нейросетевой метод в настоящее время является очень популярным и используется в разработке и иных биометрических систем, так, одним из примеров может быть интеллектуальная система Манчестерского университета SfootBD[1], что возможно в скором времени позволит признать походку биометрическими персональными данными.

[1] Costilla-Reyes O., Vera-Rodriguez R., Scully P., Ozanyan K. B. Analysis of Spatio-Temporal Representations for Robust Footstep Recognition with Deep Residual Neural Networks // IEEE Transactions on Pattern Analysis and Machine Intelligence. 2019. Vol. 41. Issue 2. P. 285–296. URL: https://ieeexplore.ieee.org/document/8275035 (дата обращения 15.10.2019).

Доля российских организаций в разработке программ face recognition очень высока. Существует большое количество российских компаний занимающихся разработкой биометрических систем, как 2D, так и 3D распознавания лица человека в разных сферах. Примером может быть компания «Вокорд» разработавшая программу Vocord FaceControl 3D[1], для распознавания лиц в местах массового скопления людей. Данная программа использует синхронизацию снимков с разных ракурсов для построения 3D модели лица человека. В дальнейшем система сравнивает получившийся результат с эталонными снимками и в дальнейшем уведомляет оператора о наличии или отсутствии совпадений. Другим примером является компания VisionLabs, разрабатывающая программы биометрической идентификации лица человека для банковской сферы[2]. Разработкой биометрических систем распознания лиц занимаются и за рубежом. При наличии широкой базы лиц, созданной на основе единой биометрической системой, станет возможным использовать данные системы в повседневной деятельности правоохранительных органов в местах массовых скоплений людей и для идентификации человека по фотороботам и поиска лиц, совершивших преступления.

В то же время стоит сказать, что биометрическая идентификация лица человека и идентификация человека по паре биометрических характеристик не всегда может обеспечить надёжный результат. Существуют пути обхода данных систем, которые используются злоумышленниками для получения неправомерного доступа к информации и денежным средствам других лиц. Так, совсем недавно в издании BlackHat была опубликована статья[3], в которой раскрываются способы обхода биометрической идентификации лица человека с помощью внедрения поддельных аудио- и видеопотоков, сбора и использования биометрических данных, либо кражи биометрических данных для получения неправомерного доступа к источникам защищённым биометрической защитой. С развитием способов биометрической идентификации растёт и число способов обойти данные системы, что становится поводом задуматься о безопасности прав лиц, использующих данные системы.

Подводя итог, стоит сказать, что биометрические персональные данные всё плотнее входят в современную жизнь. Дальнейшее развитие и работа над

---

[1] VOCORD FaceControl 3D // Сайт компании «Vocord» [Электронный ресурс]. URL: http://old.vocord.ru/catalog/products/sistemy-videonablyudeniya/vocord-facecontrol-3d/(дата обращения 15.10.2019).

[2] Luna Platform // Сайт компании «VisionLabs» [Электронный ресурс]. URL: https://visionlabs.ai/ru/products/luna-platform (дата обращения 15.10.2019).

[3] Chen Y., Ma B., Ma Z. Biometric Authentication Under Threat: Liveness Detection Hacking // BlackHat [Электронный ресурс]. URL: https://www.blackhat.com/us-19/briefings/schedule/#biometric-authentication-under-threat-liveness-detection-hacking-16130 (дата обращения 15.10.2019).

созданием биометрических систем в Российской Федерации вне зависимости от направления деятельности данных систем будут открывать новые возможности для развития криминалистической науки. В настоящее время существует большое количество разработок в данной сфере и когда-нибудь данные системы займут своё место в криминалистике, наравне со способами обхода данных систем.

Список литературы

1. Драпкин Л. Я., Долинин В. Н., Шуклин А. Е., Использование криминалистического портрета преступника в расследовании серийных убийств // Электронное приложение к Российскому юридическому журналу. 2017. № 4. С. 93–101.
2. Егоров Е. Е. О возможности использования правоохранительными органами биометрического метода распознавания лица // Информационная безопасность регионов. 2011.- № 2. С. 113–117.
3. Chen Y., Ma B., Ma Z. Biometric Authentication Under Threat: Liveness Detection Hacking // BlackHat [Электронный ресурс]. URL: https://www.blackhat.com/us-19/briefings/schedule/#biometric-authentication-under-threat-liveness-detection-hacking-16130.
4. Costilla-Reyes O., Vera-Rodriguez R., Scully P., Ozanyan K. B. Analysis of Spatio-Temporal Representations for Robust Footstep Recognition with Deep Residual Neural Networks // IEEE Transactions on Pattern Analysis and Machine Intelligence. 2019. Vol. 41. Issue 2. P. 285–296. URL: https://ieeexplore.ieee.org/document/8275035.
5. Gomez J., Barnett M. A., Natu V. Microstructural proliferation in human cortex is coupled with the development of face processing // Science. 2017. Vol. 355. Issue 6320. URL: https://science.sciencemag.org/content/355/6320/68.

Boris Yu. Chuvatkin
Student of Institute of Justice of
Ural State Law University
Supervisor – D. V. Bakhteev, PhD (Law)
Ural State Law University
(Yekaterinburg, Russian Federation)
ch-boris97@mail.ru

PRACTICE OF APPLICATION OF INTELLECTUAL SYSTEMS IN BIOMETRIC SYSTEMS OF IDENTIFICATION OF THE PERSON OF THE PERSON

Abstract: In work concepts the personal data and the automated processing of the personal data are considered. Types of the personal data fixed in national laws and orders of the European states and in the law and order of the Russian Federation are defined. The concept and features of the biometric personal data in the legislation of the Russian Federation is defined. Changes of the legislation in work with the biometric personal data in Russia make a reservation. Use possibility in law-enforcement activity of intellectual biometric systems of identification of the person of the person is analyzed.

Keywords: perception of the person, intellectual systems, biometric systems of recognition of the person of the person, category of the personal data, biometric personal data, features of the biometric personal data, the operator.