УДК 351.745.7

Н. С. Делов
доцент кафедры криминалистики
и оперативно-розыскной деятельности
Ростовского юридического института МВД России,
кандидат юридических наук

ПРИМЕНЕНИЕ БИОМЕТРИИ В ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ

Решение как общих, так и частных задач оперативно-розыскной деятельности в большинстве случаев практически невозможно без установления личности лиц, причастных к противоправной деятельности.

Методы установления личности подразделяются на традиционные и современные. Традиционными являются опрос, осмотр документов, опознание, допрос свидетелей, получение информации от конфидентов и др. К современным методам относят биометрическую идентификацию (физиологические особенности личности), анализ ДНК, использование баз данных и информационных систем.

Физиологические особенности человека условно подразделяются на две группы:

− статистические: папиллярные узоры рук, анатомическое строение лица и др.

− динамические: голос, рукописный почерк, клавиатурный почерк, походка, жесты, рост, группа крови.

На сегодняшний день достаточное распространение получило применение видеокамер, с их помощью зачастую фиксируются лица правонарушителей. Видеокамеры расположены практически повсюду: на столбах, расположенных у проезжей части, что помогает идентифицировать лицо, находящееся за рулем транспортного средства; при входе в магазины, а также внутри них; в домофоны и т. д.

Отождествление личности, основанное на биометрических признаках, является перспективным направлением, позволяющим автоматизировать и повысить точность идентификации личности. Следует отметить, что оно основано на следующем:

1. Компьютерный анализ обуславливается применением мощных вычислительных ресурсов и алгоритмов искусственного интеллекта с целью дальнейшей обработки биометрических данных.

2. Биометрические персональные данные. Применение уникальных биологических и поведенческих характеристик человека, таких как следы рук, анатомическое строение лица, голос, походка и т. д.

3. Автоматизация процесса. Снижение человеческого фактора и повышение скорости идентификации, что особенно важно в ситуациях, требующих оперативного реагирования.

Согласно Федеральному закону от 27 июля 2006 г. № 152-ФЗ «О персональных данных», биометрические данные представляют собой сведения, характеризующие физиологические и биологические особенности человека. На основании этих данных возможна идентификация личности субъекта. По общему правилу обработка биометрических персональных данных (включая их сбор, хранение, использование, передачу и т. д.) допускается только при наличии письменного согласия субъекта персональных данных. Это необходимо для защиты прав граждан и предотвращения неправомерного использования их личных данных [1].

Отметим исключения из правил о согласии. К ним относятся случаи, предусмотренные ч. 2 ст. 11 Федерального закона «О персональных данных». Эти исключения установлены для случаев, когда обработка данных необходима для обеспечения государственных интересов:

− Законодательство об оперативно-розыскной деятельности (Федеральный закон № 144 от 12 августа 1995 г. «Об оперативно-розыскной деятельности» [2]) позволяет проводить оперативно-розыскные мероприятия, которые могут включать сбор и обработку биометрических данных без согласия субъекта, если это необходимо для выявления, предупреждения, пресечения и раскрытия преступлений.

− Законодательство о противодействии терроризму (Федеральный закон от 6 марта 2006 г. № 35 «О противодействии терроризму» [3]) также может предусматривать обработку биометрических данных без согласия субъекта в целях обеспечения национальной безопасности и предотвращения террористических актов.

Также могут быть иные случаи, предусмотренные федеральными законами, когда обработка биометрических данных без согласия необходима для решения важных государственных задач, например, для обеспечения безопасности на транспорте, в местах массового скопления людей и т. д.

Применение биометрических технологий в оперативно-розыскной деятельности сопряжено с рядом серьезных проблем: этические и правовые, технические, социальные и проблемы, связанные с развитием технологий.

Технические и социальные проблемы применения биометрических данных заключаются в том, что современные биометрические системы не работают безошибочно. Допущенные ошибки могут привести к ложным обвинениям и несправедливому задержанию. Хранение больших массивов биометрических данных требует надежной защиты от хакерских атак и утечек.

Широкое использование биометрии может вызвать недоверие со стороны общества, опасение нарушения прав человека. Неправильное применение биометрических данных может привести к дискриминации определенных групп населения. Немаловажным также является обучение сотрудников правоохранительных органов правильному использованию технологий и соблюдение этических норм.

Постоянное развитие технологий требует своевременного обновления систем и обучения сотрудников. Также требуется регулярное совершенствование мер защиты.

Соблюдение всех правил оперативными сотрудниками при использовании биометрических данных, а также при их обработке имеет критическое значение для правомерного и эффективного применения этих технологий в оперативно-розыскной деятельности и других сферах. Применение биометрических технологий в оперативно-розыскной деятельности является перспективным направлением. Для того чтобы эти технологии приносили пользу, а не вред, необходимо тщательно учитывать все потенциальные риски и разрабатывать меры по их минимизации. Крайне важно соблюдать баланс между обеспечением безопасности и защитой прав и свобод граждан.

Список основных источников

1. О персональных данных [Электронный ресурс] : Федер. закон от 27 июля 2006 г. № 152-ФЗ : в ред. от 8 авг. 2024 г. Доступ из справ.-правовой системы «КонсультантПлюс». Вернуться к статье

2. Об оперативно-розыскной деятельности [Электронный ресурс] : Федер. закон от 12 авг. 1995 г. № 144-ФЗ : в ред. от 29 дек. 2022 г. Доступ из справ.-правовой системы «КонсультантПлюс». Вернуться к статье

3. О противодействии терроризму [Электронный ресурс] : Федер. закон от 6 марта 2006 г. № 35 : в ред. от 28 дек. 2024 г. Доступ из справ.-правовой системы «КонсультантПлюс». Вернуться к статье