Правовые вопросы применения системы виброизображения в качестве средства технического профайлинга

Анисимова Н.Н, Бирагов И.Л., Минкин В.А.

Не вызывает сомнения, что общество обязано защищать себя от терроризма, не нарушая при этом права граждан. В последнее время одним из наиболее эффективных средств борьбы с угрозами террористического характера являются биометрические технологии. При этом противники массового применения биометрии утверждают, что снятие и использование биометрических характеристик (биометрических параметров) человека ущемляет права граждан и противоречит Российской конституции. Попробуем рассмотреть эту проблему как с правовой, так и научной точки зрения.

Известно, что существует множество различных определений понятий «терроризм», «биометрия» и «свобода личности», не менее сотни для каждого. В рамках данной статьи мы будем использовать существующие в российском законодательстве определения терминов биометрии, терроризма и свободы личности, которые практически совпадают с общепринятыми в международной практике определениями.

Терминология и законодательство

Биометрия – это наука, изучающая биологические и поведенческие характеристики человека. Биометрические технологии используют биологическую и (или) поведенческую информацию для идентификации личности или психоэмоционального состояния человека, а под биометрическими данными понимаются любые данные, характеризующие какое-то биометрическое свойство, например, данные датчиков или данные изображения [1].

Терроризм – это идеология насилия и практика воздействия на принятие решения органами государственной власти, органами местного самоуправления или международными организациями, связанные с устрашением населения и (или) иными формами противоправных насильственных действий [2].

Права и свободы человека и гражданина подробно изложены в главе 2 Конституции Российской Федерации [3], они составляют основы правового статуса личности в России и не могут быть изменены иначе как в порядке, установленном настоящей Конституцией. Основные права человека могут быть ограничены при условии, что такие ограничения законны и необходимы: для уважения прав и репутации других лиц; для охраны государственной и общественной безопасности, общественного порядка, а также здоровья и нравственности населения [4].

Не подлежат ограничению права и свободы, предусмотренные статьями 20, 21, 23 (часть 1), 24, 28, 34 (часть 1), 40 (часть 1), 46 - 54 Конституции Российской Федерации (ст. 56, гл. 2).

Наиболее интересны, с точки зрения рассматриваемого вопроса, статьи 17, 20, 21, 22, 23 и особенно п.1 статьи 24.

Пункт 1 статьи 24 гласит: «Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются».

Вопрос в том, что представляет собой «информация о частной жизни» и насколько любая информация о человеке является частной.

Жить в обществе и быть свободным от общества невозможно. Работа правоохранительных органов, например, не представляется возможной без сбора и архивации таких биометрических характеристик человека как его внешнее изображение (фотография) и отпечатков пальцев, хотя и предусматривает ограниченный доступ к базам данных.

Частично обоснованность ограниченного применения биометрии подтверждается и существующим российским законодательством, определяющим порядок работы с

биометрической информацией в целом ряде федеральных законов, постановлений правительства и приказов по министерствам и ведомствам [5, 6, 7, 8]. При этом, до недавнего времени, биометрические данные разделялись на поведенческие и биологические, т.е. по временному принципу их получения на статические и динамические. Также существует разделение биометрических данных по принципу их применения, на данные для идентификации личности (биометрические системы второго поколения) и для идентификации состояния человека (биометрические системы третьего поколения) [9, 10].

Важный шаг вперед сделан в недавно принятом федеральном законе Российской Федерации от 27 июля 2006 г. N 152-ФЗ «О персональных данных» [11], где разграничены понятия «персональные данные» и «общедоступные персональные данные», которые могут быть отнесены и к биометрической информации. Однако расшифровка этого понятия «общедоступные персональные данные» в данном законе допускает различные толкования в других федеральных законах, что значительно снижает эффективность от введения данного термина.

Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

В федеральном законе «О персональных данных» оговорен и доступ к обработке, получению и использованию персональных данных не требующих согласия субъекта – в случаях, предусмотренных ст.6, п.2.1; ст.9, п.2.; ст.11, п. 2., естественно при выполнении требований Конвенции по правам человека [12].

Следует отметить, что негласное получение биометрической информации попадает по ограничения, оговоренные в Постановлении Правительства РФ от 1 июля 1996 г. N 770 [8]. В данном документе оговорено, что использование специальных технических средств для негласного визуального наблюдения и документирования требует обязательного лицензирования.

Доступные и закрытые персональные данные

То, что человек получает до 90% информации в мозг в виде видео изображения или зрительных образов, произошло далеко не случайно. В процессе эволюции именно этот способ получения информации об окружающем мире оказался наиболее эффективным. Во многом, благодаря этому, человек занял ведущее положение в природе. Если бы запах оказался информативней изображения, то человек и собака поменялись местами в природной иерархии. Естественно, что люди могут осуществлять функцию распознавания или идентификации, благодаря открытости видео информации о другом человеке. Изображение лица человека – это изначально открытая природой информация, поэтому накладывать законодательные ограничения на ее использование вряд ли логично. Как это ни странно, никто ранее не предлагал естественный способ классификации биометрических параметров по принципу природной открытости, хотя данное разделение представляется очевидным. До настоящего времени большинство дискуссий о применении биометрии носило крайний характер. Одни предлагали запретить всю биометрию вообще, другие предлагали «просвечивать» всех насквозь любыми техническими средствами.

Крайние точки редко находят поддержку, возможно сложности внедрения биометрии частично связаны с её нелогичным применением. Попробуем продолжить рассуждения о разграничении биометрических параметров (личных и доступных) на основе теории эволюции, здравого смысла и имеющегося опыта.

Определим, какая биометрическая информация о человеке является открытой и доступной для обозрения. Внешняя визуальная информация использовалась для человеческой идентификации задолго до появления автоматизированных технических

средств. Изображение лица человека является общедоступным для неограниченного круга лиц вне зависимости от согласия или несогласия субъекта этих данных. К таким открытым биометрическим характеристикам, безусловно, можно отнести визуальное изображение человека, лица, голос, форму руки и, вероятно, отпечаток пальца. Многие могут с нами не согласиться по поводу отпечатков пальцев, но вряд ли будут возражать по поводу открытости лица и голоса в подобной классификации.

Что касается отпечатков пальцев, в причислении их к открытым признакам, существует следующая логика: человек оставляет множество следов отпечатков пальцев в течение дня, которые легко доступны для просмотра. В природе ничто не происходит случайно, и, если в процессе эволюции природа «наградила» человека отпечатками пальцев, то, вероятно, эта визуальная генетическая характеристика оказалась целесообразной. Отпечатки пальцев человека частично аналогичны следам, которые оставляют животные. Если для выживания видов природа позволяет находить животным друг друга по следам, то так же природа позволяет определять присутствие человека по оставленным отпечаткам пальцев и использовать отпечатки пальца для идентификации личности.

Существует другой ряд биометрических параметров, получение которых невозможно без применения технических средств. Это идентификация личности по сетчатке глаза, по кровеносным сосудам и венам, а также получение информации о психоэмоциональном состоянии человека с помощью систем ЭЭГ, КГР (детекция лжи), датчиков дыхания и давления. Эти параметры не являются естественно открытыми, и их использование может быть ограничено.

Объективная физическая информации не должна зависеть от метода ее получения. Согласно основному принципу метрологии, результат измерения не должен зависеть от измерительного средства, а видеоинформация, регистрируемая телекамерой, аналогична зрительной информации, регистрируемой человеком. Если законодательно не запрещено одному человеку смотреть на другого, то телевизионное наблюдение в аналогичной ситуации не может рассматриваться, как вмешательство в частную жизнь гражданина.

При таком подходе использование технических средств для получения скрытых природой биометрических параметров нарушает естественную неприкосновенность частной жизни граждан и должно допускаться только с согласия граждан. Например, анализ детекции лжи с применением контактного полиграфа является получением скрытой природой информации и в соответствии с предлагаемой классификацией должен требовать письменного разрешения граждан на его проведение.

Введение законодательного разграничения на открытые и закрытые биометрические параметры позволит существенно упростить практику внедрения биометрических технологий. Открытые или общедоступные биометрические параметры не должны подвергаться ограничениям в доступе, в то время как получение закрытых биометрических данных должно быть возможно только с разрешения их владельца.

Безопасность аэропорта. Видеоинформация и профайлинг.

Рассмотрим пример использования различных открытых биометрических параметров для обеспечения безопасности на транспорте и, прежде всего, в аэропортах.

Согласно Федеральному закону «О транспортной безопасности» [13] транспортная безопасность – состояние защищенности объектов транспортной инфраструктуры и транспортных средств от актов незаконного вмешательства.

Большой популярностью у преступников стало пользоваться совершение террористических актов с использованием транспорта, в том числе с использованием воздушных судов. В связи с этим требуется разработка специальных мер защиты, способных значительно снизить риск проникновения на борт самолета лиц, представляющих угрозу общественной безопасности. В связи с этим в последнее время широкое распространение получил, так называемый профайл-метод или профайлинг.

Основной целью профайлинга является выявление потенциально опасных пассажиров, его основой – визуальная диагностика психоэмоционального состояния человека.

Однако основным недостатком визуальной диагностики психоэмоционального состояния человека по-прежнему является определенная сложность его объективной идентификации даже с учетом ошибок личностного и психологического происхождения при использовании профайл-метода. Не всегда удается выявить потенциальных преступников в пассажиропотоке, используя для этого лишь социально-психологические методы. Необходимо внедрение специальных технических средств, способных отражать объективные данные о потенциальной угрозе для окружающих того или иного пассажира. Данные средства призваны оказать существенную помощь людям, чьим профессиональным долгом является обеспечение безопасности и охрана правопорядка.

Одним из последних достижений в этой области является разработка биометрической технологии виброизображения, позволяющей анализировать двигательную активность человека и делать вывод о его психоэмоциональном состоянии на основе данных систем видеонаблюдения.

Служба авиационной безопасности (САБ) обеспечивает 100% досмотр пассажиров и багажа с помощью различных технических средств, использование которых определено Приказом Минтранса России «Об утверждении Правил предполетного и послеполетного досмотров» [14] (раздел II, п.10). Этот же приказ установил право сотрудников САБ и органов внутренних дел проводить опрос пассажиров в целях определения потенциально опасных и наблюдать за поведением пассажиров (раздел V, п.41).

Однако существующее законодательство, в том числе и закон «О персональных данных», создает неоднозначное понимание возможности применения биометрических методов для массового контроля. Рассматривая изображение лица человека как персональные или биометрические данные, мы попадаем под все ограничения связанные с этим понятием, а именно: сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность (биометрические персональные данные), могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных.

Возникает парадоксальная ситуация, когда субъективный человеческий анализ поведения является допустимым, а автоматизированный объективный анализ требует получения специального разрешения, в то время когда одним из принципов построения надежной системы безопасности является минимизация человеческого фактора.

Даже если подготовить специальный федеральный закон о безопасности на транспорте и в аэропортах, который позволит снять эту проблему, то окажется, что применение любой системы видеонаблюдения является незаконным, так как необходимо вначале получить письменное разрешение у каждого человека (в том числе и преступника) на видеосъемку, и только потом осуществлять запись видеоинформации.

Заключение

Законодательное разграничение полномочий между открытыми (общедоступными) и закрытыми биометрическими данными позволит с одной стороны упростить применение комфортных для граждан биометрических технологий и повысить безопасность населения, при этом с другой стороны, внесет научный подход и логику в законодательство, лишив сторонников лжесвобод аргументации в ограничении прав личности при проведении биометрического контроля.

Список литературы:

1. ГОСТ Р ИСО/МЭК 19794-1-200-1. Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными.Часть 1. Структура.
2. Федеральный закон Российской Федерации от 6 марта 2006 г. N 35-ФЗ «О противодействии терроризму». Опубликовано 10 марта 2006 г.
3. Конституция Российской Федерации (опубликовано 25 декабря 1993 года).
4. Права человека и гуманитарное право в профессиональной правоохранительной деятельности. Тезисы книги «Служить и защищать». МККК, отдел связей с вооруженными силами и силами безопасности. 2002 г., стр.16.
5. Федеральный закон от 8 августа 2001 г. N 128-ФЗ «О лицензировании отдельных видов деятельности» (с изменениями от 13, 21 марта, 9 декабря 2002 г., 10 января, 27 февраля, 11, 26 марта 2003 г.)
6. Уголовный кодекс Российской Федерации (в редакции от 28.12.2004 г.) Статья 137. Нарушение неприкосновенности частной жизни.
7. Федеральный закон от 12 августа 1995 г. N 144-ФЗ «Об оперативно-розыскной деятельности» (с изменениями и дополнениями от 18 июля 1997 г., 21 июля 1998 г., 5 января, 30 декабря 1999 г., 20 марта 2001 г., 10 января, 30 июня 2003 г.)
8. Постановление Правительства РФ от 1 июля 1996 г. N 770 «Об утверждении Положения о лицензировании деятельности физических и юридических лиц, не уполномоченных на осуществление оперативно-розыскной деятельности, связанной с разработкой, производством, реализацией, приобретением в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации, и перечня видов специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации в процессе осуществления оперативно-розыскной деятельности» (с изменениями от 15 июля 2002 г.)
9. Минкин В.А. Биометрия. От идентификации личности к идентификации мыслей, IDMagazine, N3, 2002 г.
10. Полонников Р.И. Основные концепции общей теории информации. СПб, Наука, 2006 г.
11. Федеральный закон Российской Федерации от 27 июля 2006 г. N 152-ФЗ «О персональных данных» (опубликовано 29 июля 2006 г.)
12. Европейская конвенция о защите прав человека и основных свобод (Рим, 4 ноября 1950 г. Официальный перевод на русский язык).
13. Федеральный Закон Российской Федерации от 9 февраля 2007 года N16-ФЗ «О транспортной безопасности» (Опубликовано 14.02.2007 г.).
14. Приказ Минтранса России от 25.07.07 (опубликован 17.08.07) №104 «Об утверждении Правил предполетного и послеполетного досмотров» (раздел II, п.10).

Справка об авторах:

Анисимова Надежда Николаевна – Старший преподаватель Кафедры подготовки сотрудников в сфере транспортной безопасности Центра подготовки сотрудников в сфере транспортной безопасности ВИПК МВД России.
142022 Московская обл., г.Домодедово, мкр. Авиационный, ул. Пихтовая, д.3, тел./факс: (495) 736 92 30.
E-mail: Anisimova2011@yandex.ru

Бирагов Игорь Лазаревич – Начальник Центра подготовки сотрудников в сфере транспортной безопасности ВИПК МВД России.
142022 Московская обл., г.Домодедово, мкр. Авиационный, ул. Пихтовая, д.3, тел./факс: (495) 736 92 30.

Минкин Виктор Альбертович – Заместитель директора ООО «Многопрофильное Предприятие «Элсис».
194223 г. Санкт-Петербург, пр. Тореза, 68, тел/факс: (812) 552 67 19.
E-mail: minkin@elsys.ru