УДК 34.04

БИОМЕТРИЯ – БУДУЩЕЕ НОРМОТВОРЧЕСТВО

Горелов Андрей Сергеевич,
место работы - ПАО Сбербанк, Поволжский банк
адрес места работы: г. Самара, ул. Ново-Садовая, д. 305
главный юрисконсульт Юридического управления Поволжского банка
Недогреева Светлана Геннадьевна
место работы - ПАО Сбербанк, Поволжский банк
адрес места работы: г. Самара, ул. Ново-Садовая, д. 305
старший юрисконсульт Юридического управления Поволжского банка

Аннотация: В начале статьи изложен краткий обзор данных социального опроса по реальному развитию биометрии и актуальная статистика по количеству совершенных преступлений в компьютерной сфере. В целом статья посвящена анализу недостаточного правового регулирования развития технологии биометрии в практике частных компаний (за исключением коммерческих банков). Внесены предложения по возможному совершенствованию их нормативного регулирования.

Ключевые слова: коммерческие автоматизированные информационные биометрические системы персональных данные; локальные системы.

Summary: At the beginning of the article, a brief overview of the data of the social survey on the real development of biometrics and current statistics on the number of crimes committed in the computer sphere is presented. In general, the article is devoted to the analysis of insufficient legal regulation of the development of biometrics technology in the practice of private companies (with the exception of commercial banks). Proposals were made for possible improvement of their regulatory regulation.

Keywords: commercial automated information biometric systems; personal data; local systems.

В начале данной статьи уместно вспомнить мысль, высказанную в работах К. Маркса о том, что однажды наступит такой этап развития общества, когда: «… мерой богатства будет отнюдь уже не рабочее время, а свободное время» (т. 46, ч. II, с. 217) [1]. Объективно, что в настоящее время это технически достижимо. Развитие цифровых технологий, основанных на биометрических данных физических лиц, будет высвобождать их же личное время, ранее необходимое на получение и предоставления различных услуг. Спектр применения данной технологии субъектами экономической деятельности очень велик: крупный бизнес – корпорации, операторы сотовой связи, производства, торговые сети; средний бизнес – логистика / склады, торговые и учебные / экзаменационные центры, медицинские центры, концертные залы, аренда транспорта; мелкий бизнес – частные детские сады, общественные объекты питания и т.д. Применяя данные технологии, вышеуказанные организации будут вправе создавать и уже создают в настоящее время, свои собственные - коммерческие автоматизированные информационные биометрические системы персональных данных (далее по тексту – локальные системы).

Использование технологии первоначально было связано с простыми операциями: с контролем входа/выхода и перемещения по объекту с созданием различных прав доступа; учет графика рабочих смен; фиксация действий; учет рабочего времени и фиксация нахождения на рабочем месте. В настоящее время данная технология уже используется в работе с более рискованными операциями: бесконтактный доступ к услугам (государственным, муниципальным, социальным, финансовым и т.д.); бесконтактный доступ к информации. Возможное будущее - это внедрение биометрии в избирательное право и иные процессы, связанные уже с суверенитетом стран.

Однако, в настоящее время результат социологического опроса среди совершеннолетних владельцев банковских карт в России, проведенного Fabrizio Ward по заказу Visa в январе-феврале 2020 года, показывает, что

россияне больше доверяют биометрической информации, чем паролям и ПИН-кодам, но используют её значительно реже.

Также было установлено, что и уровень доверия общества к одним и тем же технологиям биометрии различен. Банки и платежные системы опередили социальные сети, производителей мобильных телефонов и сотовых операторов по уровню доверия. Так, 48% респондентов доверяют хранение биометрических данных банкам и платежным системам. Еще 26% - производителям мобильных телефонов. 17% - операторам сотовой связи, 12% - социальным сетям [2].

В этой связи уместно рассмотреть и статистику по удельному весу преступлений, совершенных с использованием информационных телекоммуникационных технологий или в сфере компьютерной информации. На декабрь 2020 г. их количество составляет 25 % от общего числа преступлений, а именно: в сети «Интернет» - 300 337, средств мобильной связи – 218 739, расчетных (пластиковых) карт – 190 167, компьютерной техники – 28653, программных средств – 10 050; фиктивных электронных платежей – 1374 [3].

Вероятно, что развитие биометрических технологий позволило бы снизить вышеуказанное количество преступлений и сохранить имущество граждан.

Так почему общество не использует возможность снижения количества преступлений за счет совершенствования технологий? Почему человек не спешит за счет биометрии высвобождать и инвестировать свое личное время в иные полезные услуги (например - культуру, спорт, развлечения)? Почему граждане склонны с большим доверием относиться к тем же технологиям, но предоставляемым именно банками, а не иными субъектами экономической деятельности?

На наш взгляд, ответы на эти вопросы все-таки относятся к отрасли права.

В настоящее время система нормативно-правового регулирования банковского сектора РФ **четко структурирована**, а также действует эффективный банковский (ЦБ РФ) и иной государственный надзор (например – Прокуратура РФ, Роспотребнадзор) за их деятельностью. Банки строго соблюдают действующее законодательство. Следовательно, граждане интуитивно понимают, что государство контролирует деятельность банков и банкам можно доверять. Таким образом, при работе с банками вопрос технологий для граждан уходит на второй план, переходя к принципу доверия банковской системе в целом.

Напротив, на законодательном уровне **отсутствует четкая**, согласованная система нормативно-правового регулирования локальных систем персональных данных, что, в свою очередь, не позволяет организовать эффективный надзор за их деятельностью.

Стандарты организации обработки персональных данных, технологические решения, а, следовательно, и строгое исполнение требований норм права и безопасности их хранения, непрозрачны для большинства пользователей услуг частных организаций, чья деятельность иногда ограничена только одним регионом или городом.

Более того, разрозненность видов услуг не позволяет добиться аналогичного уровня доверия, как в финансовой отрасли, и по этой причине четкое законодательное регулирование, контроль за строгим исполнением, безопасностью технологией в коммерческих системах выходит на первый план. Следовательно, глобальное развитие технологий требует от законодателя повышения уровня правовой определенности в отношениях физических лиц и субъектов экономической деятельности.

В данном разделе следует отметить, что согласно ряда публикаций в СМИ в ближайшей перспективе не следует ожидать массового внедрения биометрических технологий в деятельности небольших коммерческих структур по причине повышенных требований к обработке биометрических данных, низком спросе на данную услугу, дороговизне технологий [4].

Однако, эти причины не должны останавливать развитие нормативно-правового регулирования внедрения и применения биометрических технологий в иных отраслях экономики (помимо финансового сектора).

В настоящее время ФЗ от 27.07.2006 г. № 152-ФЗ «О персональных данных» в целом регулирует требования ко всем информационным системам персональных данных (государства и субъектов экономической деятельности), но его нормы не охватывают всего спектра общественных взаимосвязей и возможных проблем в технологии биометрии.

Более того, наглядным примером отсутствия четкой системы являются сами нормы данного закона, а именно ФЗ от 27.07.2006 г. № 152-ФЗ «О персональных данных» имеет в своём составе статью 13 «Особенности обработки персональных данных в государственных или муниципальных информационных системах персональных данных», но не имеет аналогичной статьи о локальных системах персональных данных [5].

Данный закон ограничивается только нормами о том, что лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные настоящим Федеральным законом (ч. 3 ст. 6). Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом (ст. 7).

Однако, оператор самостоятельно определяет его политику в отношении обработки персональных данных (ч. 3 ст. 6). Требования к лицам, ответственным за организацию обработки персональных данных в организациях, весьма декларативны (ч. 4 ст. 22.1). Особый режим защиты персональных данных установлен законодателем только при обработке их в государственных информационных системах (ч. 8 ст. 19). Для прочих операторов установлены общие требования (ч. 1 ст. 19).

На наш взгляд, вышеуказанные нормы ФЗ от 27.07.2006 г. № 152-ФЗ «О персональных данных» более абстрактны, чем конкретны, но где нет конкретности, то и нет надлежащего поведения, регулирования, контроля. Более того, биометрические персональные данные регулируются всего одной статьей (ст. 11). Внесение изменений в отдельные законодательные акты РФ ограничилось только разрешением использования биометрических данных граждан [6]. В связи с этим, считаем, что замалчивание проблем вызывает только чувство стихийности и бесконтрольности данного рынка услуг.

В противоположность данного мнения можно привести только один пример, когда законодатель все же установил определенные правовые нормы в отношении использования биометрических персональных данных, а именно случаи использования биометрических данных при проведении видеосьемки системами видеонаблюдения, устанавливаемыми в настоящее время повсеместно. Необходимо обратить внимание, что видеокамера фиксирует, в частности, биометрические данные человека, т.е. те данные, с помощью которых возможно установить личность человека, соответственно, на хранение, использование и передачи третьим лицам этой видеозаписи необходимо согласие граждан, попавших в поле зрения камеры. Относительно данного вопроса, законодатель разъяснил случаи использования изображения человека, полученного в ходе проведения видеосъёмки без его согласия, указав в ст. 152.1 ГК РФ [7]. Об отсутствии необходимости получения согласия на использование биометрических персональных данных субъекта, в случаях, если изображение гражданина получено при съемке, которая проводится в местах, открытых для свободного посещения, или на публичных мероприятиях (собраниях, съездах, конференциях, концертах, представлениях, спортивных соревнованиях и подобных мероприятиях), либо использование изображения осуществляется в государственных, общественных или иных публичных интересах. Кроме того, как разъяснил Роскомнадзор: «посетители указанных публичных мест должны заранее предупреждаться их администрацией о

возможной фото, видеосъемке соответствующими текстовыми и/или графическими предупреждениями» [8].

Однако, установленный порядок на практике часто не соблюдается, поскольку не все организации, открытые для публичного посещения, утруждают себя размещением необходимых предупреждений, и как следствие, лишают гражданина права на получение информации о возможном сборе его персональных данных.

Крайне важно отметить, что процесс сбора, обработки, хранения биометрических персональных данных по своей сути порождает юридический факт появления цифровой копии конкретного человека [9], который реально является субъектом права (ГК РФ) и носителем суверенитета (Конституции РФ). Следовательно, подобного скудного правового регулирования биометрических технологий катастрофически недостаточно. Ведь именно распоряжения, полученные от данной цифровой копии человека, будут восприниматься программным обеспечением как воля реального человека (в зависимости от цели обработки персональных данных и заключенного договора с оператором). Следовательно, столь существенные отношения не могут подстраиваться под несовершенный закон, что можно выразить фразой Уинстона Черчиля об игре в гольф: «Гольф – это бесплодная попытка отправить неуправляемый шар в недосягаемую лунку инструментом, совершенно для того не приспособленным» [10].

Как указано выше государственные информационные биометрические системы будут надлежащим образом защищены, что будет являться гарантией достоверности волеизъявления человека (допустим при полном переходе избирательной системы страны на биометрические технологии). Но при работе в различных локальных системах, которые могут быть созданы на всевозможных технических решениях и принципиально отличных друг от друга, **не целесообразно полагаться на презумпцию достоверности волеизъявления.**

Полагаем, что в этих случаях требуется более объективное правовое подтверждение наличия истинности воли человека на совершение сделки и согласия на предоставление услуги. На наш взгляд, данное подтверждение **невозможно достичь** путем введения любого технического решения (примитивного подтверждения в программе), а возможно достичь только целостным и комплексным подходом законодателя к нормотворчеству в сфере развития биометрических систем и их безопасности; конкуренции субъектов экономической деятельности (производителей и операторов); правовой определенности для пользователей.

Следуя простой логике, конструкция права и технологий локальных систем должна быть точной копией аналогичной государственной системы. Однако, данный принцип недопустим в биометрии, требующей решения сложнейших технических задач, а также поиска путей снижения стоимости программного обеспечения / его обслуживания с целью массового применения в деятельности коммерческих организаций.

Вектор развития нормотворчества дал Президент Российской Федерации В.В. Путин, который в своем Послании Федеральному собранию от 15 января 2020 г. подчеркнул, что «**сегодня скорость технологических изменений в мире многократно возрастает**, и мы должны создать собственные технологии и **стандарты** по тем направлениям, которые определяют будущее. Речь прежде всего об искусственном интеллекте, цифровых технологиях» [11].

Следовательно, с точки зрения нормативно-правового регулирования стандарты обработки биометрических персональных данных в коммерческих локальных системах и техническая сторона процесса должна быть максимально четко обозначены, но разделены друг от друга. Техническая часть процесса должна отвечать скорости технологических изменений в мире.

На наш взгляд, вся совокупность правоотношений в обработке биометрических персональных данных в том числе в коммерческих

локальных системах должна регулироваться **отдельным федеральным-конституционным законом (ст. 108 Конституции РФ)** в связи с тем, что они затрагивают многие основные права граждан страны (ст.ст. 17, 23, 24, 29, 35, 37, 39, 41, 43, 44, 45, 46 Конституции РФ). **Многие будущие положения национального закона можно разработать, используя нормы Регламента N 2016/679 Европейского парламента** и Совета Европейского Союза "О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных)" [12]. Это также позволит согласовать нормы национального законодательства с зарубежным, что также положительно повлияет на унификацию стандартов в части технических решений в биометрии. Однако, не углубляясь в нормы вышеуказанного Регламента, считаем, что **главной задачей нормативно-правового регулирования национального права (будущего ФКЗ)** должно являться создание организационной системы предоставления услуг, основанной на неприязни удешевления технологий биометрии за счет нарушения базовых принципов её безопасности для конечных пользователей. Функционирование данной системы должно быть основано на принципах взаимосвязи правовых и технических процессов (связанных с безопасностью).

На наш взгляд, лучшие технические решения по безопасности биометрических персональных данных должны преобразоваться в правовые нормы федерального масштаба, а не регулироваться только Постановлением Правительства РФ [13] и внутриведомственными приказами.

Также правовой тренд должен следовать по пути того, что высоко рискованные операции не должны быть исключительно основаны на технологии биометрии. Это допустимо только на простых операциях фиксации: доступа к помещению; поведения; времени нахождения. **Однако, доступ к информации и услугам должен в себе комбинировать технологии биометрии и «традиционных» мер сохранения безопасности**

данных (одноразовые пароли, СМС сообщения, ПИН-код и т.д.). Взаимосвязи данных систем позволят выявлять различные отклонения еще до возникновения негативных последний и рисков.

Полагаем, что локальная система не должна хранить одновременно биометрические данные, иные персональные данные клиента, а также сведения о постоянных паролях клиента в ней. Нарушение данного принципа может полностью скомпрометировать всю систему биометрии при успешной хакерской атаке на локальные системы даже небольших операторов.

Также закон должен четко закрепить ответственность юридических лиц и должностных лиц операторов, а также ответственность компаний **поставщиков / разработчиков своего собственного программного обеспечения** и их должностных лиц за нарушение однородности требований защиты данных (каналы, хранилища, криптография). Соблюдение этих требований обоюдно необходимо и рынку биометрии, и пользователям их услуг, ведь наиболее болезненно и остро воспринимается обществом любая «утечка» информации и это подрывает доверие к технологии в целом.

С целью повышения ответственности вышеуказанных лиц, а также вовлеченности граждан в процесс использования биометрических данных необходимо провести широкое общественное обсуждение инициатив, в **частности, решения вопроса о возможности установления уголовной ответственности для разработчиков/производителей биометрических систем в связи с умышленным «удешевлением» программ, используемых для процесса сбора и хранения биометрических данных и, как следствие, «утечки» информации из реестра**. Полагаем, что это позволит осознать ответственность конкретных должностных лиц за свои действия и повысит качество предоставляемых услуг.

Однако, нормы данного закона не должны содержать техническую часть обозначенной сферы применения. Минимально необходимые стандарты технической части процесса должны формироваться

государственными контролирующими организациями совместно с профессиональными участниками данного рынка по созданию технологий биометрии.

Выполнение задачи по повышению технических стандартов возможно достичь путем внесения в данный закон соответствующих норм, стимулирующих государство **поддерживать** частные компании по разработке программного обеспечения **путем** координации их деятельности, развития научных, информационных и профессиональных интересов, выработки обязательных минимальных технических требований к программному обеспечению в целях защиты биометрических персональных данных в коммерческих системах, выработки иных рекомендаций.

Данные мероприятия позволят повысить доверие общества к данным технологиям.

В связи с вышеизложенным, следует сделать вывод, что для развития процесса сбора биометрических данных с самого начало необходимо создание и использование дорогих и качественных технологий, установление четких стандартов процесса и обозначение контролирующих функций государства.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Научный коммунизм [Электронный ресурс] // http://www.tapemark.narod.ru/kommunizm/184.html

2. Россияне считают биометрию более надежной [Электронный ресурс] // http://www.google.com/amp/s/ www.kommersant.ru/amp/4302060/

3. Ежемесячный сборник о состоянии преступности в России [Электронный ресурс] // http://crimestat.ru/analytics

4. Биометрию собрали в поправки [Электронный ресурс] // http://www.google.com/amp/s/ www.kommersant.ru/amp/4614043/

5. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (ред. от 30.12.2020) [Электронный ресурс] // КонсультантПлюс.

http://fedconsultant.ca.sbrf.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=372838&div=LAW&rnd=E86F58D006D6A20960F8B5526A536E92#03415902806368553

6. Федеральный закон от 29.12.2020 N 479-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации" (ред. от 29.12.2020) [Электронный ресурс] // КонсультантПлюс. http://fedconsultant.ca.sbrf.ru/cons/cgi/online.cgi?req=doc&ts=1674378721071574585186546 89&cacheid=495F362FEBC668F80FDB6D3A31897F64&mode=splus&base=LAW&n=372645&rnd=803DCEC3CCFDF9F8EC39BC40029091A2#0027441673892454776

7. "Гражданский кодекс Российской Федерации (часть первая)" от 30.11.1994 N 51-ФЗ (ред. от 08.12.2020) [Электронный ресурс] // КонсультантПлюс. http://fedconsultant.ca.sbrf.ru/cons/cgi/online.cgi?rnd=93105D06B1B6493BE642EEAB23CFBB45&base=LAW&n=370265&dst=4294967295&cacheid=C8BC3E469B1852262A4C20B4B8FC2762&mode=rubr&req=doc#06487113600981784

8. <Разъяснения> Роскомнадзора "О вопросах отнесения фото- и видео-изображения, дактилоскопических данных и иной информации к биометрическим персональным данным и особенности их обработки" [Электронный ресурс] // КонсультантПлюс. http://fedconsultant.ca.sbrf.ru/cons/cgi/online.cgi?req=doc&ts=1629366480022028440795587412&cacheid=BA25C7BC8C30421ED42C71060E5CCE2F&mode=splus&base=LAW&n=151311&rnd=93105D06B1B6493BE642EEAB23CFBB45#0385394152340946

9. "Дорожная карта развития "сквозной" цифровой технологии "Технологии виртуальной и дополненной реальности" http://fedconsultant.ca.sbrf.ru/cons/cgi/online.cgi?req=doc&ts=1674378721071574585186546 89&cacheid=B801650EEADC41E300C85D4A3941F86F&mode=splus&base=LAW&n=335562&rnd=803DCEC3CCFDF9F8EC39BC40029091A2#0857803400726876 9

10. Уинстон Черчиль: цитаты, остроты и афоризмы / Сост. И авт. введ. Доминик Энрайт. – Пер. с англ. – Днепропетровск: Либри, 2009, стр. 180
11. Послание Президента РФ В.В. Путина Федеральному Собранию РФ от 15 января 2020 г. // http://fedconsultant.ca.sbrf.ru/cons/cgi/online.cgi?req=doc&ts=1674378721071574585186546 89&cacheid=B9A34DEC19F8D8682B9B84FDE7FBA9BF&mode=splus&base=LAW&n=342959&rnd=803DCEC3CCFDF9F8EC39BC40029091A2#04181846275432392
12. Регламент N 2016/679 Европейского парламента и Совета Европейского Союза "О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных)" [рус., англ.] (Принят в г. Брюсселе 27.04.2016) [Электронный ресурс] // КонсультантПлюс.http://fedconsultant.ca.sbrf.ru/cons/cgi/online.cgi?req=doc&ts=166354371018189224641854 45&cacheid=D4E1A09BE14F34B6A77D06EF9DAD077C&mode=splus&base=INT&n=60453&rnd=22F4392EE0886F68906835F0A0464B56#041895920666116593
13. Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" [Электронный ресурс] // КонсультантПлюс. http://fedconsultant.ca.sbrf.ru/cons/cgi/online.cgi?req=doc&ts=2053612911060573304181083 05&cacheid=870F102ECD137CE865809A8A29AD3259&mode=splus&base=LAW&n=137356&rnd=A8DF3B343B4B86B201F71148E5BBEA57#04496005090971752