4.2. СБОР БИОМЕТРИЧЕСКИХ ДАННЫХ: ИНСТРУМЕНТ ТОТАЛЬНОЙ СЛЕЖКИ ИЛИ СРЕДСТВО ДЛЯ ДОСТИЖЕНИЯ ЗАКОННОЙ ЦЕЛИ?

Луценко С. И.
Эксперт НИИ Корпоративного и проектного управления (г. Москва).
Аналитик Института экономических стратегий Отделения общественных наук
Российской академии наук,

Автор рассматривает особенности сбора данных о гражданах России со стороны государственных органов, Банка России. Насколько правомерными являются их действия в отношении реализации проекта Единой биометрической системы? Внедрение Единой биометрический системы подразумевает соразмерность в отношении достижения законной цели. В противном случае существует правовой риск стигматизации добросовестной категории граждан.

В пояснительной записке к проекту Федерального закона «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» [10] отмечается необходимость создания Единой биометрической системы (далее – ЕБС).

Обоснованием внедрения ЕБС является сложившаяся в Российской Федерации ситуация, связанная с распространением новой коронавирусной инфекции (2019-nCoV).

Существует потребность в создании равных возможностей для граждан Российской Федерации в отношении доступности услуг и сервисов в части обеспечения полностью удаленного взаимодействия сторон различных отношений.

В целях максимального расширения количества субъектов, которые смогут получать услуги дистанционно, полагаем необходимым ускорить сбор биометрических персональных данных и их размещение в ЕБС. Данную задачу можно решить, в том числе путем самостоятельной регистрации физическими лицами своих биометрических персональных данных в указанной системе.

Законопроектом № 946734-7 устанавливается право физических лиц в порядке, установленном федеральным органом исполнительной власти, осуществляющим регулирование в сфере идентификации физических лиц на основе биометрических персональных данных, с применением мобильного телефона, смартфона, планшетного или персонального компьютера, осуществлять размещение в единой биометрической системе своих биометрических персональных данных. Такое размещение осуществляется физическим лицом с использованием программного обеспечения для технического устройства (мобильного телефона, смартфона, планшетного или персонального компьютера), предназначенного для обработки биометрических персональных данных, предоставляемого оператором единой биометрической системы.

Кроме того, отмечается, что использование единой биометрической системы с применением указанных выше биометрических персональных данных государственными органами, банками и иными организациями будет допускаться в случаях, определенных Правительством Российской Федерации по согласованию с Центральным банком Российской Федерации, а также на основании договора с оператором Единой биометрической системы. Положениями законопроекта также устанавливается право государственных органов, банков и иных организаций, осуществляющих сбор и обработку в своих информационных системах биометрических персональных данных, по согласию физического лица размещать указанные биометрические персональные данные в единой биометрической системе в порядке, установленном пунктом 1 части 13 статьи 14.1 Федерального закона «Об информации, информационных технологиях и о защите информации» [12].

В другом проекте федерального закона «О едином федеральном информационном ресурсе, содержащем сведения о населении Российской Федерации» [9], предлагается создать систему учета сведений о населении, обеспечивающую их достоверность и непротиворечивость (21.05.2020 данный законопроект был направлен в Совет Федерации и 08.06.2020 был подписан Президентом РФ (Федеральный закон от 08.06.2020 № 168-ФЗ)).

Сведения об одном физическом лице, включаемые в федеральный ресурс о населении, образуют одну запись федерального ресурса о населении, которая подписывается усиленной квалифицированной электронной подписью уполномоченного органа.

Оператор федеральной информационной системы обеспечивает защиту сведений, содержащихся в федеральной информационной системе, в соответствии с требованиями законодательства Российской Федерации об информации, информационных технологиях и о защите информации и законодательства Российской Федерации в области персональных данных.

Создание федерального ресурса о населении позволит: повысить оперативность и качество принимаемых решений в сфере государственного и муниципального управления; обеспечить достоверность и актуальность информации о населении; сократить сроки оказания государственных и муниципальных

услуг и исполнения государственных и муниципальных функций; обеспечить переход на качественно новый уровень расчета и начисления налогов на доходы физических лиц; повысить эффективность реализации государственной политики, решения вопросов социально-экономического развития, составления и реализации государственных и муниципальных программ, бюджетов бюджетной системы Российской Федерации; обеспечить повышение эффективности борьбы с правонарушениями, сокращение числа мошеннических действий при получении мер социальной поддержки и уплаты налогов, сборов и других обязательных платежей, повышение собираемости платежей в бюджеты бюджетной системы Российской Федерации [9].

Очевидно, возникает вопрос о необходимости и соразмерности сбора биометрических данных о гражданах. Не превратится ли подобная инициатива законодателя в тотальный контроль над населением или, проще говоря, в инструмент тотальной слежки, который приведет к нарушению принципа пропорциональности и права человека на неприкосновенность личной жизни?

В этой связи интересным представляется правовая позиция Конституционного Суда Республики Беларусь, который в своем решении учитывает права граждан через религиозную составляющую.

В частности, отмечается, что необходимо приложить все усилия, чтобы развитие законодательства и административной практики в сфере идентификации граждан не ущемляло их вероисповедной и мировоззренческой свободы.

Конституционный Суд Республики Беларусь [11] ссылается на обращение Священного Синода Русской Православной Церкви от 6 октября 2005 г. к органам власти стран Содружества Независимых Государств и Балтии, в котором, в свою очередь, отмечается, что нет ничего греховного в использовании для учета граждан, для обеспечения безопасности человека и общества – последних технических достижений, в том числе электронных средств, лишь развивающих уже привычные методы. Так, описания и изображения человеческого лица и тела использовались в целях безопасности еще в древние века. Совершенствование способов их записи не несет в себе ничего принципиально нового. Однако, как считает Синод, наряду с техническими преимуществами, создание и объединение массивов личной информации, а также развитие электронных средств опознания личности таит в себе немало опасностей. Возрастает зависимость человека от неизбежных технических сбоев, ошибок, халатности персонала или вмешательства злоумышленников. Не исключена возможность централизованного сбора сведений о частной жизни граждан и об их убеждениях. Это создает угрозу правам и свободе личности, делает возможным тотальный контроль за жизнью человека, в том числе за его мировоззрением. Такое развитие событий усиливает опасность предвзятого отношения к человеку на основании его религиозных, политических или иных взглядов. Главное – не допустить, чтобы люди, по многим причинам отказывающиеся от участия в новой идентификационной системе, были отнесены на обочину жизни, существенно поражены в правах, подвергнуты дискриминации при приеме на работу, распределении социальной помощи и т.д. Для таких граждан должна быть предусмотрена альтернатива, позволяющая полноценно жить в обществе, не препятствующая осуществлению их прав и свобод, пользованию законными льготами независимо от тех или иных форм идентификации личности [11].

Как отмечается в «Докладе Верховного комиссара Организации Объединенных Наций по правам человека. Право на неприкосновенность частной жизни в цифровой век» [1], государства и предприятия все чаще внедряют системы, предусматривающие сбор и использование биометрических данных, таких как ДНК, лицевая геометрия, голос, узор сетчатки и радужной оболочки глаза и отпечатки пальцев. Некоторые страны создали огромные централизованные базы данных для хранения такой информации в разных целях – от целей национальной безопасности и уголовных расследований до поиска лиц при необходимости получения основных услуг, таких как социальные и финансовые услуги и образование.

Создание массовых баз биометрических данных вызывает серьезную озабоченность в области прав человека. Такие данные носят особенно конфиденциальный характер, поскольку они по определению неразрывно связаны с конкретным лицом и его жизнью и могут подвергаться серьезным злоупотреблениям. Например, крайне трудно компенсировать последствия кражи персональных биометрических данных, которая может серьезно затронуть права физического лица. Кроме того, биометрические данные могут быть использованы не для тех целей, для которых они собирались, включая незаконное отслеживание и мониторинг отдельных лиц. С учетом этих рисков при сборе биометрических данных необходимо уделять особое внимание вопросам необходимости и соразмерности.

В этой связи вызывает тревогу тот факт, что некоторые государства приступили к осуществлению масштабных проектов с использованием биометрических данных (персональные данные), не внедрив адекватных правовых и процессуальных гарантий.

В Докладе обращается внимание на обеспечении государствами систем

Далее в Докладе обращено внимание государств на необходимости соразмерности (при достижении законной цели) при внедрении систем, предусматривающие сбор и хранение биометрических (персональных) данных.

Конвенция о защите физических лиц при автоматизированной обработке персональных данных [3] (далее – Конвенция № 108) устанавливает стандарты защиты данных в сфере автоматизированной обработки персональных данных в публичном и частном секторах. Она предусматривает (статья 8), в качестве дополнительных гарантий для субъекта данных, что любому лицу должна быть предоставлена

возможность: знать о существовании автоматизированного файла персональных данных, знать его основные цели, а также название и место обычного проживания или местонахождение контролера файла; получить через разумный промежуток времени и без чрезмерной задержки или чрезмерных расходов подтверждение того, хранятся ли касающиеся его персональные данные в автоматизированном файле данных, а также получить такие данные в доступной для понимания форме; добиваться в случае необходимости исправления или уничтожения таких данных, если они подвергались обработке в нарушение норм внутреннего законодательства, воплощающего основополагающие принципы, изложенные в статьях 5 и 6 настоящей Конвенции; прибегать к средствам правовой защиты в случае невыполнения просьбы о подтверждении или в случае необходимости предоставлении данных, их изменения или уничтожения, как это предусмотрено в пунктах «b» и «c» статьи 8.

Статья 9 Конвенции № 108 («Изъятия и ограничения») допускает изъятия из положений статей 5, 6 и 8 Конвенции только в пределах, определенных в настоящей статье: защиты безопасности государства, общественной безопасности, валютно-кредитных интересов государства или пресечения уголовных преступлений; защиты субъекта данных или прав и свобод других лиц.

Конвенция № 108 была ратифицирована Российской Федерацией 15 мая 2013 г. и вступила в силу в отношении Российской Федерации 1 сентября 2013 г. В документе о ратификации Конвенции, депонированном Российской Федерацией 15 мая 2013 г., содержится следующая оговорка:

Российская Федерация заявляет, что в соответствии с пп. «a» пункта 2 статьи 3 Конвенции – не будет применять Конвенцию к персональным данным: отнесенным к государственной тайне в порядке, установленном законодательством Российской Федерации о государственной тайне.

Российская Федерация заявляет, что в соответствии с пп. «c» пункта 2 статьи 3 Конвенции будет применять ее к персональным данным, которые не подвергаются автоматизированной обработке, если применение Конвенции соответствует характеру действий, совершаемых с персональными данными без использования средств автоматизации.

Российская Федерация заявляет, что в соответствии с пп. «a» пункта 2 статьи 9 Конвенции оставляет за собой право устанавливать ограничения права субъекта персональных данных на доступ к персональным данным о себе в целях защиты безопасности государства и общественного порядка.

Рекомендация Комитета министров о защите данных в области телекоммуникационных услуг [7], в соответствующих частях предусматривает следующее: «Вмешательство публичных органов в содержание коммуникации, включая использование средств прослушивания или записи или иных средств надзора или перехвата коммуникаций, должно осуществляться, только если оно предусмотрено законом и составляет необходимую меру в демократическом обществе в интересах: a) защиты государственной безопасности, общественного порядка, денежных интересов государства или подавления преступлений; b) защиты субъекта данных или прав и свобод других лиц.

В случае вмешательства публичных органов в содержание коммуникации национальное законодательство должно регулировать: a) осуществление права субъекта данных на доступ и исправление; b) при каких обстоятельствах компетентные публичные органы имеют право отказывать в предоставлении информации заинтересованному лицу или откладывать ее предоставление; c) хранение или уничтожение таких данных.

Федеральный закон «О персональных данных» [12], принятый в целях обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, устанавливает принципы и условия обработки персональных данных (глава 2). В силу статьи 5 данного Федерального закона такая обработка должна ограничиваться достижением конкретных, заранее определенных и законных целей; не допускается обработка персональных данных, несовместимая с целями сбора персональных данных; обработке подлежат только персональные данные, которые отвечают целям их обработки; содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки; обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки (части 2, 4 и 5).

Из системного толкования норм Федерального закона «О персональных данных» следует, что сбор, обработка, передача, распространение персональных данных возможны только с согласия субъекта персональных данных, при этом согласие должно быть конкретным. Под персональными данными понимается любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу [4].

Кроме того, под базой персональных данных должен пониматься любой упорядоченный массив данных личного характера. Не имеет значения, по какому точно критерию и в какой точно форме массив собранных данных действительно упорядочен: достаточно того, что этот массив позволяет легко найти данные, относящиеся к определенному лицу, к которому приходили домой.

Другими словами, биометрические данные охватывают весь массив данных личного характера, включая фамилии и адреса, а также иную информацию, относящуюся к семейному положению, религиозным убеждениям.

Исходя из соответствующих положений статьи 24 Конституции РФ, сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются.

Возникает вопрос, насколько действия государственных органов, кредитных учреждений будут разумными и пропорциональными в отношении сведений о гражданине (клиенте).

В первую очередь, речь идет о проработке вопроса, который касается технических требований к оборудованию, которое должно быть установлено операторами связи.

Существует риск того, что система сбора данных (например, с целью защиты национальной безопасности) может умалять или даже уничтожить демократические ценности под предлогом их защиты. Со стороны РФ необходимо создание адекватных и эффективных гарантий против превышения полномочий со стороны кредитных учреждений.

На сегодняшний день положения законодательства Российской Федерации «О персональных данных» не содержат адекватных и эффективных гарантий против произвола и риска превышения полномочий, которые присущи любой системе сбора данных.

Приведем небольшой пример в отношении обработки персональных данных с привязкой к получению кредита.

Банки при предоставлении кредита используют заявление-анкету со стандартным условием: «Я даю свое согласие на обработку, включая любые действия (или совокупность действий), предусмотренные Федеральным законом «О персональных данных», совершаемые с использованием средств автоматизации или без использования таких средств (сбор, запись, систематизацию, накопление, хранение, уточнение, обновление, изменение, извлечение, использование, передачу (предоставление, доступ!), в том числе трансграничную, обезличивание, блокирование, удаление, уничтожение), Банком моих персональных данных в объеме сведений, указанных в настоящем Заявлении, содержащихся в представленных мной в Банк документах, и биометрических персональных данных – моего фотоизображения, в целях проверки Банком представленной мной информации и принятия решения относительно возможности предоставления мне кредита, заключения и исполнения договоров, стороной, выгодоприобретателем или поручителем по которым я буду являться, в целях защиты прав и законных интересов Банка и в иных целях, указанных в заключенных мной с Банком договорах, а также даю согласие на поручение Банком обработки моих персональных данных иным лицам в вышеуказанных целях (в том числе, контрагентам Банка для сбора сведений и документов, необходимых для заключения с мной договоров, предоставления мне информации посредством телефонной связи, направления писем и СМС-сообщений, коллекторским агентствам и иным лицам для информирования меня о просроченной задолженности и ее взыскания).».

Из содержания данного пункта заявления следует, что банк получил согласие потребителя на передачу персональных данных неограниченному кругу лиц, поскольку ни точного наименования, ни адреса, ни иных конкретных данных организаций компаний и физических лиц, которым могут быть переданы персональные данные, в анкете и договоре не содержится.

Из текста заявления на получение кредита и содержания договоров невозможно установить наименование или фамилию, имя, отчество и адрес компаний, осуществляющих рассылку, организаций связи, компаний общества, перечень персональных данных, на обработку которых дается согласие субъекта персональных данных.

Таким образом, непоименованные лица, фактически становясь операторами либо лицами, получившими доступ к персональным данным потребителя, не становятся обязанными сохранять конфиденциальность таких данных.

Подписав данный кредитный договор и заявление на получение кредита потребители фактически согласились с возможностью обработки их персональных данных третьими лицами, при этом банком не были учтены установленные законом специальные требования к письменному согласию субъекта персональных данных.

Тем самым, условия кредитного договора и заявление на получение кредита не охвачены самостоятельной волей и интересом граждан (потребителей), поскольку согласие потребителей, в данном случае, определено в одностороннем порядке в виде текста (типографским способом) в заявлении на получение кредита [8].

Возникает возможность, при которой российское законодательство разрешает автоматическое хранение базы данных и недостаточно четко определяет обстоятельства, при которых информация о гражданах будет храниться и уничтожаться. Эффективность средства правовой защиты умаляется отсутствием уведомления когда-либо о передачи данных или адекватного доступа к документам, касающимся передачи данных [7].

Другими словами, недопустима ситуация, при которой государство пользуется неограниченной свободой действий, подвергая людей, находящихся под его юрисдикцией, тотальному сбору информации. Тем самым, существует опасность, что такой закон может подорвать и даже уничтожить демократию под предлогом ее защиты.

То есть, система сбора данных, потенциально может охватывать всех жителей РФ (отслеживание сообщений, передаваемых по электронным средствам связи и при помощи компьютера, а также осуществление записи любых данных, полученных в результате применения методов сбора данных, могут быть рассмотрены в свете понятий «личная жизнь»), о чем граждане не будут поставлены в известность, если не будет иметь место какая-либо утечка информации. В этой степени процедура сбора биометри-

ческих данных россиян прямо затрагивает всех пользователей. Подобную ситуацию можно рассматривать как непосредственное вмешательство государства в осуществление прав, гарантированных статьей 8 «Право на уважение частной и семейной жизни» «Конвенции о защите прав человека и основных свобод» [2; 5].

Защита персональных данных имеет основополагающее значение для осуществления лицом права на уважение его личной и семейной жизни, гарантированного статьей 8 Конвенции. Соответственно, внутригосударственное законодательство должно предусматривать достаточные гарантии защиты персональных данных от использования персональных данных с нарушением гарантий, предоставляемых статьей 8 Конвенции.

Необходимость в таких гарантиях выше тогда, когда речь идет о защите информации личного характера, которая подвергается автоматизированной обработке и не в последнюю очередь тогда, когда ее используют для своих целей государственные (надзорные) органы (например, Банк России является надзорным органом с возложенными на него государственными функциями).

Внутригосударственное законодательство должно, в частности, обеспечивать, чтобы эти данные являлись достаточными и не чрезмерными для целей их хранения и хранились в форме, позволяющей установить субъектов данных, не дольше, чем это требуется для достижения целей хранения этих данных. Кроме того, внутригосударственное законодательство должно предусматривать достаточные гарантии эффективной защиты хранящихся персональных данных от ненадлежащего использования и злоупотреблений.

Особую озабоченность может вызывать процесс стигматизации населения. Когда граждане, которые являются добросовестными (законопослушными), будут находиться в положении, и с ними будут обращаться, как с гражданами, которые являются недобросовестными (незаконопослушными), которые преступили закон [6].

Тем не менее, особенно в случаях, когда власть, возложенная на орган исполнительной власти, осуществляется тайно, риски произвола очевидны. Поэтому крайне важно иметь четкие, подробные правила для прослушивания телефонных разговоров, особенно когда доступная для использования технология постоянно становится все более изощренной.

Вместе с тем в вопросах, затрагивающих основные права, противоречило бы принципу верховенства права, одному из основных принципов демократического общества, воплощенных в Конвенции, если бы полномочия надзорных органов были выражены в форме неограниченных юридических полномочий. Соответственно, закон должен с достаточной ясностью указывать пределы любого подобного усмотрения, предоставленного компетентным органам, и способ его реализации с учетом законной цели.

По аналогии с методологией Европейского Суда, необходимо выделить целевую группу граждан, чтобы нивелировать риски, связанные с потенциальным получением информации о любом гражданине. Может возникнуть ситуация, когда понятие «лиц, идентифицированных... в качестве определенного круга лиц» в действительности может быть применено к любому лицу и истолковано как подготавливающее основу для получения информации в отношении неограниченного количества граждан.

При поиске данных контента должны применяться повышенные требования к обоснованию поиска и процессуальные гарантии.

Иначе может быть реализован алгоритм, связанный с неизбирательным широкомасштабным и систематическим сбором персональных данных лиц, зачастую включающих информацию интимного характера.

В Постановлении по объединенным делам «Digital Rights Ireland и Seitlinger and Others» [13] Суд Европейского союза признал недействительной Директиву о хранении данных, устанавливающую обязанность поставщиков общедоступных услуг электронной связи или сетей связи общего пользования хранить весь трафик и данные о местоположении на период от шести месяцев до двух лет для обеспечения доступности данных для целей расследования, обнаружения и уголовного преследования за совершение тяжких преступлений, определенных каждым государством-членом в его внутригосударственном законодательстве. По отдельности и в совокупности эти возможности слежения могут позволить государствам сделать очень точные выводы, касающиеся самых интимных моментов частной жизни любого лица. Существует потенциальная угроза неприкосновенности частной жизни вследствие обязательного неизбирательного и не основанного на подозрениях хранения данных, порождающего у затронутых им лиц ощущение, что их жизнь находится под постоянным контролем.

Литература

1. Доклад Верховного комиссара Организации Объединенных Наций по правам человека. Право на неприкосновенность частной жизни в цифровой век» (принят 10.09.2018 - 28.09.2018 на 39-й сессии Совета по правам человека ООН) // Бюллетень Европейского Суда по правам человека. Российское издание. 2019. № 10.
2. Конвенция о защите прав человека и основных свобод (Заключена в г. Риме 04.11.1950) // Собрание законодательства РФ. 2001. № 2.

3. Конвенция о защите физических лиц при автоматизированной обработке персональных данных (ETS № 108) (Заключена в г. Страсбурге 28.01.1981) // Собрание законодательства РФ. 2014. № 5.
4. Определение Верховного Суда РФ от 01.08.2017 № 78-КГ17-45 Доступ из СПС «Консультант Плюс».
5. Постановление Европейского Суда по правам человека от 06.09.1978 по делу «Класс и другие против Федеративной Республики Германии» Доступ из СПС «Консультант Плюс».
6. Постановление Европейского Суда по правам человека от 18.04.2013 по делу «M.K. против Франции» // Доступ из СПС «Консультант Плюс».
7. Постановление Европейского Суда по правам человека от 04.12.2015 по делу «Роман Захаров против Российской Федерации» // Доступ из СПС «Консультант Плюс».
8. Постановление Семнадцатого арбитражного апелляционного суда от 14.01.2020 по делу № А60-38578/2019 // Доступ из СПС «Консультант Плюс».
9. Пояснительная записка к проекту Федерального закона № 759897-7 «О едином федеральном информационном ресурсе, содержащем сведения о населении Российской Федерации» Доступ из СПС «Консультант Плюс».
10. Пояснительная записка к Проекту Федерального закона № 946734-7 «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» (ред., внесенная в ГД ФС РФ, текст по состоянию на 22.04.2020) // Доступ из СПС «Консультант Плюс».
11. Решение Конституционного Суда Республики Беларусь от 06.12.2005 № П-165/2005 «Об электронной идентификации граждан» // Доступ из СПС «Консультант Плюс».
12. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Российская газета. 2006. № 165.
13. Digital Rights Ireland and Seitlinger and Others (жалобы N C-293/12 и C-594/12) // URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0293&rid=1 (дата обращения: 08.06.2020).

References in Cyrillics

1. Doklad Verxovnogo komissara Organizacii Ob``edinenny`x Nacij po pravam cheloveka. Pravo na neprikosnovennost` chastnoj zhizni v cifrovoj vek» (prinyat 10.09.2018 - 28.09.2018 na 39-j sessii Soveta po pravam cheloveka OON) // Byulleten` Evropejskogo Su-da po pravam cheloveka. Rossijskoe izdanie. 2019. № 10.
2. Konvenciya o zashhite prav cheloveka i osnovny`x svobod (Zaklyuchena v g. Rime 04.11.1950) // Sobranie zakonodatel`stva RF. 2001. № 2.
3. Konvenciya o zashhite fizicheskix licz pri avtomatizirovannoj obrabotke personal`ny`x danny`x (ETS № 108) (Zaklyuchena v g. Strasburge 28.01.1981) // Sobranie zakonodatel`stva RF. 2014. № 5.
4. Opredelenie Verxovnogo Suda RF ot 01.08.2017 № 78-KG17-45 Dostup iz SPS «Konsul`-tant Plyus».
5. Postanovlenie Evropejskogo Suda po pravam cheloveka ot 06.09.1978 po delu «Klass i dru-gie protiv Federativnoj Respubliki Germanii» Dostup iz SPS «Konsul`tant Plyus».
6. Postanovlenie Evropejskogo Suda po pravam cheloveka ot 18.04.2013 po delu «M.K. protiv Francii» // Dostup iz SPS «Konsul`tant Plyus».
7. Postanovlenie Evropejskogo Suda po pravam cheloveka ot 04.12.2015 po delu «Roman Za-xarov protiv Rossijskoj Federacii» // Dostup iz SPS «Konsul`tant Plyus».
8. Postanovlenie Semnadczatogo arbitrazhnogo apellyacionnogo suda ot 14.01.2020 po delu № A60-38578/2019 // Dostup iz SPS «Konsul`tant Plyus».
9. Poyasnitel`naya zapiska k proektu Federal`nogo zakona № 759897-7 «O edinom federal`-nom informacionnom resurse, soderzhashhem svedeniya o naselenii Rossijskoj Federa-cii» Dostup iz SPS «Konsul`tant Plyus».
10. Poyasnitel`naya zapiska k Proektu Federal`nogo zakona № 946734-7 «O vnesenii izmene-nij v Federal`ny`j zakon «Ob informacii, informacionny`x texnologiyax i o zashhite in-formacii» (red., vnesennaya v GD FS RF, tekst po sostoyaniyu na 22.04.2020) // Dostup iz SPS «Konsul`tant Plyus».
11. Reshenie Konstitucionnogo Suda Respubliki Belarus` ot 06.12.2005 № P-165/2005 «Ob e`lektronnoj identifikacii grazhdan» // Dostup iz SPS «Konsul`tant Plyus».
12. Federal`ny`j zakon ot 27.07.2006 № 149-FZ «Ob informacii, informacionny`x texnolo-giyax i o zashhite informacii» // Rossijskaya gazeta. 2006. № 165.
13. Digital Rights Ireland and Seitlinger and Others (zhaloby` N C-293/12 i C-594/12) // URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0293&rid=1 (data obrashheniya: 08.06.2020).

Луценко Сергей Иванович (scorp_ante@rambler.ru)
Соавтор документа «Стратегия развития электросетевого комплекса Российской Федерации».

Автор проекта «Контуры Концепции развития финансового кластера Российской Федерации на долгосрочную перспективу»

Ключевые слова
Единая биометрическая система, персональные данные, сбор и обработках данных, право на уважение частной и семейной жизни, национальная безопасность

***Sergej Lutsenko,* Biometric data collection: a tool for total surveillance or a means to achieve a legitimate goal?**

Keywords
Unified biometric system, personal data, data collection and processing, right to respect for private and family life, national security

DOI: 10.34706/DE-2020-02-09

JEL classification: D83Search • Learning • Information and Knowledge • Communication • Belief • Unawareness

Abstract
The author considers the mechanism of implementation of a unified digital platform as a system of means and labor, as well as the implementation of a unified state policy in the economy.