# ВЫСТУПЛЕНИЕ

**ЕВГЕНИЯ ЖОВТИСА, председателя Совета, эксперта-консультанта Казахстанского международного бюро по правам человека и соблюдению законности**

**на презентации проекта Закона РК «О дактилоскопической и геномной регистрации»**

**«О некоторых аспектах концепции законопроекта о дактилоскопической и геномной регистрации»**

**(г.Астана, 18 ноября 2013 г.)**

Уважаемые участники,

Дактилоскопическая и геномная регистрация, по существу является сбором персональных данных граждан, иностранцев, беженцев и лиц без гражданства.

К технологиям, связанным с со сбором и обработкой персональных данных, то есть, технологиям, используемым в системах идентификации личности относятся, прежде всего, **персональные карточки**, то есть досье, назначение которых и объем информации различны в разных странах. Эти персональные карточки или досье связаны, главным образом, с системами национальной (государственной) регистрации и являются необходимым источником информации для государственного управления. Тем не менее, составление таких досье должно быть совместимо с защитой неприкосновенности частной жизни.

Вторая технология – **биометрия**, то есть процесс сбора, обработки и хранения данных о физических характеристиках человека с целью его идентификации, которая также должна предполагать защиту от возможного неправомерного или произвольного использования.

Правовое регулирование и того, и другого относится к сфере законодательства о персональных данных.

Очевидно, что правовое регулирование отношений, связанных со сбором и использованием персональных данных, необходимо и, соответственно, принятие специального закона или законов (поскольку принят, но не вступил в силу Закон о персональных данных), регламентирующих порядок сбора и использования таких данных, и в особенности ограничения в этой сфере, можно только приветствовать.

Принятие такого специального законодательства соответствует международным стандартам и зарубежной практике.

Разработчики правомерно ссылаются на зарубежный опыт в этой области.

В то же время ключевым вопросом является концепция правового регулирования сбора и использования персональных данных и, главным образом, их защита от неправомерного использования.

По отношению к данной концепции я повторю свои замечания, подготовленные в конце 2011 г. к проекту Закона о персональных данных, поскольку оба проекта регулируют однородные отношения

В правовом регулировании отношений в связи со сбором, использованием и защитой персональных данных, используются **три базовых принципа в отношении обеспечения прав человека на защиту персональных данных**:

1. **Обеспечение доступа к персональным данным о самом себе;**
2. **Обеспечение возможности исправлять неверные (устаревшие) данные о самом себе;**
3. **Обеспечение эффективных средств правовой защиты, если персональные данные использованы не по назначению.**

Последнее как раз относится к рассматриваемой Концепции.

З**аконодательство о персональных данных, помимо регламентации порядка сбора и использования персональных данных с правовой и технической точек зрения, должно, прежде всего, содержать правовые нормы защиты персональных данных, обеспечить гарантии их правомерного использования и концептуально основываться на вышеприведенных принципах**.

Именно по такому пути развиваются международное и зарубежное конституционное право, фокусируясь, прежде всего, на решении задачи защиты персональных данных, как обеспечения права на неприкосновенность частной жизни и предупреждения возможного произвола и злоупотреблений.

Поэтому при правомерности ссылок на зарубежный опыт сбора различных персональных данных, необходимо особенно внимательно посмотреть на защитительные меры, принятые в тех государствах, на которые ссылаются авторы Концепции.

Гарантии защиты персональных данных на международном уровне закреплены как в универсальных договорах по правам человека: во Всеобщей декларации прав человека 1948 г. (статья 12), Международном пакте о гражданских и политических правах 1966 г. (статья 17), Европейской конвенции о защите прав и основных свобод человека, так и в специализированных международных инструментах, более подробно регулирующих эту сферу общественных отношений.

К ним относятся по хронологии резолюции Комитета Министров Совета Европы, Рекомендации Организации экономического сотрудничества и развития о защите личных данных при их трансграничной передаче, Конвенция Совета Европы о защите личности в связи с автоматической обработкой персональных данных, 1981 г. с целым рядом рекомендаций к ней; Директива Европейского парламента и Совета Европы №95/46/ЕС «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных», 1995 г.; Рамочное решение Совета Европейского Союза №2008/977/JHA о защите персональных данных, обрабатываемых в рамках сотрудничества органов полиции и правосудия по уголовным вопросам, 2008 г. и много др.

Как следует из анализа перечисленных выше правовых документов, защита персональных данных наиболее развита в странах Северной Америки и особенно Европейского Союза, где наряду с общеевропейскими правовыми инструментами практически во всех странах приняты отдельные законы, касающиеся защиты неприкосновенности частной жизни, в том числе персональных данных. Это, прежде всего, касается защиты частной жизни от незаконного или произвольного вмешательства государства и незаконного или произвольного использования персональных данных.

То есть, главная цель правового регулирования – защита неприкосновенности частной жизни, защита, прежде всего, законопослушного гражданина от неправомерного, незаконного или произвольного использования его персональных данных, главным образом, со стороны государственных органов.

Именно поэтому в международном праве и зарубежной правоприменительной практике существует **ряд требований к процедуре сбора и использования персональных данных:**

**- они должны быть получены добросовестным и законным путем;**

**- они должны собираться и использоваться для точно определенных и не противоречащих закону целей и не использоваться для целей, несовместимых с теми, для которых были собраны;**

**- они должны относиться к делу, быть полными, но не избыточными с точки зрения тех целей, для которых они накапливаются;**

**- они должны храниться в такой форме, которая позволяет идентифицировать субъектов данных не больше, чем этого требует цель, для которой они собраны**.

Наконец, законодательство должно содержать **прямые гарантии защиты персональных данных, которые заключаются**:

- **в предоставлении любому лицу права быть осведомленным о существовании базы персональных данных и ее главных целях, ее юридическом адресе;**

**- в том, что периодически и без лишних затрат времени или средств каждый должен иметь возможность обратиться с запросом о том, накапливаются ли в базе данных его персональные данные, и получить информацию о таких данных в доступной форме;**

**- в том, что лицо вправе требовать изменения или уничтожения данных, которые не соответствуют требованиям, перечисленным выше (точности, отнесенности к определенной цели и др.);**

**- в том, что каждый вправе прибегнуть к судебной защите нарушенного права, если его запрос либо требование о доступе к его персональным данным, их уточнении или уничтожении не были удовлетворены**.

Изъятие из этих положений допускается только в том случае, если оно прямо предусмотрено законом и представляет собой необходимую в демократическом обществе меру, установленную для охраны государственной и общественной безопасности, экономических интересов государства или для пресечения преступлений.

Но и в этом случае цели должны быть ясными, критерии – определёнными, а средства правовой защиты от злоупотреблений - эффективными.

Из всего вышеизложенного, следует, что **законодательство о персональных данных неразрывно связано с законодательством о доступе к информации и законодательством о защите частной жизни.**

Именно по этому пути пошли в ряде государств. Например, в 70-80 годах прошлого века в США, Австралии, Канаде и Норвегии появились специальные законы о защите частной жизни (*Privacy Acts)*. Основным объектом защиты являлись как раз персональные данные - информационная составляющая частной жизни.

В Германии нарушение закона об охране информации о гражданах, совершенное в корыстных целях, влечёт за собой лишение свободы на срок до двух лет, во Франции – до пяти лет. В США гражданин вправе предъявить иск в случае совершения умышленных действий, причинивших вред его частной жизни. Аналогично решается вопрос и в Швеции.

Комитет ООН по правам человека в комментарии (заключительном замечании) общего порядка №16 к статье 17 Международного пакта о гражданских и политических правах, касающейся неприкосновенности частной жизни, дал весьма важные разъяснения в отношении применяемых в этой статье определений.

Так Комитет указал, что в статье 17 Пакта речь идёт о защите как от **незаконного**, так и от **произвольного вмешательства,** и что именно в законодательстве государства должна быть, прежде всего, предусмотрена защита права, закреплённого в этой статье.

При этом термин «незаконное» означает, «*что вмешательство вообще не может иметь места за исключением случаев, предусмотренных законом. Вмешательство, разрешаемое государствами, может совершаться только на основании закона, который должен в свою очередь соответствовать положениям, целям и задачам Пакта*».

А выражение «*произвольное вмешательство*» также связано с защитой права, предусмотренного в статье 17, и «*может также распространяться на допускаемое законом вмешательство.* ***Введение понятия произвольности призвано обеспечить, чтобы даже вмешательство, допускаемое законом, соответствовало положениям, целям и задачам Пакта и в любом случае являлось обоснованным в конкретных обстоятельствах***».

Комитет указал, что «*даже в отношении вмешательства, которое соответствует Пакту,* ***в соответствующем законодательстве должны подробно определяться конкретные обстоятельства, в которых такое вмешательство может допускаться****.* ***Решение о санкционировании такого вмешательства должно приниматься только конкретным органом, предусмотренным законом, и строго индивидуально***».

Необходимо также отметить, что защита права на неприкосновенность частной жизни, в том числе и персональных данных, не ограничивается принятием соответствующего законодательства.

Система защиты и предусматривает и её институциональное воплощение.

Так в ряде стран Европы, Австралии, Новой Зеландии, Канаде предусматривается создание института специального государственного должностного лица, который отвечает за все законодательство о защите данных. Это лицо называется комиссаром, или уполномоченным, или омбудсманом, контролирует исполнение закона и проводит соответствующие расследования. В некоторых случаях этот чиновник выступает против нарушителя. Комиссар также отвечает за просветительскую работу в обществе и международные связи в области защиты данных. Описанная модель была принята во многих странах, хотя полномочия комиссара в разных странах сильно различаются, и некоторые комиссары испытывают нехватку ресурсов и сложности при исполнении своей миссии.

В Германии, например, действуют уполномоченные по защите персональных данных (по числу федеральных земель), каждый из которых имеет штат из 20–50 сотрудников, а в Канаде создана специальная комиссия по защите частной жизни.

Исходя из вышеприведённых концептуальных подходов к правому регулированию вопросов сбора, обработки и использования персональных данных и, прежде всего, их защиты, и не ставя под сомнение необходимость принятия комментируемого закона, можно сделать ряд замечаний к предложенному законопроекту.

1. Представляется целесообразным рассматривать проект Закона о дактилоскопической и геномной регистрации данных в пакете с законодательством о доступе к информации и о защите персональных данных, которое должно быть приведено в соответствие с международными стандартами в этой области, включая вводимый в действие Закон о персональных данных.

 **2.** В проекте Закона нет эффективных средств правовой защиты от использования персональных данных человека без его ведома. Представляется необходимым закрепить в законе гарантии того, что персональные данные, собранные в рамках одной информационной системы не будут без ведома гражданина передаваться и использоваться в других информационных системах. При этом в ряде случаев представляется вполне допустимым сбор, передача и использование персональных данных без согласия лица, но с обязательным его уведомлением. Исключения из этого правила должны быть прямо закреплены в законе, основываться на легитимной цели и их перечень должен быть исчерпывающим.

3. Ещё в Законе о персональных данных из сферы регулирования закона, в соответствии сп.2 ст. 3 проекта Закона **исключены «***персональные данные, отнесённые в установленном порядке к разведывательной, контрразведывательной, антитеррористической деятельности, а также сведениям, составляющих государственные секреты; персональных данных в соответствии с требованиями финансового законодательства Республики Казахстан; персональных данных, собираемых в соответствии с законами Республики Казахстан об оперативно-розыскной деятельности, правовой статистике и специальных учётах, исполнительном производстве, национальных реестрах идентификационных номеров, а также о противодействии легализации (отмыванию) доходов, полученных незаконным путём, и финансированию терроризма; персональных данных, собираемых при осуществлении уголовно-процессуального, уголовно-исполнительного, административного законодательства Республики Казахстан, а также в целях обороны страны, безопасности государства и охраны правопорядка».* Очевидно, что будет иметь отношение также и к данным дактилоскопической и геномной регистрации, что такжеставит определённые вопросы в отношении эффективности средств правовой защиты от их незаконного или произвольного использования.

В Рамочном решении Совета Европейского Союза №2008/977/JHA о защите персональных данных, обрабатываемых в рамках сотрудничества органов полиции и правосудия по уголовным вопросам, 2008 г., вполне обоснованно говорится о том, что усиление борьбы с преступностью в пределах Европейского союза и, соответственно, б***о***льшая координация деятельности правоохранительных органов и спецслужб государств – членов ЕС предъявляет одновременно повышенные требования к защите персональных данных граждан этих государств.

Участие Республики Казахстан в Конвенции о правовой помощи и правовых отношениях по гражданским, семейным и уголовным делам 1993 г., Конвенции о правовой помощи и правовых отношениях по гражданским, семейным и уголовным делам, 2002 г., в межгосударственных организациях типа ШОС, ОДКБ и т.д., очевидно, предполагает определённый обмен информацией, в том числе персональными данными. В свою очередь, это предъявляет и требование к их адекватной и эффективной защите.

В вышеупомянутом Рамочном решении указывается, что при сборе и обработке персональных данных в области предупреждения, расследования преступлений, уголовного преследования необходимо обеспечивать законность и гарантии, что персональные данные не будут использованы произвольно.

То есть, как законодательство соответствующей страны, так и соглашения о правовой помощи по уголовным делам между государствами, должны содержать гарантии и эффективные средства правовой защиты таких данных от незаконного или произвольного использования.

Более того, Рамочное решение даже устанавливает правила получения согласия соответствующего государства на передачу персональных данных, хотя и предусматривает исключительные случаи, когда интересы безопасности требуют немедленных действий.

При этом Рамочное решение устанавливает, что национальное законодательство о персональных данных должно предусматривать обязанность информировать субъекта персональных данных об их передаче другим странам или третьим сторонам, а также устанавливать возможные ограничения и исключения в этой области.

Очевидно, что исключение из сферы регулирования закона о персональных данных ряда перечисленных в п.2 ст.3 проекта Закона персональных данных не соответствует вышеприведённой международной и зарубежной практике.

Это, видимо, будет касаться и целого ряда случаев сбора и использования дактилоскопических и геномных данных.

Есть вопросы и к ряду конкретных положений Концепции законопроекта.

Актуальность принятия законопроекта обосновывается необходимостью создания единой базы учета граждан по дактилоскопической и геномной информации, однако с учётом того, что дактилоскопирование и геномная регистрация для подавляющего большинства граждан будут добровольными, говорить о полной единой базе не приходится.

Концепция не учитывает, что принцип добровольности вступает в противоречие с принципом обязательности, если в отношении того или иного лица будет прекращено уголовное преследование или вынесен оправдательный приговор, или несовершеннолетний будет снят с профилактического учета и он, его родители и другие лица захотят, чтобы их дактилоскопическая регистрация была аннулирована. Аналогично, - когда погашена или снята судимость. Уголовное законодательство однозначно устанавливает, что снятие судимости устраняет любые правовые последствия. Концепция должна учитывать необходимость восстановления прав таких лиц, причём это должно происходить автоматически, по заявлению лица, а не по специальному судебному решению.

Это же касается всех работников, определённых для обязательной дактилоскопической регистрации, если они уволятся с места работы или выйдут на пенсию.

Не очень понятно, почему граждане, выезжающие в целях трудоустройства за рубеж или, например, выезжающие на постоянное место жительства должны подвергаться дактилоскопической или геномной регистрации, если в странах, куда они направляются, таких требований нет. И касается ли этого государственных служащих или граждан, выезжающих на за рубеж на отдых.

Особенные

Тем не менее, **общий вывод заключается в том, что проект Концепции не в полной мере соответствует международным стандартам сбора и использования персональных данных, прежде всего, в части недостаточности и неэффективности гарантий защиты персональных данных от незаконного и, главным образом, произвольного использования, а также отсутствия независимого специализированного уполномоченного органа по защите персональных данных**.

И в этой части

*Евгений Жовтис,*

*ноябрь 2013 г.*