Экспертное заключение по проекту закона РК «О персональных данных»

Лоскутов И.Ю.

Генеральный директор

ТОО «Компания «ЮрИнфо»

I. Введение

Предметом настоящего исследования является проект Закона Республики Казахстан «О персональных данных» (далее - Проект), разработанный в соответствии с пунктом 30 Плана законопроектных работ Правительства РК на 2011 год, утвержденного постановлением Правительства Республики Казахстан от 30 декабря 2010 года № 1467, и внесенный 27 сентября 2011 года в Правительство Республики Казахстан.

Разработка Проекта обусловлена необходимостью законодательного закрепления порядка работы с персональными данными. Проектом предлагается создание правовой основы для 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. Так, Проектом вводятся понятия персональных данных и определяются порядок их обработки, основы организационно-правового обеспечения деятельности юридических лиц и государственных органов, организующих и осуществляющих обработку данных физических лиц.

Проектом регулируются общественные отношения, связанные с обработкой персональных данных физических лиц, осуществляемой государственными органами, юридическими и физическими лицами с использованием средств автоматизации или без них.

В ходе исследования Проекта ставились задачи проведения:

1) оценки качества, обоснованности, своевременности, правомерности проекта, соблюдения в проекте закрепленных Конституцией Республики Казахстан прав человека и гражданина;

2) определения возможной эффективности нормативного правового акта;

3) выявления возможных отрицательных последствий принятия проекта в качестве нормативного правового акта.

II. Обзор основных международных стандартов, регулирующих вопросы защиты персональных данных, а также передового опыта других стран

Необходимость защиты персональных данных базируется на одном из фундаментальных прав человека: защите от вмешательства в личную жизнь. В статье 12 Всеобщей декларации прав человека (принята и провозглашена резолюцией 217 А (III) Генеральной Ассамблеи от 10 декабря 1948 года) указывается: «Никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произвольным посягательствам на неприкосновенность его жилища, тайну его корреспонденции или на его честь и репутацию. Каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств».

Неспособность гарантировать право на защиту личных данных ставит под удар другие смежные права и свободы, включая свободу выражения, свободу мирных собраний, свободу доступа к информации, принцип недискриминации, а, в конечном счете, стабильность конституционных демократий. Поэтому в статье 17 Международного Пакта о гражданских и политических правах (далее - МПГПП) (Нью-Йорк, 19 декабря 1966 г.) эта формулировка была расширена в части незаконных вмешательств и посягательств и звучит так: «Никто не может подвергаться произвольному или незаконному вмешательству в его личную и семейную жизнь, произвольным или незаконным посягательствам на неприкосновенность его жилища или тайну его корреспонденции или незаконным посягательствам на его честь и репутацию. Каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств».

МПГПП был ратифицирован Законом Республики Казахстан от 28 ноября 2005 года № 91-III и вступил в силу для РК 24 апреля 2006 года. А, как известно, международные договоры, заключенные Республикой Казахстан в соответствии с Конституцией Республики в установленном порядке и ратифицированные Парламентом Республики Казахстан, имеют приоритет перед ее законами (пункт 3 статьи 4 Конституции Республики Казахстан). Также в пункте 11 Нормативного постановления Верховного Суда Республики Казахстан от 10 июля 2008 года № 1 «О применении норм международных договоров Республики Казахстан» (с изменениями от 21.04.2011 г.) прямо говорится о том, что в необходимых случаях суды должны руководствоваться нормами Международного пакта о гражданских и политических правах, ратифицированного Парламентом 28 ноября 2005 года, для обеспечения выполнения обязательств Республики Казахстан как участника указанного международного пакта.

В 1988 году Комитет ООН по правам человека принял Замечание общего порядка № 16 к статье 17 МПГПП. Согласно этому документу, обязательства Республики Казахстан, вытекающие из данной статьи, требуют от государства принятия законодательных и других мер для действенного запрещения произвольного или незаконного вмешательства в личную и семейную жизнь человека, а также защиты этого права.

Комитет определил термины: «незаконного вмешательства», означающего, что вмешательство вообще не может иметь место за исключением случаев, предусмотренных законом, соответствующим положениям, целям и задачам Пакта; «произвольного вмешательства», допускаемого законом, соответствующего положениям, целям и задачам Пакта и не являющегося обоснованным в конкретных обстоятельствах; «семьи», охватывающей всех тех, кто входит в состав семьи, как она понимается в обществе соответствующего государства-участника; «жилища», указывающего на то место, в котором человек проживает или занимается своими обычными делами. То, что в статье 17 МПГПП речь идёт о защите как от незаконного, так и от произвольного вмешательства, означает, что именно в законодательстве государства должна быть прежде всего предусмотрена защита права, закреплённого в этой статье.

В течение достаточно долгого времени, ни в международных актах, ни в национальном законодательстве никаких специальных правил о порядке получения, хранения, обработки и передачи персональных данных не было. Но, с появлением информационных технологий в 60 - 70 годах значительно увеличился интерес к персональным данным и частной жизни. Изобретение мощных компьютеров и, соответственно, появление возможности их использования в качестве средства слежки и контроля частной жизни повлекло за собой необходимость принятия нормативных актов, регулирующих сбор и обработку персональных данных. Поэтому, начиная с 1970-х гг. в промышленно развитых странах стало появляться соответствующее законодательство. Таким образом, история формирования законодательной базы защиты персональных данных насчитывает более чем тридцатилетнюю историю. В 1973 и 1974 гг. Комитет министров Совета Европы принял две резолюции о защите неприкосновенности частной жизни в связи с созданием электронных банков данных — одну для частного, другую для государственного сектора. Обе резолюции рекомендуют правительствам стран — членов Совета Европы принять меры к обеспечению соблюдения базовых принципов защиты, относящихся к получению данных, качеству данных и праву частного лица на получение информации о своих персональных данных и способах их использования.

На национальном уровне, первый закон о защите персональных данных был принят в Германии, в земле Гессен в 1970 году. До принятия этого закона в мире не было подобных актов. В целом, по состоянию на сентябрь 2011 года насчитывается уже 76 стран, в которых действуют законы, регулирующие порядок защиты неприкосновенности частной жизни и персональной информации. Перечень некоторых из них приводится в Приложении 1. Недавно они впервые были приняты в таких странах, как Ангола, Украина и Индия. В законодательных органах Бразилии, Грузии, Филиппин, Таиланда, Ганы и Южной Африки рассматриваются проекты таких законов. Всего в настоящее время, за пределами Европы есть 27 законов о неприкосновенности частной жизни.

Первое поколение законов о защите личных данных зародилось в период, когда вычислительные системы использовались немногочисленными, и прежде всего, государственными контролерами данных (термин является аналогом определения «держатель»). Основная угроза, по мнению авторов законов первого поколения, заключалась в том, что некое государство, получив доступ ко всем информационным банкам данных, превратится в информационную супердержаву. Поэтому, формулируя требования законодательства, авторы старались особое внимание уделить новым технологиям обработки информации и сделать их применение управляемым и прозрачным.

Главным фактором, благодаря которому родилось второе поколение законодательства о защите персональных данных, стало решение Федерального конституционного суда Германии, объявившего в декабре 1983 года некоторые изменения, внесенные в этом же году в Закон о защите данных, не соответствующими Конституции Германии.

Общий смысл этого решения сводился к тому, что, согласно Конституции, каждому человеку гарантируется право самоопределения в использовании, передаче и раскрытии его личных данных. Суд также постановил, что право самоопределения должно быть надлежащим образом обеспечено и при электронной обработке личных данных, поскольку «нет никакой необходимости отказываться от современных технологий и переходить на бумажные картотеки». Тем не менее, в случае электронной обработки возникают существенные угрозы для права самоопределения, так как обладатель этого права не может с достаточной достоверностью знать, что в конкретный момент происходит с его данными, и поэтому личные данные, обрабатываемые в электронной форме, должны быть защищены более надежно, чем бумажные картотеки. Это решение оказало огромное влияние на законы целого ряда европейских государств: принципы, заложенные в нем, появляются в законодательстве о защите личных данных ряда европейских стран.

Характеризуя второе поколение законодательства о защите личных данных (1990-е годы), можно отметить один наиважнейший фактор: законодательство этого поколения гарантирует человеку соблюдение его прав в отношении личных данных в процессе всего цикла их обработки, и не ограничивается отдельными его элементами. Законодатели поняли, что решение гражданина не может быть ограничено его согласием или несогласием в отношении автоматизированной обработки данных, так как технологии обработки информации с использованием ЭВМ проникли в общество до такой степени, что несогласие повлечет за собой существенное увеличение стоимости обработки данных, прежде всего для их владельца.

Нормативные акты в отношении защиты личных данных, принимавшиеся в тот период, становились все более абстрактными и отвязанными от конкретных технологических решений: технический прогресс, массовое использование ЭВМ и популяризация компьютерных сетей в скором времени сделали бы прежние методы регулирования невозможными. Именно поэтому законодатели старались максимально обеспечить право человека на самоопределение в отношение своих личных данных, которое, по крайней мере, теоретически, наделяет человека способностью отстоять свои права на защиту его данных при любой форме их обработки. Требования к технической защите автоматизированных систем были понижены, и благодаря этому был достигнут оптимальный баланс между эффективностью и безопасностью обработки данных.

Потребность в разработке межгосударственных нормативных актов возникла сразу же после принятия национальных законов о защите личных данных в США и Европе, дабы не создавать препятствий для их трансграничной передачи.

Первым документом такого уровня стали Рекомендации о защите личных данных при их трансграничной передаче, разработанные Организацией экономического сотрудничества и развития в 1980 году. Первичная цель этого документа — избежать препятствий для полноценного экономического сотрудничества, связанных с необоснованными требованиями к защите личных данных.

Следующим шагом стало принятие в 1981 году Советом Европы Конвенции о защите личности в связи с автоматической обработкой персональных данных (Страсбург, 28 января 1981 г.), к которой приняты дополнения от 15 июня 1999 г., позволяющие вступление европейских сообществ в Конвенцию. Данная Конвенция - первый обязывающий международный инструмент, защищающий физических лиц от злоупотреблений, которые могут иметь место при сборе и обработке данных, и ставящий в то же время задачу регулировать трансграничный поток персональных данных. Конвенция не только дает гарантии применительно к сбору и обработке персональных данных, но и запрещает, если национальное право не обеспечивает надлежащих гарантий, обработку «чувствительных» данных относительно расовой принадлежности лица, его политических взглядов, здоровья, религии, сексуальной жизни, уголовного прошлого и т.п. Конвенция также дает лицу право знать, что данные о нем собраны, и в случае необходимости иметь возможность их исправить. Ограничения изложенных в Конвенции прав возможны только в случае, когда под угрозой оказываются высшие интересы (т.е. безопасность государства, интересы обороны и т.д.). Конвенция также предписывает определенные ограничения применительно к трансграничным потокам личных данных в те государства, где правовое регулирование не обеспечивает их должной защиты. Основным мотивом разработки Конвенции являлась необходимость гармонизации законодательства европейских стран, поэтому в 1981 году Еврокомиссия публикует рекомендации для государств-членов ЕС принимать соответствующие соглашения об использовании Конвенции. По состоянию на 13 апреля 2011 года общее число ратификаций/вступлений в силу Конвенции составляет 43.

В 1995 году была принята Директива Европейского парламента и Совета Европейского Союза от 24 октября 1995 года № 95/46/ЕС «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных» (в редакции Регламента Европейского парламента и Совета ЕС 1882/2003 от 29 сентября 2003 года). Основная цель, дважды продекларированная в Директиве, является производной от статьи 100а Соглашения о создании Европейского Экономического Сообщества, а именно — создание единого внутреннего рынка.

Третье поколение законодательства о персональных данных представлено в Европе Директивой Европейского Парламента и Совета Европейского Союза от 12 июля 2002 года № 2002/58/ЕС «В отношении обработки персональных данных и защиты конфиденциальности в секторе электронных средств связи» (Директива о конфиденциальности и электронных средствах связи) (в редакции Директивы 2006/24/ЕС Европейского парламента и Совета ЕС от 15 марта 2006 г., Директивы 2009/136/ЕС Европейского парламента и Совета ЕС от 25 ноября 2009 г.). Директива обеспечивает гармонизацию национальных положений, необходимых для гарантии соответствующего уровня защиты основных прав и свобод, и, в частности, права на частную жизнь и конфиденциальность информации о частной жизни в связи с обработкой персональных данных в сфере электронных коммуникаций, и для обеспечения свободного движения таких данных, передвижения оборудования для электронной связи и услуг электронной связи в Сообществе. Основной тренд этого поколения документов направлен на обеспечение права самоопределения человека при автоматизированной обработке его персональных данных в условиях глобализации современного мира, когда все границы стерты: в Директиве 2002/58/ЕС говорится о минимизации персональных данных в пользовательских сетях и их анонимности везде, где это возможно.

В Декларации Комитета министров о правах человека и верховенстве права в Информационном Обществе от 13 мая 2005 года CM (2005) 56 final подчеркуивается, что Государства-члены должны поддерживать условия для саморегулирования и совместного регулирования со стороны частного сектора в целях защиты права на частную жизнь и тайну переписки. Ключевым принципом поддержки такого регулирования должно быть то, что любая обработка персональных данных госорганами или частным сектором должна быть совместимой с правом на частную жизнь; исключения ограничены рамками параграфа 2 Статьи 8 Конвенция о защите прав человека и основных свобод (Рим, 4 ноября 1950 г.) и параграфа 2 Статьи 9 Конвенции о защите граждан при автоматической обработке персональных данных.

Таким образом, на сегодняшний день, Европейское право в области защиты персональных данных, прошедшее через долгий путь становления и модернизации, не прекращающийся и по сей день, является весьма прагматичным: оно дает защиту тем объектам и субъектам, которым эта защита необходима, и ровно настолько, насколько эта защита экономически оправдана. Такой подход оказался крайне эффективным: меры по защите систем обработки персональных данных не кажутся избыточными и, что самое главное, являются весьма действенными: согласно социологическим исследованиям, 80% европейских операторов и субъектов персональных данных считают себя защищенными.

В рамках СНГ был разработан Модельный закон «О персональных данных» (принят на четырнадцатом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ, постановлением от 16 октября 1999 года № 14-19), в основу которого положен европейский подход к персональным данным. Кроме того, в Москве 28 октября 2010 года был подписан Меморандум о сотрудничестве уполномоченных органов по защите прав субъектов персональных данных, правда, без участия представителей РК.

Что касается, биометрических данных, то следует отметить, что в 2002 году 118 стран мира подписали под эгидой ICAO Новоорлеанское соглашение «Doc 9303. Машиносчитываемые проездные документы. Часть 1 Машиносчитываемые паспорта. Том 2. Спецификации на электронные паспорта со средствами биометрической идентификации», которое признает биометрику лица (на остальные параметры большинство стран пока не согласились из-за дороговизны мероприятия) основой идентификации для загранпаспортов и въездных виз следующего поколения.

Вопросы защиты персональных данных находятся в призме внимания мирового сообщества и в последнее время. Так, в Довильской декларации «Группы восьми» «Неизменная приверженность свободе и демократии» (27 мая 2011 года) говорится: «Мы призываем разработать общие подходы, с учетом национальных законодательств и на основе соблюдения основных прав, которые защищали бы персональные данные, в то же время позволяя осуществлять законную передачу данных».

На пятом совещании Форума по управлению использованием Интернета «Сотворение будущего совместными усилиями» (Вильнюс, 14-17 сентября 2010 года) было отмечено, что разработка законов о неприкосновенности частной жизни в действительности является вкладом в усиление безопасности. Как отмечалось, это особенно касается случаев хищения персональных данных, которые приобретают самые большие масштабы в странах с наиболее слабой защитой неприкосновенности частной жизни.

В Мадридской декларации о защите личных данных «Глобальные стандарты по защите личных данных для глобального мира» (3 ноября 2009 года) предупреждается, что законодательство в области защиты личных данных и институты, работающие в этом направлении, не могут в полной мере учитывать новые методы наблюдения, применяемые на практике, включая «поведенческий таргетинг», базы данных ДНК и других биометрических показателей, объединение данных государственного и частных секторов, а также особые факторы риска, которым подвержены уязвимые группы населения (дети, мигранты, представители меньшинств).

Подводя итоги, следует отметить, что при рассмотрении зарубежного опыта правового регулирования использования персональных данных обращает на себя внимание унифицированность, которая выражается в обеспечении безопасности собранных персональных данных; обеспечении механизмов, которые позволяют субъекту персональных данных узнавать о наличии и о содержании его персональных данных, а также требовать их исправления; ограничение объема и использования персональных данных перечнем целей, для которых они предназначены, которые не могут быть изменены без согласия субъекта персональных данных; указание лиц и их реквизитов, несущих ответственность за соблюдение решений и правил, касающихся защиты персональных данных и неприкосновенности частной жизни, а также создание специального органа, обеспечивающего контроль за соблюдением прав субъекта персональных данных (например, Комиссии, Управления и пр.), усиленный режим охраны особых категорий персональных данных (о национальной принадлежности, взглядах и убеждениях, здоровье и сексуальной жизни, судимостях). Различия в национальных подходах, проявляющиеся в настоящее время в законах, законопроектах и законодательных предложениях, касаются таких аспектов, как масштаб действия законодательного акта, акцентирование в нем различных элементов системы защиты, детальное соблюдение вышеперечисленных принципов, а также система контроля за исполнением законодательства. Кроме того, в качестве примеров можно указать на различия в категоризации данных, не подлежащих разглашению, и в методах обеспечения открытости и индивидуального участия. Разумеется, традиционные различия между юридическими системами разных стран также служат источником несоответствий - как с точки зрения подходов к законотворчеству, так и в смысле детальной разработки регулятивных рамок для защиты персональных данных. Некоторые страны считают, что механизмы защиты данных, относящихся к частным лицам, могут быть аналогичны тем, что необходимы для защиты данных, касающихся деловых предприятий, ассоциаций и групп, обладающих или не обладающих статусом юридического лица. Опыт ряда стран также свидетельствует о том, что четко разграничить персональные и неперсональные данные достаточно сложно. Например, данные, относящиеся к небольшой компании, могут одновременно затрагивать ее владельца или владельцев и содержать более или менее секретную персональную информацию. В подобных случаях ОЭСР рекомендуется распространять действие механизмов защиты, применяемых главным образом к персональным данным, и на корпоративные структуры.

Законодательной базой любой национальной системы защиты персональных данных служит закон типа Data Protection Act (Закон о защите данных). В некоторых национальных системах защиты данных системообразующее законодательное ядро состоит не из одного, а из двух взаимодополняющих законов - закона типа Data Protecton Act и закона типа Information Freedom Act (Закон о свободе информации, принятие которого в РК постоянно откладывается), которые нередко даже разрабатываются и принимаются одновременно. В других системах принцип свободы доступа к информации непосредственно закладывается в положениях закона как Data Protecton Act.

Обобщенную структуру закона типа Data Protection Act составляют:

1) признаки персональных данных;

2) права субъекта данных в связи с обработкой и использованием данных о нем;

3) установленные законом правила доступа к чужим персональным данным, их раскрытия и передачи;

4) изъятие из правового регулирования данных в интересах государственной и общественной безопасности, в связи с расследованием преступлений и т. п.;

5) установленные законом меры правового регулирования сбора, хранения, обработки, передачи и использования персональных данных:

- учреждение национального органа власти (или системы органов власти) по защите персональных данных,

- регистрация (или лицензирование) обработки персональных данных; создание и ведение национальных регистров держателей и пользователей персональных данных,

- лицензирование передачи персональных данных за пределы национальной территории;

6) требования к организационно-техническим мерам по обеспечению безопасности данных при их сборе, обработке, использовании, передаче и хранении;

7) нормы, устанавливающие ответственность за нарушения принципов защиты данных и иных положений закона о защите данных.

Унифицированный международный подход также исходит из того, что обработка персональных данных в государственном и частном секторе должна осуществляться:

1) справедливо, законно и на пропорциональной основе для достижения конкретных, четко сформулированных и законных целей;

2) на основании прозрачной политики, адекватного информирования субъектов данных, и без какой-либо произвольной дискриминации в отношении них;

3) с соблюдением точности, приватности и безопасности данных, законности обработки, а также прав субъектов данных на доступ, исправление, уничтожение данных, а также на возражение против их обработки;

4) с соблюдением принципов подотчетности и ответственности, даже если обработка производится поставщиками услуг от имени государственных органов;

5) с обеспечением соответствующих гарантий, если данные являются уязвимыми (уязвимыми считаются следующие персональные данные: Данные, которые затрагивают наиболее интимные сферы жизни субъекта данных, или Данные, которые, в случае злоупотреблений, могут: Привести к незаконной или произвольной дискриминации, или Повлечь серьезный риск для субъекта данных);

6) с обеспечением того, чтобы персональные данные, передаваемые за границу, пользовались защитой, предусмотренной вышеупомянутыми стандартами;

7) при условии контроля со стороны независимых и беспристрастных надзорных органов, наделенных соответствующими полномочиями и ресурсами, а также обязанных сотрудничать между собой;

8) с применением современных профилактических мер, направленных, в частности, на предупреждение и выявление нарушений, основанных на назначении должностных лиц, ответственных за приватность, а также на эффективных проверках и оценках влияния на приватность.

Таким образом, законы о защите неприкосновенности частной жизни и индивидуальных свобод в сфере персональных данных стараются охватить все последовательные этапы цикла, начиная со сбора данных и заканчивая их уничтожением, и обеспечить при этом максимально полное информирование, участие и контроль со стороны индивидуума.

III. Текстуальный и существенный анализа законопроекта и рекомендации по его совершенствованию

Согласно пункту 3 статьи 19 Закона Республики Казахстан от 24 марта 1998 года № 213-I «О нормативных правовых актах» (с изменениями и дополнениями по состоянию на 05.07.2011 г.), текст нормативного правового акта излагается с соблюдением норм литературного языка, юридической терминологии и юридической техники, его положения должны быть предельно краткими, содержать четкий и не подлежащий различному толкованию смысл. В соответствии с Нормативным постановлением Конституционного Совета от 27 февраля 2008 года № 2, закон должен соответствовать требованиям юридической точности и предсказуемости последствий, то есть его нормы должны быть сформулированы с достаточной степенью четкости и основаны на понятных критериях, позволяющих со всей определенностью отличать правомерное поведение от противоправного, исключая возможность произвольной интерпретации положений закона. Между тем, изучение Проекта показывает, что ряд предлагаемых в нем норм сформулирован с нарушением правил юридической техники, в результате чего некоторые его предписания выражены нечетко. Речь идет о следующих положениях Проекта, рассматриваемых ниже постатейно.

Преамбула Проекта.

Различается деятельность, связанная с обработкой персональных данных, с использованием средств автоматизации или без использования таких средств.

Между тем, далее по тексту закона не приводится определение понятия «средства автоматизации». В действующем законодательстве, только в Законе Республики Казахстан от 11 января 2007 года № 217-III «Об информатизации» (с изменениями и дополнениями по состоянию на 21.07.2011 г.) содержится определение автоматизации, как применения информационно-коммуникационных технологий для обработки, систематизации, хранения и передачи информации с целью облегчения и вытеснения форм человеческого труда, повышения производительности и прозрачности процессов. Соответственно, под средствами автоматизации следует понимать информационно-коммуникационные технологии.

Не приводится четких критериев для отграничения случаев, когда средства автоматизации используются и когда не используются.

В случаях, когда средства автоматизации не используются, идет ли речь о неавтоматизированной обработке систематизированных наборов персональных данных (списков, картотек, дел, сводов и т.д.), когда обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации: позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным? Если да, то почему бы это не указать прямо в законе?

Чтобы конкретизировать такое положение, обратимся к опыту Европейского Союза, в частности, к Директиве 95/46/ЕС, в которой более четко формулируется сфера ее применения в отношении персональной информации, обрабатываемой без средств автоматизации. Директива применима к неавтоматизированной обработке, если при этом данные структурированы, систематизированы (классифицированы) в файлы (досье) на основании определенных критериев, что облегчает доступ к нужной информации (файлу, досье). В действительности, в этом случае, как и в случае с автоматизированной обработкой, персональная информация представлена виде базы данных, только без использования средств автоматизации, и характер операции с файлами и досье аналогичен характеру операций, производимых с файлами при автоматизированной обработке; впрочем, представить обратную ситуацию, когда сведения персонального характера не были бы структурированы при неавтоматизированной обработке, крайне затруднительно. Для справки: под файлом в Директиве понимается систематизированная определенная совокупность персональных данных, к которой можно получить доступ, найти в базе на основании определенных критериев — идентификаторов, имени, фамилии и т.д.

Статья 1. Основные понятия, используемые в настоящем Законе

3) объект персональных данных

Правовая защита персональных данных это, своего рода, договор гражданина с государством и его органами власти, гарантирующий ему неприкосновенность личной жизни, и регламентирующий тот минимум сведений, которые мы готовы сообщить о себе, чтобы быть служащими учреждений, клиентами банков, посетителями различных организаций и т.д. В конечном итоге, защита персональных данных, это защита не информации, а персоналий. В связи с этим, главное и концептуальное возражение по Проекту вызывает предложение называть физическое лицо, к которому относятся соответствующие персональные данные - объектом, а не субъектом персональных данных. По тексту Проекта говорится о правах объектов, но какие права могут быть у объекта?

Между тем, согласно пункту 1 статьи 13 Конституции Республики Казахстан (принята на республиканском референдуме 30 августа 1995 года) (с изменениями и дополнениями по состоянию на 02.02.2011 г.), каждый имеет право на признание его правосубъектности и вправе защищать свои права и свободы всеми не противоречащими закону способами. Нормы пункта 1 статьи 13 Конституции развиты в гражданском законодательстве: категорию «правосубъектность» составляют гражданско-правовые понятия правоспособности и дееспособности граждан.

В статье 13 Гражданского кодекса Республики Казахстан,принят Верховным Советом Республики Казахстан 27 декабря 1994 года (с изменениями и дополнениями по состоянию на 22.07.2011 г.) установлено, что способность иметь гражданские права и нести обязанности (гражданская правоспособность) признается в равной мере за всеми гражданами. Именно граждане являются субъектами гражданских прав, а объектами гражданских прав могут быть имущественные и личные неимущественные блага и права. К личным неимущественным благам и правам и относятся, в том числе, неприкосновенность частной жизни, личная и семейная тайна.

Также, например, в статье 3 Закона Республики Казахстан от 11 января 2007 года № 217-III «Об информатизации» (с изменениями и дополнениями по состоянию на 21.07.2011 г.) указывается, что объектами информатизации являются: электронные информационные ресурсы, информационные системы, информационные работы и электронные услуги, а вот к субъектам информатизации относятся: государственные органы, физические и юридические лица, осуществляющие деятельность или вступающие в правоотношения в сфере информатизации на территории Республики Казахстан.

Попытка же представить человека и гражданина объектом, заставляет предположить, что субъектом в данном случае, государственные органы-разработчики Проекта видят себя.

2) персональные данные

Проект использует выражение «информация (зафиксированная на материальном носителе)». Такая же формулировка есть и в Модельном законе «О персональных данных» (принят на четырнадцатом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ, постановлением от 16 октября 1999 года № 14-19). Однако, если в Модельном законе расшифровывается, что такое материальные носители (материальные объекты (в том числе физические поля), в которых персональные данные находят свое отображение в виде символов, образов и сигналов), то в казахстанском Проекте, да и в целом, в законодательстве такого определения нет.

Если объектом (субъектом) персональных данных является любое физическое лицо, то речь может идти не только о гражданах Республики Казахстан, но также и о иностранных гражданах и лицах без гражданства, которых также нельзя ущемлять в личных правах. В таком случае, не понятно, почему в число персональных данных не включена информация о гражданстве? Она, как и еще ряд данных указана, например, в Постановлении Правительства Республики Казахстан от 5 июня 2007 года № 460 «Об утверждении перечня персональных данных физических лиц, включаемых в состав государственных электронных информационных ресурсов».

Если персональные данные работника - информация о работнике, необходимая при возникновении, продолжении и прекращении трудовых отношений, не понятно, почему в число персональных данных включена только информация о профессии, а не сведения о трудовой деятельности (данные о трудовой занятости на текущее время с полным указанием должности, подразделения, организации и ее наименования, ИНН, адреса и телефонов, а также реквизитов других организаций с полным наименование занимаемых ранее в них должностей и времени работы в этих организациях, сведения о номере, серии и дате выдачи трудовой книжки (вкладыша в нее) и записях в ней, содержание и реквизиты трудового договора с работником организации или гражданско-правового договора с гражданином, сведения о заработной плате (номера счетов для расчета с работниками, данные зарплатных договоров с клиентами, в том числе номера их спецкартсчетов и т.д.)?

По непонятной причине из понятийного аппарата и в целом из Проекта было удалено понятие «специальные категории персональных данных» - персональные данные о расовой, национальной принадлежности, наличии судимости, политических взглядах, религиозных или философских убеждениях, членстве в профессиональном союзе, состоянии здоровья, интимной жизни. По сложившейся международной практике, они относятся к категории особых персональных данных, которым предоставляется особый, усиленный режим правовой защиты. Исключение этой нормы из Проекта явно не будет способствовать защите прав и свобод граждан.

В целом, если рассматривать персональные данные как любую информацию, связанную с физическим лицом - субъектом данных, идентичность которого известна или может быть установлена непосредственно или косвенно путем использования таких данных как индивидуальный идентификационный номер, один или несколько физических, физиологических, психологических, экономических, культурных или социальных признаков, характерных для лица, то казахстанская формулировка представляется зауженной. При том, что сопутствующий проект («О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам персональных данных») оставляет довольно широкие формулировки в Трудовом кодексе (персональные данные работника — информация о работнике, необходимая при возникновении, продолжении и прекращении трудовых отношений, ст. 65) и Законе об информатизации (персональные данные (электронные информационные ресурсы персонального характера) - сведения о фактах, событиях, обстоятельствах жизни физического лица и (или) данные, позволяющие идентифицировать его личность), п.п. 17 ст.1).

Но авторы основного Проекта приняли точку зрения тех, кто предлагал дать исчерпывающий перечень сведений, которые законом отнесены к категории персональных данных. В связи с чем возникает вопрос о том, почему законом не будут защищаться такие персональные данные, которые зачастую используются для противоправных действий, как номер сотового телефона, адрес электронной почты, номер водительских прав, номер кредитной карточки и т.д.? Ведь опыт правового регулирования в других странах опровергают такой подход. Исчерпывающий перечень не может быть установлен и, более того, не должен устанавливаться законом, поскольку любое ограничение содержания персональных данных выльется в ограничение прав субъекта персональных данных. Можно попытаться классифицировать персональные данные и дополнить определение перечнем соответствующих групп информации, но и этот перечень должен быть открытым. Другой способ доопределения персональных данных заключается в установлении перечня сведений, которые нельзя отнести к персональным данным, защищаемым законом.

Статья 2. Цель настоящего Закона

Если, как указанно в данной статье, целью Закона действительно является обеспечение защиты прав и свобод человека при обработке его персональных данных, то, как уже указывалось выше, не следует его называть объектом персональных данных.

Статья 3. Сфера действия настоящего Закона

Первоначально Проект содержал перечень из четырех видов отношений, на которые действие закона не будет распространяться. Что, в принципе, соответствовало общепринятой международной практике. Очевидно, в процессе согласования Проекта разработчиком с иными государственными органами, каждый из них постарался по максимуму вывести свою сферу регулирования из-под действия закона. В результате этот перечень оказался расширен до 22 позиций и заканчивается расплывчатым указанием на иные случаи, предусмотренные законодательными актами Республики Казахстан. Очевидно, что такие неоправданно широкие формулировки, позволяющие полностью освободить от гарантий, предусмотренных Проектом, например, деятельность при осуществлении уголовно-процессуального, уголовно-исполнительного, административного законодательства Республики Казахстан, а также в целях обороны страны, безопасности государства и охраны правопорядка, не могут быть признаны приемлемыми. Также в Проекте указано, что действие настоящего Закона не распространяется на отношения, возникающие при отправлении правосудия, но не указано, насколько это применимо к размещению персональных данных в Единой автоматизированной информационно-аналитической системы судебных органов Республики Казахстан и т.д.

Поэтому вышеуказанный перечень следует максимально сузить и предельно конкретизировать, исходя из того, что все без исключения организации являются держателями персональных данных и должны рассматривать требования Закона о персональных данных с точки зрения обеспечения прав и свобод граждан, закрепленных Конституцией РК. Возможно, в Проекте следует просто указать, что при обработке персональных данных в целях безопасности, обороны и т.д., по перечню, настоящий Закон применяется в том объеме, в каком другими законами не установлено иначе. В противном случае, государственным органам будет создан комфортный режим, при котором им фактически не будет чиниться никаких существенных препятствий при сборе, обработке и использовании персональных данных граждан, а дополнительные обязанности возникнут лишь у частных организаций.

Проект не содержит возможности распространения персональных данных, если эта информация является общественно важной, что является существенным ограничением свободы слова. Например, Проект не содержит понятия «публичного лица». А как известно из практики Европейского суда по правам человека, о таких людях без их согласия можно собирать и распространять данные персонального характера, если они являются важными для общества. В Проекте существует исключение только в отношении кандидатов на выборные государственные должности.

Статья 4. Принципы обработки персональных данных

Логичным продолжением данной статьи должна была стать статья 7 «Условия обработки персональных данных», которую объединили со статьей 3. В результате, если раньше перечисленные там виды деятельности просто не требовали согласия субъектов персональных данных, то теперь они вообще выведены из сферы действия закона. С этим никак нельзя согласиться.

Статья 5. Законодательство Республики Казахстан в области персональных данных

Пункты 2 и 3 фактически дублируют содержание статьи 4 Конституции РК. Непонятно, зачем их повторять в законе.

Статья 6. Порядок получения или отзыва согласия объекта на обработку персональных данных

Персональные данные должны быть получены и использованы добросовестным и законным образом, что предполагает, прежде всего, наличие согласия субъекта, то есть реализацию права на информационное самоопределение, за исключением случаев, прямо установленных законом. Суть проблемы в том, что Проектом предусмотрено согласие на обработку персональных данных в двух формах: на бумажном носителе, подписанном собственноручно или в форме электронного документа, удостоверенного посредством ЭЦП. Этим Проект рискует фактически поставить вне закона всю интернет-коммерцию и заблокировать возможность использования веб-технологий для передачи пользователями всемирной сети Интернет своих персональных данных, даже если они действуют по собственной воле и в собственном интересе. Вне закона, могут оказаться популярные социальные сети, а использование электронной почты, если строго следовать нормам закона, налагает на владельцев почтовых серверов и даже почтовых ящиков практически невыполнимые требования. Связано это с тем, что ЭЦП на сегодня и ближайшую перспективу имеет весьма ограниченное хождение в Казахстане и используется преимущественно для доступа к государственным сервисам Электронного правительства. Наивно также ожидать, что владельцы разного рода социальных сетей, форумов, блоггерских площадок и т.п. интернет-ресурсов, собирающих персональные данные своих пользователей, заведут с ними длительную бумажную переписку. Как контролировать подлинность и правомерность размещения персональных данных в аккаунтах пользователей, как получить согласите на перевод всего, что на странице пользователя указано, в категорию общедоступных? Что касается электронной почты, то даже если некая организация, предоставляет этот сервис только своим работникам, то, наверняка в подписях электронных писем, получаемых ими, содержатся сведения об их корреспондентах - фамилии, имена и отчества, названия должностей, номера телефонов, адреса электронной почты, как минимум. Как быть, если отправитель сообщает в электронном письме или в сообщениях на форумах свои персональные данные и передает их по незащищенным каналам связи? Как может владелец интернет-магазина доказать согласие на обработку персональных данных покупателя? Ведь покупки в сети Интернет связаны с сообщением магазину данных, необходимых для оплаты и доставки заказанного товара или услуги. А если это данные не покупателя, а какого-то другого человека, которые покупатель посчитал нужным использовать при оформлении заказа, а это третье лицо не только не давало согласия, но и знать не знает об использовании его данных? Как быть при покупке в Интернете авиабилетов, когда пассажир может указать не только свои данные, но сведения о других лицах, для которых приобретаются билеты? Организация, в которой я работаю, в числе прочих видов деятельности, занимается поиском и систематизацией информации, в т.ч., относящейся к персональным данным (типа справочников «кто есть кто» и т.п.) в открытых источниках. Но вдруг кто-то из субъектов, увидев информацию о себе, посчитает свои права нарушенными, а информацию - полученной незаконным способом? Чтобы доказать свою правоту, мы должны не только хранить все скрин-шоты сайтов, с которых были получены данные, но и, поскольку их достаточно легко подделать (модифицировать), все эти скрин-шоты нотариально заверять. Иначе выполнить требования закона о необходимости доказательства общедоступности данных практически невозможно. Отдельная тема, это получающий все большее распространение такой способ поиска работы и кандидатов на вакансии как интернет-рекрутинг. Сегодня ты заходишь на сайт, авторизуешься, создаешь по заданной форме свое резюме, указываешь предпочтения и ждешь, когда начнут поступать предложения. А с принятием Проекта проще будет пешком сходить в кадровое агентство. Получение письменного согласия делает весь бизнес незаконным или абсолютно бессмысленным. При этом интересы самих соискателей вакансий, для защиты интересов которых вроде бы и создается закон, абсолютно не учтены.

Характерно, что действующий Закон Республики Казахстан от 11 января 2007 года № 217-III «Об информатизации» (с изменениями и дополнениями по состоянию на 21.07.2011 г.), очевидно учитывающий данную специфику сетевых отношений, не предъявляет подобных требований в статьях, посвященных персональным данным (13, 44).

Но следует признать, что в этом направления также есть ряд проблем. Например, в Казахстане информация об администраторах доменов в зоне KZ является общедоступной, т.е. любой желающий может свободно получить сведения об администраторе домена, его контактные данные, место прописки. А ряд стран перестали публиковать данные об администраторе домена, дабы защитить персональные данные (например, в России, с принятием закона о защите персональных данных).

В качестве альтернативного зарубежного опыта можно привести следующие формулировки:

согласие субъекта персональных данных - любое документированное, в частности письменное, добровольное волеизъявление физического лица о предоставлении разрешения на обработку его персональных данных в соответствии с сформулированной целью их обработки (ст.2 Закона Украины от 1 июня 2010 года № 2297-VI «О защите персональных данных»);

согласие - добровольное выражение воли субъекта данных относительно обработки его персональных данных с известной ему целью. Согласие на обработку особых персональных данных должно быть выражено ясно - в письменной, в приравненной к ней или в другой форме, несомненно доказывающей волю субъекта данных (ст. 2 Закона Литовской Республики «О правовой защите персональных данных от 11 ноября 1996 г. № I-1374, редакция на 1 сентября 2011 года).

В этой части также, возможно, решить проблему смогла бы легализация согласия на обработку персональных данных действием, например, когда субъект персональных данных регистрируется на интернет-ресурсе или пользуется магазином, в котором висит плакат о ведущейся видеосъемке. Следует, однако, отметить, что даже законодательное закрепление «согласия действием» в данном случае не поможет, так как во многих случаях человек попадает в поле видеокамеры прежде, чем знакомится с предупреждением о ведущейся видеосъемке. Получается, это должен быть специально оговоренный случай, не требующий получения согласия на обработку персональных данных.

Статья 7. Особенности обработки биометрических персональных данных

Логичным и соответствующим международной практике было бы указать в рамках данной статьи, как именно должно получаться согласие при широко распространенной сейчас практике повсеместного сбора биометрических персональных данных в видеозаписях внутренних и наружных систем охранного телевидения и банковских терминальных устройств, при получении данных в устройствах, использующих для идентификации биометрические данные человека. Напомним, что в Национальном плане действий в области прав человека в Республике Казахстан на 2009-2012 годы (одобрен резолюцией Президента Республики Казахстан от 5 мая 2009 года № 32-36.125) указывается, что: «использование данных видеонаблюдения также должно подлежать правовому регулированию с целью защиты прайвеси», «необходимы законодательные ограничения на видеонаблюдения и закрепление обязанности работодателя согласовывать подобные вопросы с работником».

Возникает и ряд иных вопросов по применению данной статьи, например, обязательно ли получать отдельное письменно согласие по форме на размещение фотографии работника организации на личном листке по учету кадров, на удостоверении сотрудника организации и в общедоступных источниках организации (в т.ч. в электронном виде, на интернет-ресурсах организации и т.д.), при оказании услуг по снятию ксерокопии с документов, удостоверяющих личность и имеющих фотографию владельца?

Вряд ли стоит отдавать столь важные вопросы на откуп подзаконных актов.

Статья 12. Международная передача персональных данных

То, что заключение международных коммерческих контрактов было выведено из под сферы действия закона, было сделано по предложению НЭП «Союз «Атамекен».

Обоснование этому было названо то, что защита прав объектов персональных данных будет существенно тормозить процесс обмена сведениями с зарубежными партнерами, делая невозможными многие коммерчески перспективные проекты. Однако, каким именно образом этот процесс будет тормозиться и почему коммерческие интересы должны в данном случае превалировать над правами человека, не вполне понятно.

Единственное условие, обозначенное в статье 12, - обеспечение адекватной защиты персональных данных иностранным государством, на территорию которого осуществляется их передача. Однако, каким образом держатель будет определять достаточность такой защиты - совершенно непонятно. В Российской Федерации 25 июля 2011 года, в связи с многочисленными вопросами по применению, схожая формулировка статьи 12 «Трансграничная передача персональных данных» Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» была полностью изложена в новой редакции.

Кроме того, международные стандарты указывают, что национальное законодательство, относящееся к стороне, передающей данные, может разрешить международную передачу персональных данных в государства, которые не обеспечивают уровень защиты, предусмотренный в данном документе, если такая передача необходима и производится в интересах субъекта данных в рамках договорных отношений, для защиты жизненно важных интересов субъекта данных или другого лица, либо когда это требуется по закону в общественных интересах.

Проект также умалчивает, кем, в каком порядке и объеме, при наступлении каких обстоятельств и в каком соотнесении с международными обязательствами может быть запрещена или ограничена трансграничная передача данных.

Если учитывать, что по Проекту распространение персональных данных включает в себя, в том числе, размещение в информационных телекоммуникационных сетях, а также то, что в нем упомянута международная передача персональных данных, но не определено, в какой мере закон распространяется на иностранные юридические и физические лица, то с его применением в отношении интернет-ресурсов определенно возникнут сложности. Ведь, где именно проходит в Интернете территория Казахстана, а где начинается территория иностранных государств, наше законодательство не поясняет. Во многих случаях владелец сайта (интернет-ресурса) обладает различной информацией о лице, посетившем этот ресурс. Посетитель сайта может добровольно заполнить анкету на сайте, ответить в ходе использования сайта на определенные вопросы его владельца; сохраняется информация о действиях посетителя на сайте (сведения о товарах, которыми интересовался посетитель, их ценовой группе и т.п.). Наконец, владельцу сайта становится доступной и определенная техническая информация о посетителе и его компьютере с помощью так называемых куки (cookie).

В этом плане, территориальная сфера действия закона выглядит достаточно туманно, оставляя ряд вопросов. Например, будет ли закон применяться при обработке персональных данных юридическими или физическими лицами, находящимися вне территории РК, но с использованием в процессе обработки средств, находящихся на территории РК и наоборот и т.д.

Статья 16. Обязанности держателя при сборе персональных данных

В европейских странах сбор персональных данных также сопряжен с выполнением ряда дополнительных условий. Наиболее распространенна обязанность оператора (держателя) данных регистрироваться (в Германии, Нидерландах и др.) или уведомлять (в Великобритании, Испании, Италии, Франции и др.) орган, уполномоченный следить за соблюдением правил о сохранности данных. Уведомление такого органа до совершения действий с персональными данными предусмотрено и Директивой Европейского Сообщества № 95/46/ЕС. Невыполнение указанной обязанности может караться серьезным штрафом или даже рассматриваться как уголовное преступление (например, в Великобритании, Италии, Нидерландах, Франции).

Статья 17. Обязанности держателя по обеспечению защиты персональных данных при их обработке

Как уже указывалось выше, если ты частный предприниматель, а вся база твоих клиентов — это небольшая табличка, которую ты держишь в программе Google Docs, «облачном» сервисе Google для документов, и физически твоя табличка находится где-то на сервере в США, то ты нарушаешь сразу несколько статей Проекта.

В статье не определен субъект, в компетенцию которого входит определение порядка процедуры оценки соответствия средств защиты информации (обеспечения соблюдения требований стандартов информационной безопасности), а также не указаны критерии оценки эффективности принимаемых мер по обеспечению безопасности персональных данных.

Статья 20. Обязанности держателя по устранению нарушений законодательства, допущенных при обработке персональных данных

Представляется, что вопрос о том, что считать достижением цели обработки персональных данных, а также какие данные подлежат хранению - достаточно неоднозначен.

Статья 21. Государственный контроль и надзор в области обработки персональных данных

Как уже указывалось выше, международная практика идет по пути создания специального органа, обеспечивающего контроль за соблюдением прав субъекта персональных данных. В казахстанском Проекте уполномоченный орган по защите прав субъектов персональных данных не определен, хотя разговоры о том, что нужно как можно скорее определить, какие органы отвечают за защиту права на частную жизнь, и какие эффективные процедуры для этого существуют, ведутся давно.

Между тем, в Мадридской декларации о защите личных данных «Глобальные стандарты по защите личных данных для глобального мира» (3 ноября 2009 года), например, содержится призыв к странам, которые еще не создали комплексных рамок и независимого органа по защите личных данных, сделать это в как можно кратчайшие сроки. В Замечаниях общего порядка Комитета ООН по правам человека 1988 года № 168 к статье 17 МПГПП прямо указывается, что необходима также информация о том, какие органы власти правомочны осуществлять контроль за подобным вмешательством в строгом соответствии с законом и в каком порядке и в каких органах заинтересованные лица могут обжаловать нарушение права, закреплённого в статье 17 Пакта.

Поскольку современные национальные системы защиты данных являются системами государственно-правового регулирования обработки и использования персональных данных, то практически все они содержат активный регулирующий компонент - национальный орган (или систему органов) по защите данных, наделяемый регистрационно-разрешительными, контрольно-надзорными, а также арбитражными, экспертными и методологическими функциями. Основные требования, предъявляемые к национальному органу по защите данных международными соглашениями о гармонизации систем защиты данных, - компетентность и независимость.

Выводы

Таким образом, проведенный анализ показал, что отдельные нормы Проекта не соответствуют направлениям, указанным в Национальном плане действий в области прав человека в Республике Казахстан на 2009-2012 годы (одобрен резолюцией Президента Республики Казахстан от 5 мая 2009 года № 32-36.125).

Технико-юридические недостатки Закона создают возможность для неоднозначного понимания некоторых содержащихся в нем положений, что на практике может привести к произвольному истолкованию и неадекватному применению данного законодательного акта и, как результат, к необоснованному ограничению прав и свобод человека и гражданина.

Приложение 1

Перечень некоторых национальных законов о защите неприкосновенности частной жизни и персональной информации

Австрия (Закон «О защите персональных данных», 1999 г.), Австралия (Закон «О неприкосновенности частной жизни», 2000 г.), Азербайджан (Закон «О персональных данных», 2010 г.), Албания (Закон «О защите персональных данных», 1999 г.), Армения (Закон «О персональных данных», 2002 г.), Бельгия (Закон «О защите персональных данных», 1992 г.), Болгария (Закон «О защите персональных данных», 2002 г.), Босния и Герцеговина (Закон «О защите персональных данных», 2001 г.), Великобритания (Закон «О защите данных», 1998 г.), Венгрия (Закон «О защите персональных данных и раскрытие данных представляющие общественный интерес», 1992 г.), Греция (Закон «О защите лиц относительно обработки персональных данных», 1997 г.), Германия (Федеральный закон «О защите данных», 1990 г.), Дания (Закон «Об обработке персональных данных», 2000 г.), Зимбабве (Закон «О доступе к информации и защите частной информации», 2002 г.), Израиль (Закон «О защите частной жизни», 1981 г.), Ирландия (Закон «О защите данных», 1988 г.), Исландия (Закон «О персональных данных», 2000 г.), Испания (Закон «О защите данных», 1999 г.), Италия (Кодекс о защите данных, 2003 г.), Канада (Закон «О защите персональной информации и электронных документов», 2000 г.), Кыргызстан («Об информации персонального характера», 2008 г.), Латвия (Закон «Об охране данных физических лиц», 2000 г.), Литва (Закон «Об правовой защите персональных данных», 1996 г.), Лихтенштейн (Закон «О защите данных», 2002 г.), Македония (Закон «О защите персональных данных», 2005 г.), Молдова (Закон «О защите персональных данных», 2007 г.), Нидерланды (Закон «О защите персональных данных», 2000 г.), Новая Зеландия (Закон «О защите частной жизни», 1993 г.), Норвегия (Закон «О персональных данных», 2000 г.), Польша (Закон «О защите персональных данных», 1997 г.), Португалия (Закон «О защите персональных данных», 1998 г.), Россия (Закон «О персональных данных», 2006 г.), Румыния (Закон «О доступе к персональному досье и его раскрытию секуритате», 1999 г., Закон «О защите лиц относительно обработки персональных данных и свободного распространения таких данных», 2001 г.), Сербия (Закон «О защите персональных данных», 1998 г.), Словакия (Закон «О защите персональных данных», 2002 г.), Словения (Закон «О защите персональных данных», 2004 г.), США (Закон «О защите частной жизни», 1974 г.; «О защите личных данных», 1980 г.), Украина (Закон «О защите персональных данных», 2010 г.), Хорватия (Закон «О защите персональных данных», 2003 г.), Чехия (Закон «О защите персональных данных», 2000 г.), Швеция (Закон «О персональных данных», 1998 г.), Швейцария (Федеральных закон «О защите данных», 1992 г.), Эстония (Закон «О защите персональных данных», 2003 г.), Финляндия (Закон «О персональных данных», 1999 г.), Франция (Закон «О защите данных», 1978 г.), Южная Корея (Закон «О защите персональной информации, находящейся в ведении органов власти»), Япония (Закон «О защите персональной информации» 2003 г.).

Информация об Уполномоченных органах по защите персональных данных,

министерств (ведомств), в компетенции которых находятся вопросы защиты персональных данных государств - участников СНГ

№

п/п

Государства-участники СНГ

Наличие закона о ПД

Орган, министерство (ведомство) по защите прав субъектов персональных данных

1.

Республика Молдова

Закон Республики Молдова

№ 17-XVI от 15.02.2007

«О защите персональных данных»

Национальный центр по защите персональных данных Республики Молдова

2.

Украина

Закон Украины «О защите персональных данных»

от 1 июня 2010 г. № 2297 VI

Государственная служба специальной связи и защиты информации Украины.

(Уполномоченный орган по вопросам криптографической и технической защиты информации)

3.

Азербайджанская Республика

Закон Азербайджанской республики «О персональных данных»

от 11.05.2010 г.

№ 998 III g

Функции осуществляют Министерство связи и информационных технологий

Министерство Юстиции Азербайджана в пределах своей компетенции

4.

Республика Беларусь

Закона о ПД нет. Есть Закон Республики Беларусь «Об информации, информатизации и защите информации»

от 10.11.2008 г.

№ 455-З

Оперативно-аналитический центр при Президенте Республики Беларусь.

(Уполномоченный орган по технической защите информации)

5.

Туркменистан

Закона нет

Занимается вопросами защиты ПД Министерство связи Туркменистана в пределах своей компетенции

6.

Республика Узбекистан

Закон разработан, но не принят (находится в Службе национальной безопасности)

Служба национальной безопасности

7.

Республика Армения

Закон Республики Армения

от 07 ноября 2002 г.

№ ЭР-422

Министерство транспорта и связи Республики Армения

Полиция Республики Армения

8.

Российская Федерация

Федеральный закон от 27 июля 2006 г. № 152-ФЗ "О персональных данных"

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), Управление по защите прав субъектов персональных данных

9.

Кыргызская Республика

Закон Кыргызской Республики от 14 апреля 2008 года № 58 «Об информации персонального характера»

Государственная

Регистрационная Служба при Правительстве Кыргызской Республики

Приложение 2

Международные акты по защите персональных данных

Универсальные международные акты

· Статья 12 Всеобщей декларации прав человека (принята и провозглашена резолюцией 217 А (III) Генеральной Ассамблеи от 10 декабря 1948 года)

· Статья 17 Международного пакта о гражданских и политических правах (Нью-Йорк, 19 декабря 1966 года)

· Основные положения Организации по экономическому сотрудничеству и развитию о защите неприкосновенности частной жизни и международных обменов персональными данными (23 сентября 1980 года)

· Статья 16 Конвенции о правах ребенка (Нью-Йорк, 20 ноября 1989 года.)

· Мадридская декларация о защите личных данных «Глобальные стандарты по защите личных данных для глобального мира» (3 ноября 2009 года)

· Резолюция Форума по управлению использованием Интернета 2010 «Сотворение будущего совместными усилиями» (Вильнюс, 14-17 сентября 2010 года)

· Резолюции Международной конференции уполномоченных органов по защите данных и приватности (2000-2010)

· Довильская декларация «Группы восьми»: «Неизменная приверженность свободе и демократии» (27 мая 2011 года)

Европейские акты

· Статья 8 Конвенции о защите прав человека и основных свобод (Рим, 4 ноября 1950 года)

· Конвенция о защите личности в связи с автоматической обработкой персональных данных (Страсбург, 28 января 1981 г., с дополнениями от 15 июня 1999 г.)

· Директива Европейского парламента и Совета Европейского Союза от 24 октября 1995 года № 95/46/ЕС «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных» (в редакции Регламента Европейского парламента и Совета ЕС 1882/2003 от 29 сентября 2003 года)

· Рекомендация Комитета Министров государствам-членам Совета Европы по защите неприкосновенности частной жизни в Интернете (1999. N R (99) 5)

· Директива Европейского Парламента и Совета Европейского Союза от 12 июля 2002 года № 2002/58/ЕС «В отношении обработки персональных данных и защиты конфиденциальности в секторе электронных средств связи» (Директива о конфиденциальности и электронных средствах связи) (в редакции Директивы 2006/24/ЕС Европейского парламента и Совета ЕС от 15 марта 2006 г., Директивы 2009/136/ЕС Европейского парламента и Совета ЕС от 25 ноября 2009 г.).

· Декларация Комитета министров о правах человека и верховенстве права в Информационном Обществе от 13 мая 2005 года CM (2005) 56 final

Иные региональные акты

· Статья 18 Каирской декларации о правах человека в исламе(1990 года)

· Статья 4.3 Декларации о принципах свободы самовыражения в Африке (2002 года)

· Статья 5 Американской декларации прав и обязанностей человека (1948)

· Структура обеспечения приватности Азиатско-тихоокеанского экономического сотрудничества (2004)

· Модельный закон «О персональных данных» (принят на четырнадцатом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ, постановлением от 16 октября 1999 года № 14-19)

Специализированные акты

Новоорлеанское соглашение ICAO 2002 года «Doc 9303. Машиносчитываемые проездные документы. Часть 1 Машиносчитываемые паспорта. Том 2. Спецификации на электронные паспорта со средствами биометрической идентификации»

Источник: Лоскутов И.Ю. Сохранить 1

0

Добавить ваш комментарий | Порекомендовать новость | Напечатать (с комментариями) | Отослать новость другу

Поделиться страницей:

ДРУГИЕ НОВОСТИ ПО ТЕМЕ