

Защита персональных данных



Обеспечение безопасности персональных данных — объективная потребность. Ведь сегодня информация о людях превращается в самый дорогой товар. Такая информация в руках злоумышленника — мощное оружие

Персональные данные — важная составляющая более широкого понятия — приватность. Поэтому защита персональных данных — это составляющая часть обеспечения приватности. Приватность, наряду со свободой слова и другими правами, является одной из основных ценностей человечества.

На сегодня основными европейскими документами в области защиты персональных данных являются Конвенция Совета Европы «О защите личности в связи с автоматической обработкой персональных данных» и Директива Европарламента «О защите физических лиц при автоматизированной обработке персональных данных», ETS № 108, 1981 г. Последняя обязательна для всех государств-членов ЕС и является предметом для подражания в области законодательства, в том числе и в нашей стране. Страны Евросоюза последовательно приводят свое законодательство в соответствие с Директивой. В Великобритании еще в 1998 году был принят «Закон о защите персональных данных» — «Data Protection Act 1998». Его техниче-

ская реализация — проект стандарта «Specification for the management of personal information in compliance with the Data Protection Act 1998» (BS 10012, 2009). Параллельно с англичанами свою версию стандарта по безопасности персональных данных выпустили в США. Проект документа по защите персональных данных для американских государственных структур — «Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)» (SP 800122) регламентирует выполнение Законов «The Privacy Act of 1974» и «Privacy Protection Act of 1980». Канада выпустила «Privacy Code» — набор документов для реализации законодательства по защите сведений о частных лицах (The Privacy Act и PIPEDA).

В государствах-членах Евросоюза определения персональных данных, как правило, максимально широкие, в результате чего гражданами на практике зачастую не выполняется соответствующее законодательство из-за излишней «нагрузки». Соответствующие органы государственной власти, как правило, не

предпринимают никаких действий, кроме особых случаев. Важными остаются вопросы возникновения коллизий между требованиями приватности и интересами свободы слова. Современными европейскими законами, как правило, запрещается сбор, хранение, использование и распространение без согласия субъекта данных именно критических персональных данных, как это сделано в Законе Украины № 2297-VI.

Украина. Право на частную жизнь

Право на приватность в нашем государстве гарантируется Конституцией Украины, в которой в статье 32 говорится: «Никто не может подвергаться вмешательству в его личную и семейную жизнь, кроме случаев, предусмотренных Конституцией Украины»* (*здесь и далее — перевод автора). Кроме того, в Конституции предусмотрена защита еще некоторых аспектов приватности. Так, статья 30 защищает неприкосновенность жилища (территориальная приватность), статья 31 — тайну переписки, телефонных разговоров, телеграфной и другой корреспонденции (коммуникационная приватность), статья 32 предусматривает запрет сбора, хранения, использования и распространения конфиденциальной информации о лице без его согласия (информационная приватность), а статья 28 предусматривает запрет подвергать лицо без его свободного согласия медицинским, научным или другим исследованиям (защищая некоторые элементы физической приватности).

Конституционные нормы определяют исчерпывающий перечень оснований для вмешательства в приватность и условий для такого вмешательства. Однако существует много отраслевых норм права, противоречащих требованиям Конституции. Именно такие нормы не соответствуют международным стандартам, практике Европейского законодательства.



Рис. 1. Веб-ресурс российского регистратора операторов персональных данных



Рис. 2. Сайт в Интернете, где за плату предлагаются базы персональных данных, например, база данных водительских удостоверений

Ситуация с защитой персональных данных в нашей стране по ряду причин требовала срочного правового вмешательства, создания отдельного законодательного акта. В марте 2006 года Верховная Рада Украины принял закон «О защите персональных данных», однако, этот закон был вето Президентом В. Ющенко, в частности, на том основании, что он не был согласован с Конвенцией Совета Европы. 9 января 2007 года проект в обновленной редакции с учетом предложений Президента был одобрен Верховной Радой. Однако затем без специальных обоснований Президент снова использовал свое право вето.

Тем временем без нормативной базы по защите персональных данных продолжалось обсуждение законопроектов и параллельно создание Единого государственного автоматизированного реестра физических лиц (ЕГАРФЛ), а также других государственных реестров, содержащих персональные данные. Несмотря на отсутствие законных оснований, Президент Украины своим Указом от 30 апреля 2004 года № 500 «О создании Единого государственного реестра физических лиц» санкционировал создание и ведение такого реестра. Этим указом функции создания и ведения реестра были возложены на МВД на основе Единой государственной автоматизированной паспортной системы (ЕГАПС), концепция которой была утверждена постановлением правительства еще в 1997 году. Для выполнения работ по созданию ЕДАПС МВД определила частную компанию — корпорацию «ЕДАПС». Таким образом, персональные данные, которые граждане Украины передавали государственному органу, затем передавались частной структуре. Позднее уже другое

руководство МВД передало частной структуре также вопросы выдачи бланков для паспортов, базу ГАИ и т. д.

В Украине существует еще целый ряд нарушений права приватности, характерный пример — история с идентификационными номерами, выдающимися Государственной налоговой администрацией. Этот номер — действительно эффективный инструмент, с помощью которого осуществляется сбор и обработка данных о гражданах Украины. Сфера его использования постоянно расширяется и выходит далеко за рамки той цели, с которой он был создан по закону — налогового учета. При отсутствии идентифика-

ционного кода невозможно легальное трудоустройство, доступ к пенсионному обеспечению, реализация права на образование, получение дипломов об образовании, оформление субсидий и т. д. То есть, фактически, сложилась административная практика сознательного нарушения законодательства Украины о запрете использования налогового номера для иных целей.

Этот и многочисленные другие примеры обусловили необходимость появления законодательного акта, посвященного проблематике приватности, защиты персональных данных, его срочного утверждения, даже при наличии некоторых

ТЕЛЕКОМ-ИНФО

Примеры противоречий в законе

В заявлениях правозащитников подчеркивается наличие многочисленных противоречий и казусов в принятом законе. Приведем некоторые из них. Справедливой кажется мысль о том, что придется регистрировать как базу собственную визитницу. Действительно, приведенное в законе определение термина «база персональных данных» вполне относится к визитнице. Это же, кстати, относится и к списку жильцов многоквартирного дома, вывешенного в подъезде. Закон может уничтожить историческую науку в Украине. Например, в соответствии с частью 9 статьи 6 Закона «использование персональных данных в исторических, статистических или научных целях может осуществляться только в обезличенном виде». То есть в учебниках истории записи должны выглядеть примерно так: «Персона А. провела переговоры с персоной Б.», «Флаг над рейхстагом подняли персоны I, II и III». В научных работах нельзя делать ссылки на других коллег, даже при наличии их письменного согласия. Кроме того, Закон позволяет правоохранительным органам производить сбор и обработку информации о расовом и этническом происхождении, религиозных убеждениях личности. Такая практика, в соответствии с Рекомендациями Совета Европы, является проявлением дискриминации и должна быть запрещена. Еще один пример касается школьных журналов, в которых ведется учет посещения и успеваемости учеников. Школьные журналы теперь также считаются базами персональных данных, поэтому родители не могут ознакомиться с отметками ребенка без его письменного согласия. Кроме того, администрация школы должна регистрировать все журналы, внесение изменений в них. Вызывает удивление и необходимость оповещать орган власти «о каждом изменении сведений, необходимых для регистрации соответствующей базы», которая среди прочего включает информацию обо всех распорядителях (пользователях) такой базы данных.

недоработок. В результате в этом году 24 июня Президент Украины подписал Закон Украины № 2297-VI «О защите персональных данных», принятый Верховной Радой Украины 1 июня 2010 года. Данный закон призван регулировать отношения, связанные с защитой персональных данных во время их обработки и вступает в силу с января 2011 года.

Последние изменения законодательного акта подобного типа также были внесены и в федеральное законодательство России 1 июля 2010 года (Федеральный закон РФ № 152-ФЗ «О персональных данных» был принят 27 июля 2006 года). Российский закон вступил в силу 1 января 2007 года (необходимая защита должна была быть обеспечена так называемыми операторами персональных данных, которые до 01.01.2010 года должны были привести свои информационные системы в соответствие с оговоренными в законе требованиями). Уполномоченными федеральными органами в России, регулирующими деятельность в сфере обработки персональных данных, являются:

✓ Россвязькомнадзор (Федеральная служба по надзору в сфере связи и массовых коммуникаций) — осуществляет контроль и надзор за соответствием обработки персональных данных требованиям законодательства.

✓ ФСТЭК России (Федеральная служба по техническому и экспортно-

му контролю) — устанавливает методы и способы защиты информации в информационных системах в пределах своих полномочий.

✓ ФСБ РФ (Федеральная служба безопасности РФ) — устанавливает методы и способы защиты информации в информационных системах в пределах своих полномочий (регулирует сферу использования криптографических средств защиты информации).

В украинском законодательстве определено, что уполномоченный государственный орган по вопросам защиты персональных данных — это центральный орган исполнительной власти, который создается в соответствии с законодательством (но какой именно, до сих пор неизвестно).

Сегодня перед многими компаниями, деятельность которых связана с оказанием услуг отдельным гражданам на договорной основе (безусловно, к таким относятся сети интернет-магазинов, интернет-провайдеры, веб-службы, операторы сотовой связи и т. д.), остро встали вопросы не только о защите персональных данных клиентов, но и о самой возможности сбора, хранения, обработки и использования таких данных. И самый первый вопрос из этого списка состоит в том, какая же информация может быть отнесена к персональным данным? Обратимся к Закону Украины № 2297-VI (Статья 2): «персональные

данные — ведомости или совокупность ведомостей о физическом лице, которое идентифицировано или может быть идентифицированным». Совокупность таких данных — это база персональных данных: «база персональных данных — именованная совокупность упорядоченных персональных данных в электронной форме и/или в форме картотек персональных данных».

Подобными общими словами дано определение и в российском законе (статья 3 Федерального закона РФ № 152-ФЗ): «персональные данные — любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация».

Понятие «база персональных данных» в российском законе не определено, зато есть определение информационной системы персональных данных: «информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств».

Таким образом определение персональных данных в Законе Украины № 2297-VI является более широким, чем в ст. 23 Закона «Об информации», и позволяет считать персональными данными практически любую информацию о физическом лице. Можно сделать вывод, что персональными данными и в Украине, и в России, является ФИО в сопровождении любых других идентификационных данных, например, адреса, телефона или образовательного статуса.

Для выяснения, какое же отношение имеет физическое лицо или компания к защите персональных данных, большое значение имеет определение субъектов отношений, связанных с персональными данными (статья 4 Закона Украины № 2297-VI):

«Субъектами отношений, связанными с персональными данными, являются:

- ✓ субъект персональных данных;
- ✓ владелец базы персональных данных;
- ✓ распорядитель базы персональных данных;

ТЕЛЕКОМ-ИНФО

Что делать?

Представляется необходимым:

- ✓ срочно утвердить государственный орган, ответственный за вопросы защиты персональных данных;
- ✓ продлить срок ввода в действие Закона Украины № 2297-VI (для перестройки и адаптации в России, например, не хватило четырех лет);
- ✓ обеспечить действительно уведомительный характер владельцев и распорядителей баз персональных данных;
- ✓ ввести категоричность персональных данных и определить условия использования данных из различных категорий;
- ✓ ввести понятие «публичной личности» и отдельно определить условия защиты персональных данных для этой категории граждан;
- ✓ в явном виде обозначить связь Закона Украины № 2297-VI с правом на приватность, уважением частной жизни граждан;
- ✓ в любом виде категорически запретить сбор и обработку информации о расовом, этническом происхождении и религиозных убеждениях людей;
- ✓ уточнить условия защиты персональных данных умерших людей, исторических личностей и т. п.;
- ✓ определить условия использования и защиты биометрических данных, ввести их категоричность;
- ✓ четко обозначить понятие «персональный номер», использование которого не предусмотрено законодательством;
- ✓ различные идентификационные номера (базы данных различных органов власти) должны использоваться отдельно, не допустимо создание единого кода для накопления всей информации о личности, в частности, номера должны использоваться только для тех целей, для которых они были созданы.

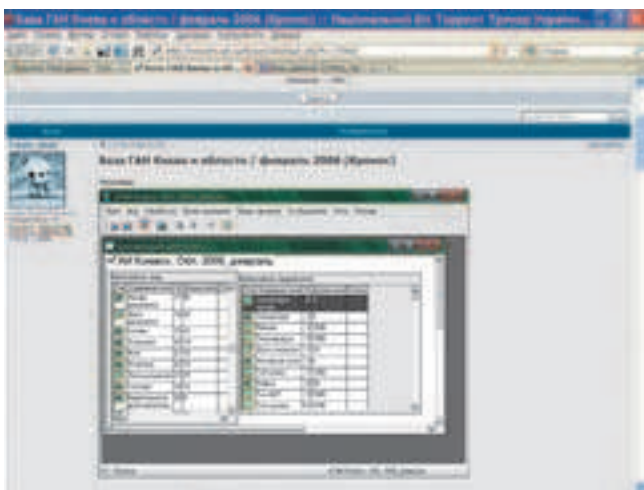


Рис. 3. В свободном (платном) доступе база данных ГАИ Киева и области

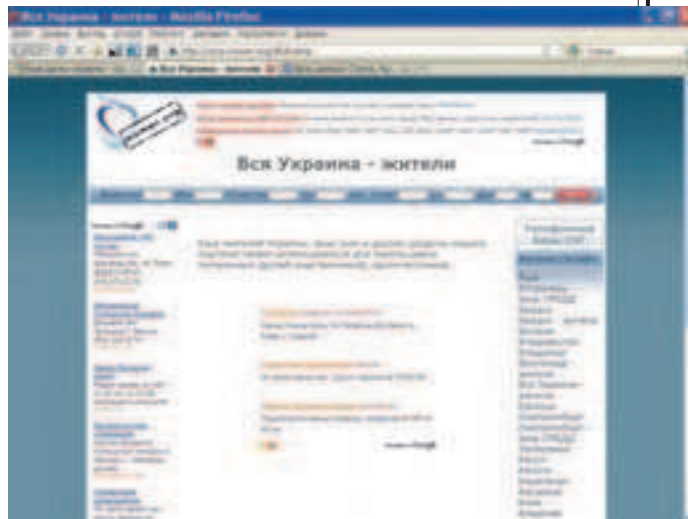


Рис. 4. Все жители Украины как на ладони

- ✓ третье лицо;
- ✓ уполномоченный государственный орган по вопросам защиты персональных данных;
- ✓ другие органы государственной власти и органы местного самоуправления, к полномочиям которых относится осуществление защиты персональных данных».

В России введен новый специальный субъект — «оператор». По-видимому он соответствует одновременно «владельцам» и «распорядителям» из украинского Закона. В настоящее время в российском реестре операторов, осуществляющих обработку персональных данных <http://www.pd.rsoc.ru/operators-registration/notify/>, содержатся сведения о 142 041 операторах персональных данных (по состоянию на 01.11.2010 года).

Как в российском, так и в украинском законодательстве предусмотрен уведомительный характер обработки персональных данных. Владелец или распорядитель (оператор) до начала обработки персональных данных обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных. Затем данные о владельцах или распорядителях (операторах) вносятся в специальный реестр операторов. Информация, содержащаяся в реестре, становится общедоступной.

Вместе с тем бытующее мнение о том, что нет необходимости регистрироваться как владелец или распространитель персональных данных, является ошибочным. Таким образом многие компании пытаются оправдать свое бездействие в области обеспечения безопасности персональных данных. Однако если компания не предпринимает никаких

усилий по защите персональных данных, это однозначно расценивается как невыполнение требований законодательства. Кроме того, при регистрации возможен отказ со стороны государственного органа, то есть смысл уведомительного характера регистрации явно нарушен.

Требования Закона Украины распространяются на все государственные и коммерческие организации, обрабатывающие в своих информационных системах персональные данные физических лиц (сотрудников, клиентов, партнеров и т. п.), независимо от размера и формы собственности. Практически каждая организация имеет отдел кадров с картотекой сотрудников, то есть является владельцем и распространителем персональных данных. Закон касается большинства населения как участников процесса «обработки» данных. А так как субъектом персональных данных является каждый человек, то Закон носит всеобщий характер и касается каждого.

Следует обратить внимание на то, что в соответствии со статьей 5 Закона Украины, объектом защиты являются только персональные данные во время их обработки в базах персональных данных. Казалось бы это сужает действие Закона, однако обратимся к трактованию понятия «обработка данных».

В соответствии с российским законом, «обработка персональных данных — действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных».

Похожее определение и в Законе Украины: «обработка персональных

данных — любое действие или совокупность действий, осуществленных полностью или частично в информационной (автоматизированной) системе и/или в картотеках персональных данных, которые связаны со сбором, регистрацией, накоплением, хранением, адаптацией, изменением, обновлением, использованием и распространением (распространением, реализацией, передачей), обезличиванием, уничтожением сведений о физической персоне».

Вспомним общепринятые определения, одно из которых можно найти в экономико-математическом словаре Лопатникова: «обработка данных [data processing, information processing] — процесс приведения данных к виду, удобному для использования. Независимо от вида информации, которая должна быть получена, и типа оборудования любая система обработки данных выполняет три основные группы операций: подбор исходных, входных данных (сбор данных), собственно их обработку (в процессе которой система оперирует промежуточными данными), получение и анализ результатов, то есть выходных данных».

Приведенные же в законах определения являются слишком общими, и соответственно, охватывают все процедуры манипуляции с данными, что, с одной стороны, противоречит общепринятому определению, а с другой, — практически снимает все ограничения к применению вышеуказанных законов. ●

Дмитрий ЛАНДЭ,
Заместитель директора ИЦ «ЭЛВИСТИ»

Продолжение статьи
см. на CD, а также
на ресурсе www.ht.ua

