ПРАВОВОЕ РЕГУЛИРОВАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В ЗАКОНОДАТЕЛЬСТВЕ ЗАРУБЕЖНЫХ ГОСУДАРСТВ

В.П. Иванский

Кафедра административного и финансового права
Российский университет дружбы народов
ул. Миклухо-Маклая, 6, Москва, Россия, 117198

В статье рассматриваются законодательные акты о защите персональных данных Австрии, Дании, Великобритании, Исландии, Франции и Финляндии в части изучения законодательного опыта в определении понятий «персональные данные» и их классификации.

Ключевые слова: персональные данные; матрикула; неприкосновенность сферы частной жизни; компьютерные и телекоммуникационные технологии.

I. *Актуальные теоретические аспекты защиты персональных данных в России и за рубежом*

Актуальность данной статьи заключается в том, что правовая защита информационного аспекта сферы частной жизни человека в последние десятилетия в эпоху развития информационных технологий приняло глобальный и всеохватывающий характер (1). И эта проблема захватила не только Россию, где, казалось, правовой опыт регулирования персональных данных намного меньше, чем в индустриально развитых странах, но и страны ЕС. С одной стороны, благодаря бурному развитию компьютерных и телекоммуникационных технологий обмен информацией в мире стал более легким и более быстрым, а с другой, такое развитие привело к формированию принципиально новых факторов, таящих угрозы для права граждан на невмешательство в частную жизнь:

– впервые появившейся возможности хранить и обрабатывать информацию, используемую для управления государством и бизнесом, не в обезличенной, а в *персонифицированной* форме;

– скрытному (в восприятии человека) характеру накопления, хранения, обработки и передачи информации в компьютерах;

– появлению особо опасных информационных объектов со сверхвысокой концентрацией персонифицированной информации (базы и банки данных, пространственно-распределенные информационные системы).

Такой лавинный рост потоков информации представляет собой и серьезный вызов в отношении права людей на частный характер персональных данных. Вопросы защиты данных, в том числе их трансграничное измерение, затрагивают людей повседневно — на работе, в контактах с государственными органами, при приобретении товаров или услуг, а также в поездках или при по-

сещении страниц в Интернете. Поэтому неслучайно в конце июля 2011 г. Президент Российской Федерации Д.А. Медведев подписал новый закон о внесении существенных изменений в ныне действующий Федеральный закон «О персональных данных» № 152-ФЗ от 27 июля 2006 г.

До подписания указанного Федерального закона Президентом РФ Государственной Думе Федерального Собрания потребовалось около двух лет, чтобы подготовить эти изменения в закон № 152 «О персональных данных».

Документ определяет случаи обработки персональных данных, а также сроки предоставления оператором информации по запросу гражданина.

Кроме того, эти изменения внесли конкретику в определения таких понятий, как «персональные данные», «оператор», «обработка персональных данных», а также расширили перечень случаев, когда допускается обработка персональных данных.

Отметим, что закон № 152 был принят еще в 2006 г., но из-за многочисленных отсрочек все его положения вступили в силу только с 1 июля 2011 г. Полное вступление в силу закона № 152 неоднократно откладывалось в связи с тем, что вовремя не были подготовлены соответствующие подзаконные акты, а операторы персональных данных были не готовы к выполнению новых требований [7].

Сегодня также Совет Европы и Европейская комиссия объединяют усилия в обеспечении основного права человека — права на защиту информации о гражданах.

Так, Евросоюз намерен модернизировать законодательство в области защиты персональных данных, чтобы обеспечить право граждан входящих в его состав государств на сохранение тайны частной информации. В первую очередь Еврокомиссия намерена проконтролировать деятельность социальных сетей, например, Facebook, который в одностороннем порядке поменял автоматические настройки приватности, не предупредив об этом пользователей. Еврокомиссар по вопросам юстиции Вивиан Рединг (Viviane Reding) в своей речи перед европарламентариями о реформе законодательства упомянула такое образное выражение, как «право быть забытым». В итоге многие пользователи не догадываются, что выложенная ими на сайте личная информация становится общедоступной, причем практически навсегда [3].

В. Рединг предлагает законодательно обязать подобные сайты ввести так называемое правило «приватность по умолчанию». То есть пользователи социальных сетей и других подобных сайтов должны давать явно выраженное согласие на опубликование своих персональных данных. А практика, когда такие данные становятся публичными «по умолчанию», то есть если пользователь не выберет «приватный режим» в настройках, должна быть признана незаконной. «Для установления настроек приватности иногда требуется значительное усилие пользователя»,— считает еврокомиссар. По ее мнению, само по себе наличие этих настроек не является достаточным показателем согласия пользователя на опубликование персональных данных. Правило «приватность по умолча-

нию» также предполагает запрет передачи персональных данных пользователей различным приложениям, доступным в социальных сетях.

В. Рединг также предлагает распространить законы ЕС на все ресурсы, которыми пользуются граждане ЕС, независимо от места их регистрации. Таким образом, нововведения могут затронуть и сервисы компании Google.

«Право быть забытым» касается также некоторых информационных ресурсов, архивы которых доступны в сети. Если европейские законодатели поддержат предложение Рединг, граждане ЕС смогут потребовать удалить из таких архивов свои фотографии и интервью, которые были сделаны много лет назад,— даже если в прошлом они дали согласие на интервью в газете или появление в телесюжете.

28 января 2011 г. отмечалось 30-летие Конвенции Совета Европы о защите физических лиц в отношении автоматизированной обработки данных личного характера (Конвенция № 108). В Страсбурге во время зимней сессии Парламентской ассамблеи Совета Европы Вивиан Рединг заявила, что "эффективная защита данных имеет жизненно важное значение для наших демократий и лежит в основе других основных прав и свобод. Нам необходимо установить равновесие между заботой о частной жизни и свободным потоком информации, которая помогает создать новые экономические возможности. Именно эти вопросы я хотела бы рассмотреть в наших предложениях по модернизации правил защиты данных ЕС в 2011 г.» [9].

II. *Актуальные практические аспекты правовой защиты персональных данных в России и за рубежом*

В практике европейских судов уже немало судебных решений по защите персональных данных. Так, например, испанский суд в одном из недавних решений постановил убрать информацию о человеке из поисковой выдачи Google.

Истец — доктор Гуидитто Руссо — был раскритикован в одной из статей испанской газеты El Pais еще в 1991 г. (речь шла о разногласиях между врачом и его пациентом, которые были вскоре устранены), однако до сих пор при вводе в Google его имени все равно одним из первых появляется этот негативный материал. Руссо указывал, что из-за Google его материальное благосостояние ухудшается, и в своем иске просил убрать ссылку на порочащую его статью из поисковой выдачи. При этом к газете El Pais, на сайте которой размещена заметка, таких требований не выдвигалось, поскольку периодические издания попадают под действие закона о свободе самовыражения средств массовой информации [3]. Возможно, с принятием нового европейского законодательства эта ситуация изменится.

Такие же актуальные проблемы по защите информации приватного характера граждан имеют место в США, Германии и других странах. Южнокорейское подразделение компании Apple уже выплатило первую компенсацию пользователю iPhone за несанкционированный сбор данных о его местоположении. Размер компенсации, которая выплачена юристу Ким Хен-суку Apple Korea,

составил $946, сообщается со ссылкой на должностных лиц районного суда Чханвона.

В последнее время давление на Apple по вопросу несанкционированного сбора и хранения данных о местонахождении пользователей неуклонно возрастало.

Вопрос приобрел остроту после того, как обнаружилось, что устройства, выпущенные компанией, в течение нескольких месяцев сохраняют незакодированную информацию о пользователях. Смартфоны с ОС Google Android также, как выяснилось, регулярно передают вовне данные о местонахождении пользователя.

Рассмотрением дела о незаконном сборе информации мобильными устройствами с операционными системами Google и Apple занялся и Сенат США. В ходе заседания представителям компаний пришлось ответить на ряд вопросов, касающихся используемых ими технологий. Ранее парламентский комитет, в ведении которого находится вопрос о защите персональных данных граждан, уже разослал письма шести разработчикам ОС для мобильных устройств, в том числе Apple и Google, с требованием предоставить больше информации об отслеживании информации о пользователях. Компании пояснили, что геоданные собираются на анонимной основе.

В мае 2011 г. Apple представила обновление для программного обеспечения, позволяющее пользователям самостоятельно контролировать сбор данных о местонахождении.

Американские правозащитники, специализирующиеся на вопросах защиты частной жизни граждан, предъявили претензии к корпорации Apple, производящей iPad и iPhone— устройства, которые сохраняют информацию о перемещениях их владельцев. По утверждению правозащитников, данные, сохраненные устройствами, не зашифрованы и фактически находятся в свободном доступе. «Собирание, хранение и использование данных о перемещениях пользователей без их разрешения неприемлемо. Это нарушает действующее в стране законодательство», — заявляют правозащитники [11; 12].

Еврокомиссия требует также и от Германии принять новый закон о резервном сохранении персональных данных. В противном случае Германии грозит расследование в связи с нарушением европейских соглашений [8; 10].

В 2011 г. Союз потребителей России подал в суд на девять интернет-магазинов и сервис продажи железнодорожных билетов Railwayticket.ru за разглашение ими персональных данных клиентов и в отношении «Мегафона». По мнению Союза потребителей, интернет-магазины совершили сразу три нарушения: они нарушили права клиентов на неприкосновенность частной жизни, на конфиденциальность персональных данных и на качество товаров и услуг. Роскомнадзор в ходе проверки отправленных с сайта «Мегафона» сообщений установил более 80 интернет-магазинов, информация о покупателях которых попала в открытый доступ в Сети [1; 13].

III. *Опыт правовой регламентации понятия «персональные данные» в законах стран Западной Европы*

Вышеуказанные актуальнейшие теоретические и практические проблемы защиты персональной информации определили интерес исследователя обратиться к законодательному опыту зарубежных государств в регламентировании понятий «персональные данные» и классификации их видов, так как именно последние являются основным объектом посягательств на неприкосновенность сферы частной жизни [5. С. 117–211].

В странах, находящихся на этапе компьютерного информационного общества или в фазе перехода к такому обществу, основным объектом посягательств на сферу частной жизни стала персонифицированная информация, обрабатываемая автоматизированными электронными средствами (компьютерными и телекоммуникационно-компьютерными информационными системами). Такую информацию стали называть «персональными данными». Термином «машинные данные», или просто «данные», в большинстве стран обозначают информацию, полученную в результате обработки на ЭВМ или подготовленную в специальной форме для такой обработки. Причины же специального выделения категории «персональных данных» из общего понятия «данные» связаны с тем, что такие данные являются потенциально уязвимыми атрибутами сферы частной жизни человека.

Довольно быстро было обнаружено, что персонифицированную информацию в компьютерах можно условно разделить на две категории:

– *«нейтральные»* персонифицированные данные, к раскрытию и распространению которых субъект данных относится индифирентно;

– *«чувствительные»* персонифицированные данные, циркуляцию которых субъект данных стремится ограничить. Именно эта категория получила название «*персональных данных*» и была квалифицирована как информация, несанкционированный доступ или ненадлежащее использование которой приводит к посягательствам на права частной жизни субъекта данных.

Таким образом, персональные данные определяются по критерию *«чувствительности».*

Так как понятие «чувствительности» персональной информации достаточно субъективно и зависит от восприятия субъекта данных, то на базе многих прецедентов в гражданском судопроизводстве стран общего права был выработан следующий принцип: публикация некоего факта частной жизни (персональных данных) признавалась посягательством на сферу частной жизни, если было доказано, «что публикация этого факта была высоко предосудительной с точки зрения любого благоразумного человека, наделенного обычной чувствительностью» [18. P. 53]. Смысл этого судебного критерия в том, «что закон не предназначен для защиты сверхчувствительных людей, поскольку каждый человек должен до некого обоснованного предела открывать свою жизнь для пристального внимания общества».

С точки зрения критерия «чувствительности», определение оксфордского правоведа Раймонда Уэкса представляется многим исследователям каноническим: «*Персональная информация* могла бы определяться как те факты, сообщения или мнения, которые связаны с данным индивидом и относительно которых можно было бы ожидать, что он считает их интимными или конфиденциальными и, следовательно, желает остановить или, по крайней мере, ограничить их циркуляцию» [22. P. 31].

В национальных законах о защите данных в определении понятия «персональные данные» не применяется критерий «чувствительности», но он используется при делении персональных данных на *«обычные»* и *«чувствительные»* (или «особо чувствительные») в других статьях этих же законов. Это связано с большим разнообразием персональных данных, используемых в компьютерных информационных системах, с одной стороны, и относительной субъективностью критерия «чувствительности», с другой стороны. В самих же определениях понятия «персональные данные» используется, как правило, другой критерий — *критерий «идентифицируемости субъекта данных»* на основании этих данных.

Классический пример использования этого критерия дает определение из Австрийского закона 1978 г. в его новой редакции Закона 2000 г. о защите данных:

«*Данные* — информация, хранимая на носителе данных и имеющая отношение к некому идентифицированному или имеющему высокую вероятность идентификации субъекту данных (персональные данные)» [16].

Датские законодательные акты 1979 г. о регистрах публичных органов власти и о частных регистрах в их новой редакции Закона об обработке персональных данных 2000 г. определяют понятие «персональные данные» следующим образом:

«Для целей настоящего законодательного акта слова «*персональные данные*» должны пониматься как обозначение данных, которые могут быть отнесены к идентифицируемым индивидуумам, даже если такое отнесение предполагает знание персонального регистрационного номера или любых подобных специальных средств идентификации такого индивидуума» [17].

Значительно более сложным и интересным является британское определение персональных данных. Законодательный акт 1984 г. в его новой редакции Закона 1998 г. о защите данных вводит в нормативное определение дополнительные категории «мнение» и «намерение»:

«Статья 1(3). Термин «*персональные данные*» означает данные, состоящие из информации, связанной с неким живым индивидом, который может быть идентифицирован на основании этой информации (или с помощью этой и иной информации, находящейся в распоряжении пользователя данных), включая любое выражение мнения о данном лице, но без какого-либо указания о намерениях пользователя данных в отношении этого лица» [21].

Таким образом, любое выражение *мнения* об индивиде (субъекте данных) включается в состав персональных данных, тогда как любое указание на *намерения* пользователя данных в отношении субъекта данных однозначно исключается из состава персональных данных (необходимо подчеркнуть, что намерения третьей стороны, поскольку они в явной и недвусмысленной форме не исключены законом, включаются в состав персональных данных).

Другой важной особенностью британского определения является оговорка «или с помощью этой и иной информации, находящейся в распоряжении пользователя данных». Поскольку Великобритания разрабатывала свой закон о защите персональных данных почти на десятилетие позже других стран — участниц Конвенции 108 Совета Европы [6], то легислатура Соединенного Королевства имела возможность учесть опыт применения аналогичных зарубежных законов. Приведенная выше оговорка призвана предупредить распространенную среди пользователей данных уловку: чтобы данные не подпадали под юрисдикцию законодательства о защите персональных данных, они хранят их в компьютере в псевдообезличенной форме — без упоминания идентифицирующих сведений о субъекте данных, но с привязкой к идентификационным кодам. Таблица же соответствия кодов и субъектов данных хранится (в ручной форме или на магнитных носителях) отдельно и при необходимости обеспечивает идентификацию субъектов данных этой якобы обезличенной компьютерной информации.

Исландский законодательный акт 1989 г. о регистрации и обращении с персональными данными в его новой редакции Закона о защите конфиденциальности 2000 г. распространяет понятие «*персональные данные*» и на сведения о юридических лицах (т.е. признает так называемое «корпоративное право на невмешательство в частную сферу»): «...к персональным данным относятся данные, связанные с частными, финансовыми или иными делами индивидов, институтов, компаний или иных юридических лиц, которые эти лица обоснованно должны держать в секрете» [15].

Определение из Французского закона 1978 г. об обработке данных, файлах данных и индивидуальных свободах подчеркивает, что правовое регулирование обработки персональных данных распространяется как на публичный, так и на частный сектора: «Статья 4. ...*персональные данные* — это данные, которые позволяют в любой форме, прямо или косвенно, установить личность физического лица, в отношении которого эти данные собраны, независимо от того, физическим или юридическим лицом эти данные были обработаны» [14; 19].

Особо следует отметить тщательную проработку определений персональных данных и смежных с ними понятий в Финском законодательном акте 1988 г. о персональных данных и его новой редакции Закона о персональных данных 1999 г.:

«1. Термин *«персональные данные*» означает любое описание любого физического лица или характеристик физического лица или жизненных обстоятельств, которое может быть признано как описывающее определенное частное

физическое лицо или его семью или тех, кто живет с ним в одном и том же жилище;

Термин «*файл персональных данных*» означает любой набор данных, содержащий персональные данные, обработанные при помощи компьютера, а также любой перечень, картотеку или иной набор данных, содержащий персональные данные и организованный соответствующим образом, благодаря которому данные о любом конкретном физическом лице могут быть найдены легко и без чрезмерных затрат;

2а. Термин «*файл редакционных данных*» означает любой файл персональных данных, предназначенный единственно для редакторских операций любого члена редакции средства массовой информации и недоступный для посторонних...

Термин «*персональные кредитные данные*» означает персональные данные, предназначенные для использования в оценке финансового статуса физического лица, его способности соответствовать своим обязательствам или степени оказываемого ему кредитного доверия...

7а. Термин «*матрикула*» означает любой файл персональных данных, предназначенный для публикации, в который физические лица входят в соединение со сведениями о конкретной профессии или образовании, членстве в некой профессиональной организации или ином обществе, со своим статусом или достижениями в области культуры, спорта, экономической жизни или иной гражданской деятельности или в соединении с другими сопоставимыми факторами» [20].

Этот законодательный акт относится к так называемым «законам второго поколения», учитывает опыт применения предыдущих отечественных и зарубежных законов и содержит ряд принципиально новых моментов. Пункт 1 распространяет понятие «персональные данные» на сведения о семье субъекта данных и о тех, «кто живет с ним в одном и том же жилище».

Пункт 2 выводит понятие «персональные данные» за пределы чисто компьютерной информации, распространяя его на данные в информационных системах иных технологий (ручных, механических и т.д.).

Принципиальной новинкой являются нормативные определения «отраслевых» персональных данных в п. 2а, 6 и 7а (для кредитной отрасли и для средств массовой информации).

Особенно важным представляется появление в законе нормативных определений терминов «файл редакционных данных» и «матрикула», поскольку после внедрения компьютерных технологий в повседневную работу печатной и электронной прессы обработка персональных данных в средствах массовой информации стала объектом правового регулирования одновременно со стороны деликтных средств правовой защиты сферы частной жизни от посягательств в форме несанкционированных публикаций или публичной огласки, сформировавшихся в «докомпьютерную эпоху», и со стороны международных актов [2] и национальных законодательств по защите персональных данных.

Проработка в законе таких нормативных определений способствует тому, чтобы взаимоотношения деликтного и международно-национального законодательства по защите персональных данных в этой точке соприкосновения сфер их правового регулирования были не конкурентными, а взаимно дополняющими.

Возвращаясь к критерию «чувствительности», отметим, что он используется в зарубежном законодательстве для отнесения некоторых видов персональных данных к категориям данных, требующим при обработке повышенных мер защиты или вообще запрещенным для обработки. При этом национальный закон о защите персональных данных либо содержит прямое указание на отнесение данных к определенной категории, либо наделяет представителей государственной власти (как правило, министра, курирующего национальный орган по защите данных, иногда премьер-министра) полномочиями принятия оперативных решений по данному вопросу.

Как показало исследование зарубежных законов о защите данных в странах, несмотря на некоторые исключения большинство стран делит персональные данные по критерию «чувствительности» на *три категории*:

– «*обычные*» персональные данные — их сбор, обработка, использование и передача — возможны без специального разрешения, в режиме, предписанном национальными законами;

– «*чувствительные*» персональные данные — их сбор, обработка, использование и передача — требуют особых мер защиты и безопасности, специально установленных законом;

– «*особо чувствительные*» персональные данные — их сбор, обработка, использование и передача — либо вообще запрещены законом либо разрешены только в исключительных случаях с использованием специальных мер защиты и безопасности.

Общепризнанными видами «чувствительных» персональных данных являются данные об арестах; банковские данные; данные кредитных отчетов и кредитных историй; данные об образовании и трудовой деятельности (как правило, только данные, содержащие оценку способностей и трудовых качеств индивида); медицинские данные; налоговые данные.

Набор «особо чувствительных» персональных данных, подлежащих особо тщательной защите, может варьироваться в различных странах в зависимости от национального менталитета, но, как правило, к этой категории относятся данные о расовом и этническом происхождении, религиозных верованиях, политических убеждениях, членстве в профессиональных ассоциациях, политических и общественных организациях, состоянии здоровья, особенностях сексуального поведения, криминальном прошлом (данные о вынесенных и исполненных обвинительных судебных приговорах по уголовным делам).

В качестве примера, иллюстрирующего механизм применения критерия «чувствительности», приведем краткое описание его применения в бельгийской национальной системе защиты персональных данных.

В Бельгии контролер (держатель) файлов должен соблюдать особо строгие правила обработки и использования в отношении трех категорий персональных данных: 1) «*высокочувствительных»* данных; 2) *медицинских* данных; 3) *судебных* данных (категории 2 и 3 считаются просто «чувствительными» данными).

Что касается первой категории, то Бельгийский законодательный акт 1992 г. о защите данных (BDPA) [23] предоставляет наивысшую степень защиты данным, связанным с расой, этническим происхождением, сексуальным поведением, политическими взглядами или действиями, религиозными или философскими убеждениями, членством в любом профессиональном или трудовом союзе или принадлежностью к государственной службе здравоохранения (все они далее называются «высокочувствительными данными»).

Любой контролер файлов может обрабатывать эту категорию высокочувствительных данных только для целей, разрешенных BDPA, или во исполнение этого законодательного акта.

Поскольку сам BDPA не предусматривает никаких разрешенных целей для обработки высокочувствительных данных, то эти цели в деталях устанавливаются Королевскими указами № 6 и 7, конкретизирующими и регламентирующими исполнение вышеуказанного законодательного акта. BDPA допускает исключения для юридических лиц и организаций де-факто (таких, как профсоюзы, службы здоровья, политические партии), но только в отношении данных, связанных с их собственными членами.

В отношении *второй категории* следует отметить, что контролер файлов может обрабатывать медицинские данные только после получения заранее письменного разрешения субъекта данных или, в качестве альтернативы, под строгим надзором и при ответственности лечащего врача. В категорию медицинских включаются все данные, раскрывающие информацию, связанную с предыдущим, текущим или будущим состоянием физического или умственного здоровья субъекта данных, за исключением данных явно административного или оценочного характера, относящихся к ходу лечения и медобслуживания. Медицинские данные не могут передаваться третьим сторонам, за исключением тех случаев, когда это делается во исполнение закона или когда закон содержит явно выраженное и недвусмысленное разрешение на такую передачу. Медицинские данные также могут передаваться другим лечащим медработникам после получения заранее специального письменного разрешения от заинтересованного лица (субъекта данных) или для целей медицинской обработки в чрезвычайных ситуациях и в случаях опасности (ст. 7 BDPA).

Отнесенные к *третьей категории* криминальные и судебные персональные данные могут обрабатываться только во исполнение закона или для целей, определенных законом, причем в эту категорию включается и обработка данных об уголовных обвинительных приговорах и наказаниях из документов, хранимых в национальных криминальных архивах, а также обработка данных из криминальных документальных записей, хранимых муниципалитетами (ст. 8 § 4), обработка таких данных адвокатами (ст. 8 § 6) и юридическими лицами,

уполномоченными на то королевским указом, — во всех этих случаях обработчик данных обязан заранее посылать субъекту данных уведомление о предстоящей обработке относящихся к нему криминальных данных.

И наконец, Бельгийский законодательный акт 1992 г. о защите данных в явно выраженной и недвусмысленной форме запрещает любому контролеру файлов сбор любых высокочувствительных, медицинских, криминальных или судебных данных в Бельгии для передачи через границу с целью обработки на иностранной территории по той причине, что их обработка в Бельгии также запрещена (ст. 4 § 2).

Таким образом, в последние годы вопросы защиты частной жизни и персональных данных в связи с экспоненциальными темпами развития информационных технологий требуют объединения финансовых и интеллектуальных ресурсов ЕС и России по внесению радикальных изменений:

– во-первых, начать консультации членам Совета Европы по обновлению содержания Конвенции № 108 для повышения уровня стандартов защиты данных, а значит сферы частной жизни, не только в Европе, но и во всем мире. Ибо обмен персональными данными — это также часть обеспечения безопасного и стабильного общества;

– во-вторых, своевременно, с развитием компьютерных и телекоммуникационных технологий, вносить в национальное законодательство стран ЕС и России изменения в части использования персональных данных, обеспечивающих людей товарами и услугами, особенно в среде Интернет — от банковских операций и путешествий до социальных сетей. Особого пристального внимания законодателей заслуживает правовая защита приватности сферы частной жизни в социальных сетях, где информация личного характера либо предается огласке без согласия человека, либо является недостоверной из-за несвоевременной ее актуализации и ошибок.

ПРИМЕЧАНИЯ

(1) В англосаксонской правовой семье право на защиту частной жизни, неприкосновенность сферы частной жизни именуется «The law of privacy» или «privacy». «Прайвеси» (privacy) — это биопсихическая по своему происхождению и социокультурная по характеру своего развития формула защищенности особой, интимной сферы частной жизни человека, сферы формирования и существования личности индивида как устойчивой системы социально-значимых черт, характеризующих индивида как члена общества или общности.

По совокупности выполняемых им социальных функций «прайвеси» следует определить как специфический социальный механизм, который общество вырабатывает, чтобы способствовать целенаправленной (т.е. социально релевантной, а не хаотической или антисоциальной) психической адаптации личности к окружающим социальным условиям и, в конечном итоге, обеспечить полноценную интеграцию индивида в данное общество, не нанося вреда индивидуальности человека.

Центральной социальной функцией этого механизма является защита «социальной маски» индивида, т.е. того «информационного образа», который индивид демонстрирует социальному контролю (наблюдению) со стороны окружающих.

«Прайвеси» как *правовой (юридический) институт* в узком смысле этого понятия вводится в орбиту системы прав человека в форме «права на неприкосновенность частной жизни» (right to privacy) и получает позитивное закрепление в законодательстве. В рамках формирующегося *правового* института «прайвеси», особое место занимает «подсистема» правовой защиты сферы частной жизни в связи с использованием информационных технологий, поскольку именно она служит правовым обеспечением центральной социальной функции «прайвеси» — функции защиты «информационного образа» («социальной маски») индивида [4. С. 1–34].

ЛИТЕРАТУРА

[1] В Москве подан иск к 10 интернет-сервисам, допустившим утечку персональных данных покупателей. URL: http://www.pravo.ru/news/view/58425.

[2] Директива 95/46/ЕС Европейского парламента и Совета Европейского Союза о защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных 1995 г. URL: http://pd.rsoc.ru/docs/up_organe.pdf.

[3] Евросоюз защитит право граждан «быть забытыми» в век Интернета. URL: http://www.pravo.ru/interpravo/practice/view/52669.

[4] *Иванский В.П.* Правовая защита информации о частной жизни граждан (опыт современного правового регулирования). — М., 2000.

[5] *Иванский В.П.* Правовая защита сферы частной жизни в США: теория и практика. — М., 2010.

[6] Конвенция Совета Европы о защите физических лиц в отношении автоматизированной обработки данных личного характера от 28 января 1981 г. URL: http://webwarper.net/ru/conventions.coe.int/Treaty/RUS/Treaties/Html/108.htm.

[7] Медведев смягчил закон «О персональных данных». URL: http://www.pravo.ru/news/view/58100.

[8] Немецкие правозащитники подали иск к Facebook. URL: http://www.pravo.ru/ /story/58611/43331.

[9] Новости в Совете Европы // Вестник Европы. — 2011. — № 30. URL: http://magazines.russ.ru/vestnik/2011/30/no10.html.

[10] От Германии требуют собирать больше информации о гражданах. URL: http://www.pravo.ru/interpravo/news/view/52424.

[11] Правозащитники заявляют, что устройства Apple «шпионят» за пользователями. URL: http://www.pravo.ru/interpravo/news/view/52792.

[12] Apple выплатила первую компенсацию по иску о слежке за пользователями iPhone. URL: http://www.pravo.ru/story/view/57486

[13] «Яндекс» и «Мегафон» представили новые доказательства вины друг друга в утечке смс-переписки. URL: http://www.pravo.ru/news/view/57740.

[14] Act on Data Processing, Data Files and Individual Liberties (1978, France). URL: http://pd.rsoc.ru/docs/up_organe.pdf.

[15] Art.1 of Act Concerning the Registration and Handling of Personal Data (1989, Iceland) and Lög um persónuvernd og meðferð persónuupplýsinga (2000). URL: http://pd.rsoc.ru/ /docs/up_organe.pdf.

[16] Austrian Data Protection Act (1978) and Datenschutzgesetz (2000). URL: http://pd.rsoc.ru/ /docs/up_organe.pdf.

[17] Denmark Private Registers Act (1979) and Public Authorities Registers Act (1979) and Lov om behandling af personoplysninger (2000). URL: http://pd.rsoc.ru/docs/up_organe.pdf.
[18] Freedman W. Right of Privacy in Age of Computer. — L. — L., N.Y., 1986.
[19] Loi relative à l'informatique, aux fichiers et aux libertés (1978). URL: http://pd.rsoc.ru/ /docs/up_organe.pdf.
[20] Personal Data File Act (1988, Finland) and Henkilötietolain taustaa (1999). URL: http://pd.rsoc.ru/docs/up_organe.pdf.
[21] UK Data Protection Act 1984 (Data Protection Act 1998). URL: http://pd.rsoc.ru/ /docs/up_organe.pdf.
[22] Wakes R. Protection of Privacy. — L.; Sweet & Maxwell, 1980. — (Mod. legal studies).
[23] Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens. URL: http://cwisdb.kuleuven.be/pisa/nl/ juridisch/privacywet.htm#Privacywet.

THE LEGAL REGULATION OF THE PERSONAL DATA IN THE FOREIGN COUNTRIES

V.P. Ivanskiy

The Department of Administrative and Financial Law
Peoples' Friendship University of Russia
6, Miklukho-Maklaya st., Moscow, Russia, 117198

The article addresses legislation on data protection in Austria, Denmark, The United Kingdom, Iceland, France and Finland regarding studying of legislative experience in the definition of «personal data» concept and their classification.

Key words: personal data and their types; matrikula; integrity in private life, computer and telecommunication technologies.