УДК 342.7 + 347:004
ББК Х400.323 + Х400.7

В. М. Кафтанникова

ПРОБЛЕМЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

V. M. Kaftannikova

PROBLEMS OF PERSONAL DATA LEGAL REGULATION IN STATE INFORMATION SYSTEMS

Статья представляет собой обзор нормативных правовых актов, которые контролируют деятельность в сферах персональных данных и информационных систем, и анализ последних нововведений законодательстве в сфере защиты персональных данных. В обзор входят нормативные акты Российской Федерации и зарубежные нормативные акты. Автор рассматривает требования к персональным данным в информационных системах. Проводится анализ действующего законодательства и совместимости различных нормативных актов, регулирующих деятельность в сфере защиты персональных данных.

На основании анализа делается вывод о том, что в текущем законодательстве присутствуют некоторые недочеты, но, в общем, прослеживается положительная тенденция в сфере защиты персональных данных в государственных информационных системах.

Ключевые слова: *информационные системы, персональные данные, государственные информационные системы.*

The article is a review of legal acts, which control activities in the fields of personal data and information systems, and analysis of the latest innovations in the legislation in personal data protection. The review includes the regulations of the Russian Federation and foreign regulations. The author examines the requirements for personal data in information systems. There is analysis of the current legislation and the compatibility of the different regulations governing activities in the field of personal data protection.

Conclusion is based on the analysis and contains the fact that the current legislation there are some flaws, but overall, there is a positive trend in the field of protection of personal data in public information systems.

Keywords: *information systems, personal data, state information systems.*

Возникновение информационных систем персональных данных можно приурочить к моменту возникновения информационных систем, т. е. ко времени появления электронно-вычислительных машин. Основную роль в истории защиты персональных данных сыграла Конвенция Совета Европы от 28 января 1981 года «О защите личности в связи с автоматической обработкой персональных данных» (ратифицирована Федеральным законом от 19 декабря 2005 г. № 160-ФЗ) (далее — Конвенция)[1]. В Конвенции еще не дано определение информационным системам персональных данных (далее — ИСПДн), но можно выделить составляющие ИСПДн: «автоматизированная база данных» и «автоматическая обработка». ИСПДн предполагает под собой любой набор данных, с которым осуществляются следующие операции, если они полностью или частично осуществляются с применением автоматизированных средств: накопление данных, проведение логических или/и арифметических операций с такими данными, их изменение, стирание, восстановление или распространение. Согласно Конвенции, персональные данные в информационных системах должны отвечать следующим требованиям:

— должны быть получены и обработаны добросовестным и законным образом;

— должны накапливаться для точно определенных и законных целей и не ис-

пользоваться в противоречии с этими целями;

— должны быть адекватными, относящимися к делу и не быть избыточными применительно к целям, для которых они накапливаются;

— должны быть точными и в случае необходимости обновляться;

— должны храниться в такой форме, которая позволяет идентифицировать субъектов данных не дольше, чем этого требует цель, для которой эти данные накапливаются.

В 2001 году Российская Федерация подписала Конвенцию Совета Европы о защите физических лиц при автоматизированной обработке персональных данных. Необходимым шагом Российской Федерации как стороны Конвенции стало принятие Федерального закона № 152-ФЗ «О персональных данных»[2], целью которого является обеспечение 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. Следует отметить, что еще в 1997 году Указом Президента РФ № 188 были определены сведения конфиденциального характера[3], которые определены как перечень данных, относящихся к персональным (сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях и т. д.). В законе «О персональных данных» появляется определение термина: информационная система персональных данных — совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств. В Федеральном законе № 149 «Об информации, информационных технологиях и о защите информации»[4] появляется определение «государственные информационные системы» — федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов. В законе «О персональных данных» указываются принципы обработки персональных данных, которым должны следовать операторы (в случае с государственными системами оператором будет, в общем случае, являться государственный или муниципальный орган), причем можно отметить, что данные принципы копируют требования, представленные в Конвенции.

Согласно закону «О персональных данных», оператор должен принимать необходимые правовые, организационные и технические меры при обработке персональных данных в информационных системах или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении персональных данных.

Особенности обработки персональных данных в государственных или муниципальных ИСПДн выделены в отдельную статью закона, в которой указывается, что государственные органы, муниципальные органы создают в пределах своих полномочий, установленных в соответствии с федеральными законами, государственные или муниципальные информационные системы персональных данных. Федеральными законами могут быть установлены особенности учета персональных данных в государственных и муниципальных ИСПДн, в том числе использование различных способов обозначения принадлежности персональных данных, содержащихся в соответствующей государственной или муниципальной ИСПДн, конкретному субъекту персональных данных.

В рамках исследования законодательства в сфере регулирования оборота персональных данных в государственных информационных системах особый интерес представляет ст. 19 ФЗ «О персональных данных», п. 5 которой гласит, что «федеральные органы исполнительной власти… иные государственные органы в пределах своих полномочий принимают нормативные правовые акты, в которых определяют угрозы безопасности персональных данных, актуальные при обработке персональных данных в формационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки». Можно заметить, что данный пункт (а также предыдущие пункты ст. 19 ФЗ «О персональных данных») стал основополагающим для утверждения новых требований к защите персональных данных при их обработке в информационных системах персональных данных (далее — требования к защите персональных данных).

Одним из последних нововведений законодательства можно считать новое постановление Правительства № 1119, вступившее в силу 15 ноября 2012 г.[5], пришедшее на смену постановления Правительства Российской Федерации № 781 от 17 ноября 2007 г[6]. И в связи с этим сразу возникает вопрос о документах, которые создавались в соответствии с тем или иным пунктом постановлению № 781. Для многих специалистов в области защиты персональных данных открыто стоит вопрос о том, имеют ли силу данные документы, или они утратили ее с выходом в свет нового постановления Правительства РФ. Действительно, данная ситуация ввела в заблуждение работников, но, с юридической точки зрения, данные документы официально не утратили силу и должны применяться в части, не противоречащей новому акту.

Например, приказ ФСТЭК России от 05.02.2010 № 58 противоречит постановлению Правительства № 1119 в следующих пунктах: п. 1.4 полностью теряет смысл, поскольку ссылается на классификацию информационных систем; в пунктах 2.2, 2.11, 2.12, 3.1—3.4 упоминается класс информационных систем; классификация согласно Постановлению № 781 утратила силу; а также «методы и способы защиты информации от несанкционированного доступа в зависимости от класса ИС» — противоречит уже исходя из названия. Таким образом, документ, не потеряв своей юридической силы, потерял свойство полезности. Общественность ждет новых нормативно-правовых актов, которые придут на смену таким документам с отсутствием конкретики.

В рамках данного вопроса необходимо рассмотреть и соответствие нового постановления ФЗ «О персональных данных», а именно п. 3 ст. 19, который гласит о том, что «Правительство Российской Федерации с учетом возможного вреда субъекту персональных данных, объема и содержания обрабатываемых персональных данных, вида деятельности, при осуществлении которого обрабатываются персональные данные, актуальности угроз безопасности персональных данных устанавливает уровни защищенности, требования к защите персональных данных при их обработке в ИСПДн, требования к материальным носителям...». Ознакомившись с постановлением № 1119, можно заметить, что основными критериями для обеспечения защиты являются объем персональных данных и их содержание; актуальность угроз; признак того, что сотрудник оператора или нет. Вред субъекту и вид деятельности оператора во внимание не принимается. Весьма актуальным, но не понятным со стороны непосредственного применения, явилось введение ряда дефиниций, в частности информационная система, обрабатывающая специальные категории персональных данных; информационная система, обрабатывающая биометрические персональные данные; информационная система, обрабатывающая общедоступные персональные данные; информационная система, обрабатывающая иные категории персональных данных; информационная система, обрабатывающая персональные данные сотрудников оператора.

Одним из главных нововведений постановления № 1119 является изменение принципа обеспечения соответствующего уровня защищенности персональных данных в зависимости от актуальных угроз, объема данных (убран критерий по численности в 1000 субъектов ПДн) и принадлежности данных к информационной системе персональных данных, обрабатывающих данные сотрудников оператора. Если сравнивать два постановления по требованиям к защите персональных данных и мероприятиям по обеспечению безопасности персональных данных, то можно заметить тенденцию к сокращению таких требований. Согласно новому постановлению, контроль за выполнением настоящих требований организуется и проводится оператором самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей не реже 1 раза в 3 года.

В постановлении № 781 устанавливалось, что безопасность персональных данных достигается путем исключения несанкционированного доступа. В постановлении № 1119 не говорится про мероприятия, касающиеся несанкционированного доступа, а в ст. 19 ФЗ «О персональных данных» обеспечение безопасности определяется уже совершенным действием, а именно «обнаружением фактов несанкционированного доступа к персональным данным и принятием мер». Кроме того, в постановлении № 1119 появились требования об автоматической регистрации в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе.

Также стоит заметить, что ст. 19 ФЗ «О персональных данных» в последней редакции содержит определение угроз

безопасности персональных данных при их обработке. В общем, многие требования остались прежними: методы и способы защиты информации в информационных системах устанавливаются ФСТЭК и ФСБ в пределах их полномочий; средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия. Безопасность персональных данных при их обработке в информационной системе обеспечивает оператор или лицо, которому на основании договора оператор периодически поручает обработку персональных данных; содержание электронного журнала обращений.

Конечно, большой резонанс вызвала отмена многих требований в сравнении с постановлением № 781. Прекратили действовать такие требования, как: защита речевой информации и информации, обрабатываемой техническими средствами, а также информации, представленной в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнитно-оптической и иной основе; порядок проведения классификации информационных систем устанавливается совместно ФСТЭК, ФСБ и Минкомсвязи; возможные каналы утечки информации при обработке персональных данных в информационных системах определяются ФСТЭК и ФСБ в пределах их полномочий; многие другие требования, связанные с конкретными действиями по защите безопасности информационных систем персональных данных, перестали быть актуальными. Вероятно, с одной стороны, можно увидеть в этом позитивную сторону, но, в противном случае, на сегодняшний день вся ответственность по защите лежит на операторе ПДн, кроме того отсутствует сама методология защиты данных.

Как отмечают специалисты по защите персональных данных, новый документ не привнес в их деятельность ничего нового и конкретного: «та же оценка соответствия, тот же непонятный электронный журнал, то же требование утверждения списка допущенных лиц, то же требование установление режима безопасности в помещениях, та же отсылка к нормативным документам ФСТЭК и ФСБ»[7].

Таким образом, можно сделать вывод, что постановление Правительства № 1119 вступит в полную силу при наличии соответствующих документов регуляторов в сфере персональных данных — ФСТЭК и ФСБ по поводу методики определения актуальных угроз безопасности для информационных систем персональных данных.

На данный момент действующими признано около 50 нормативно-правовых актов в сфере защиты персональных данных федерального уровня — постановления правительства, указы президента, федеральные законы. Несмотря на то что проверки регуляторами информационных систем на предмет защищенности в них персональных данных начались относительно недавно, нельзя не заметить общую тенденцию к усилению защиты ИСПДн и повышение уровня грамотности регуляторов и операторов в данной сфере.

Примечания

1. Конвенция Совета Европы от 28 января 1981 года «О защите личности в связи с автоматической обработкой персональных данных». Страсбург, 28 января 1981 г.
2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» // Российская газета. — 2006. — № 165.
3. Указ Президента № 188 от 1997 г. // Российская газета. — 1997. — 18 марта.
4. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Российская газета. — 2006. — № 165.
5. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // СЗ РФ. — 2012. — № 45. — Ст. 6257.
6. Постановление Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» // Российская газета. — 2007. — № 260.
7. *Лукацкий А.* Бизнес без опасности — URL: http://lukatsky.blogspot.ru/2012/11/781-1119.html (Дата обращения 13.05.2013).

References

1. Konvencija Soveta Evropy ot 28 janvarja 1981 goda «O zashhite lichnosti v svjazi s avtomaticheskoj obrabotkoj personal'nyh dannyh». Strassburg, 28 janvarja 1981 g.

2. Federal'nyj zakon ot 27 ijulja 2006 g. № 152-FZ «O personal'nyh dannyh» // Rossijskaja gazeta. — 2006. — № 165.
3. Ukaz Prezidenta № 188 ot 1997 g. // Rossijskaja gazeta. — 1997. — 18 marta.
4. Federal'nyj zakon ot 27 ijulja 2006 g. № 149-FZ «Ob informacii, informacionnyh tehnologijah i o zashhite informacii» // Rossijskaja gazeta. — 2006 g. — № 165/
5. Postanovlenie Pravitel'stva RF ot 01.11.2012 № 1119 «Ob utverzhdenii trebovanij k zashhite personal'nyh dannyh pri ih obrabotke v informacionnyh sistemah personal'nyh dannyh» // SZ RF. 2012. № 45. St. 6257.
6. Postanovlenie Pravitel'stva Rossijskoj Federacii ot 17 nojabrja 2007 g. № 781 «Ob utverzhdenii Polozhenija ob obespechenii bezopasnosti personal'nyh dannyh pri ih obrabotke v informacionnyh sistemah personal'nyh dannyh» // Rossijskaja gazeta. — 2007. — № 260.
7. *Lukackij A.* Biznes bez opasnosti. — URL: http://lukatsky.blogspot.ru/2012/11/781-1119.html (Data obrashhenija 13.05.2013).

КАФТАННИКОВА Влада Михайловна, аспирант кафедры конституционного и административного права, Южно-Уральский государственный университет. 454080, Челябинск, пр. Ленина, 76. E-mail: ladalk@gmail.com

KAFTANNIKOVA Vlada Mikhailovna, graduate student of Constitutional and Administrative Law Department, South Ural State University. Bld. 76, Lenina Ave., Chelyabinsk, 454080. ladalk@gmail.com