РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА
И ГОСУДАРСТВЕННОЙ СЛУЖБЫ
ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

М. Ю. Брауде-Золотарёв, Е. С. Сербина
В. С. Негородов, И. Г. Волошкин

Персональные данные в государственных информационных ресурсах

| ИЗДАТЕЛЬСКИЙ ДОМ ДЕЛО |
МОСКВА | 2016

УДК 342
ББК 67.400.7
Б87

Б87 **Брауде-Золотарёв, М. Ю., Сербина, Е. С., Негородов, В. С., Волошкин, И. Г.**
Персональные данные в государственных информационных ресурсах / М.Ю. Брауде-Золотарёв, Е.С. Сербина, В.С. Негородов, И.Г. Волошкин. М. : Издательский дом «Дело» РАНХиГС, 2016. — 56 с. — (Научные доклады: государство и право).

ISBN 978-5-7749-1121-9

В распоряжении органов государственной власти и органов местного самоуправления находится значительный объем информации о гражданах Российской Федерации, поэтому обработка персональных данных в публичном секторе – одна из наиболее важных областей информационного регулирования. Некоторые нормативно-правовые акты в этой сфере устарели, в том числе в связи с новыми рисками, связанными с расширяющимся применением в государственном секторе России современных информационно-коммуникационных технологий. При внесении изменений в правовые акты, регулирующие обработку персональных данных, необходимо учитывать обширный зарубежный опыт и международные обязательства России по защите персональных данных.

ISBN 978-5-7749- 1121-9

УДК 342
ББК 67.400.7

Оглавление

Обозначения, определения и сокращения

Базовый регистр — Базовый регистр информации, необходимой для предоставления государственных услуг в городе Москве, созданный Распоряжением Правительства Москвы № 376-РП.

ГРН — Государственный регистр населения.

Директива 95/46/ЕС — Директива 95/46/ЕС от 24 октября 1995 г. «О защите физических лиц в отношении обработки персональных данных и о свободном движении таких данных».

ЕС — Европейский союз.

ЖКХ — Жилищно-коммунальное хозяйство.

Закон о персональных данных, Федеральный закон № 152-ФЗ — Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Конфиденциальность — недопустимость распространения персональных данных операторами их обработки без согласия их носителя.

«Конвенция о защите персональных данных» — Конвенция Совета Европы о защите физических лиц в отношении автоматизированной обработки данных личного характера от 1981 г. № 108.

Обезличивание персональных данных — действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

РФ — Российская Федерация.

ОГИР ЗАГС-ПВС-ЖКХ — система объединенных государственных информационных ресурсов ЗАГС, паспортно-визовых служб и паспортных столов жилищно-эксплуатационных контор.

Трансграничная передача персональных данных — передача персональных данных оператором через государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

Федеральный закон № 24-ФЗ — Федеральный закон от 20 февраля 1995 г. № 24-ФЗ «Об информации, информатизации и защите информации».

Федеральный закон № 149-ФЗ — Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Федеральный закон № 210-ФЗ — Федеральный закон от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг».

Федеральный закон № 242 — Федеральный закон № 242 от 21 июля 2014 года «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях».

ФСБ — Федеральная служба безопасности.

ФСТЭК — Федеральная служба по техническому и экспортному контролю.

NIST — National Institute of Standards and Technology.

SSN — Social Security number.

USB — Universal Serial Bus.

1. Анализ действующего правового регулирования персональных данных в Российской Федерации и других странах

Основной российский закон в области защиты персональных данных — Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» — был принят достаточно давно, и практика его применения выявила ряд недостатков.

Во-первых, закон содержит ряд крайне сложных в реализации требований, что создает необоснованные барьеры в работе операторов персональных данных и толкает их на нарушения закона. В то же время для граждан избыточное регулирование закона в большей степени порождает неудобства, нежели действительно обеспечивает безопасность их персональных данных.

Во-вторых, часть положений закона в настоящее время устарели или потеряли актуальность, а некоторые появившиеся за 8 лет аспекты работы с персональными данными он не регулирует вовсе, в частности Федеральный закон № 152-ФЗ «О персональных данных» не учитывает современного уровня развития интернета и замедляет развитие электронной коммерции и облачных сервисов в Российской Федерации.

1.1. Общие недостатки Федерального закона № 152-ФЗ

Одним из основных теоретических недостатков ФЗ «О персональных данных» является то, что он не называет четких критериев отнесения тех или иных сведений к категории персональных данных, а также не определяет механизмов их соотношения с иными видами информации ограниченного доступа, вследствие чего зачастую одни и те же данные могут быть отнесены к различным видам информации ограниченного доступа. Например, в режиме коммерческой тайны могут охраняться персональные данные контрагентов; в режиме профессиональной тайны охраняется информация персонального характера, характеризующая пользователей предоставляемых услуг (врачебная, нотариальная, адвокатская, банковская тайны и т.п.). При этом режимы охраны различных видов информации ограниченного доступа предполагают отличные друг от друга сроки сохранения конфиденциальности соответствующей информации, дополнительные гарантии прав субъекта, а также виды ответственности за их нарушение. Возможность составления закрытых перечней данных, относимых исключительно к тому или иному виду информации ограниченного доступа, является достаточно спорной. Однако минимизация разницы между степенью уязвимости прав субъекта соответствующих сведений, безусловно, остается необходимой. По нашему мнению, указанная проблема может быть решена путем реализации субъектом соответствующей информации своего права на установление режима, предусмотренного ФЗ «О персональных данных», в соответствии с которым будет установлен ограниченный доступ к ней со стороны третьих лиц, а также наложен ряд обязанностей на оператора, производящего ее обработку. Так, установление режима коммерческой тайны в отношении какой-либо информации (например, данных авторов изобретений, используемых предпринимателем для извлечения прибыли и, соответственно, представляющих для него коммерческую ценность) не исключает возможность получе-

ния правообладателем письменного разрешения указанных субъектов на обработку их персональных данных. Более того, в случае неправомерных действий в отношении персональных данных со стороны оператора (в данном случае правообладателя) они могут быть обжалованы субъектом в уполномоченный орган по защите прав субъектов персональных данных или в суд без нарушения установленного режима коммерческой тайны. Это возможно в силу ст. 6 Федерального закона от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне», предусматривающей обязанность правообладателя предоставлять соответствующую информацию органам государственной власти, иным государственным органам, а также органам местного самоуправления по их мотивированному требованию.

Остается открытым вопрос относительно статуса изображения гражданина — правомерно ли относить его к персональной информации, ведь именно изображение служит зачастую одним из основных идентификаторов личности. Так, например, по изображению человека можно получить информацию о его биометрических данных, национальности, религиозной принадлежности и др. В настоящее время статус изображения человека как объекта правовой охраны определяется в гражданско-правовом порядке (ст. 152.1 Гражданского кодекса РФ) и существенно отличается от принципов охраны персональных данных граждан, установленных Федеральным законом «О персональных данных». Оптимальным в данном случае было бы обращение к положениям Директивы 95/46/ЕС Европейского парламента и Совета Европейского союза от 24 октября 1995 г. «О защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных», рассматривающей видеоданные как персональные данные.

Существует немало противоречий между Федеральным законом № 152-ФЗ и другими нормативно-правовыми актами, регулирующими смежные с защитой персональных данных сферы, в том числе с актами международного уровня.

1.2. Противоречия между Федеральным законом № 152-ФЗ и нормами международного права

В отличие от Конвенции «О защите физических лиц при автоматизированной обработке персональных данных» 1981 г. и Директивы 95/46/ЕС, в Законе о персональных данных отсутствует ряд важных положений, касающихся защиты персональных данных.

Закон о персональных данных не относит к персональным данным с особым режимом защиты данные, относящиеся к административным правонарушениям, уголовным судимостям или мерам безопасности, национальному идентификационному номеру или другому общепринятому идентификатору, более того, идентификатор сведений о физическом лице вовсе не признается персональными данными. Закон о персональных данных не регулирует статус и режим обработки идентификатора сведений о физическом лице.

Директива 95/46/ЕС, в отличие от Закона о персональных данных, устанавливает требование к результату (например, критерии оптимального уровня защиты), который должен быть достигнут в результате принятия оператором персональных данных надлежащих мер по защите персональных данных.

Закон о персональных данных не устанавливает однозначных требований для всех операторов, направленных на обеспечение защиты персональных данных, для случаев, когда уведомление Роскомнадзора об обработке персональных данных не требуется.

В отличие от Директивы 95/46/ЕС и законодательств некоторых стран — членов ЕС, Закон о персональных данных не предусматривает проведение уполномоченным органом в области защиты персональных данных предварительных проверок в отношении случаев обработки персональных данных, создающих конкретные риски для прав и свобод субъектов данных.

В качестве примера можно рассмотреть распоряжение Правительства Москвы от 12 мая 2011 г. № 376-РП, которым утверждено положение о Базовом регистре информации, не-

обходимой для предоставления государственных услуг в городе Москве (далее — Базовый регистр). Данный регистр содержит большой объем сведений о жителях Москвы, являющихся персональными данными. Обработка персональных данных посредством их включения в Базовый регистр и обработки нарушает следующие положения Конвенции «О защите физических лиц при автоматизированной обработке персональных данных» ETS № 108:

– Требование сообщать субъектам персональных данных о включении их персональных данных, полученных от третьих лиц, в Базовый регистр нарушает право субъектов персональных данных, предусмотренное пунктом «a» ст. 8 Конвенции. Согласно пункту «a» ст. 8 Конвенции, любое лицо вправе знать о существовании автоматизированного файла данных личного характера, знать его основные цели, а также название и место обычного проживания или место делового обзаведения контролера файла.

  В нарушение этого принципа персональные данные получаются не у субъектов персональных данных, при этом сами субъекты персональных данных о включении их данных в Базовый регистр и об обработке их персональных данных в составе Регистра не уведомляются, им не сообщается предусмотренная Законом о персональных данных информация об обработке персональных данных.

– Принцип, согласно которому персональные данные, подвергающиеся автоматизированной обработке, собираются и обрабатываются на справедливой и законной основе (пункт «a» ст. 5).

  Персональные данные, которые включаются в Базовый реестр, изначально были предоставлены субъектами этих данных для других целей (как правило, для целей предоставления конкретной государственной или муниципальной услуги, а не для целей их бессрочного хранения в Базовом регистре в совокупности с большим количеством иных данных об этом

субъекте для неограниченного круга применений). Обработка персональных данных исключительно в целях, для которых они были предоставлены, является одной из составляющих принципа законности обработки персональных данных (пункт «а» ст. 5 Конвенции).

– Принцип, согласно которому персональные данные, подвергающиеся автоматизированной обработке, хранятся для определенных и законных целей и не используются иным образом, несовместимым с этими целями.

В случае Базового регистра также существует проблема в слишком широко сформулированном исключении из общего правила об обработке персональных данных (п. 4 ч. 1 ст. 6 Закона о персональных данных). Формально хранение персональных данных в Базовом регистре осуществляется для целей предоставления государственных услуг, т.е. для определенной законом цели.

Однако на самом деле для предоставления государственных услуг такое хранение не является необходимым. Более того, Федеральный закон № 210-ФЗ предусматривает единственный способ получения органами власти сведений, находящихся в распоряжении других органов власти — в порядке межведомственного взаимодействия, осуществляемого после поступления запроса на получение услуги от заявителя. Основные положения, касающиеся этого порядка, установлены тем же Федеральным законом № 210-ФЗ, а агрегирование персональных данных в едином информационном ресурсе (регистре, базе данных) данным законом не предусмотрено.

– Принцип, согласно которому персональные данные, подвергающиеся автоматизированной обработке, должны являться адекватными, относящимися к делу и не чрезмерными для целей их хранения.

Состав сведений Базового регистра является чрезмерным для целей предоставления каждой конкретной государственной или муниципальной услуги. Хранение всей совокупности сведений (в том числе персональ-

ных данных), необходимых для предоставления всех без исключения государственных услуг, является чрезмерным по отношению к цели предоставления каждой конкретной государственной услуги.

Рассмотренный пример можно считать характерным для публичного сектора, использующего расширенное, за пределами сформулированных Конвенцией принципов, толкование п. 4 ч. 1 ст. 6 Закона о персональных данных.

1.3. Противоречия между Федеральным законом № 152-ФЗ и Федеральным законом № 149-ФЗ

Имеет место некоторая несогласованность понятия «конфиденциальность информации» в Федеральном законе от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и понятия «конфиденциальность персональных данных» в Федеральном законе от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Так, в Федеральном законе № 149-ФЗ (ст. 2) конфиденциальность информации — это «обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя». В такой конструкции термин «передавать» подразумевает конкретного адресата, однако на практике его может не быть. Кроме того, согласие обладателя информации на передачу информации третьим лицам не может быть единственным для этого условием, так как законодательство Российской Федерации, прежде всего законодательство о безопасности и Федеральный закон «О персональных данных», предусматривают и иные законные основания в качестве исключения из общего правила (наличия согласия субъекта персональных данных)[1].

[1] *Волчинская Е.К.* Некоторые правовые проблемы применения Федерального закона «О персональных данных» // Персональные данные. 2009. № 2.

Ст. 7 Федерального закона «О персональных данных» содержит более точное определение, относящееся к конфиденциальной информации — конфиденциальности персональных данных: «Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом».

1.4. Противоречия между Федеральным законом № 152-ФЗ и Федеральным законом № 210-ФЗ

В соответствии с ч. 3 ст. 7 Федерального закона № 210-ФЗ, в случае если для предоставления государственной или муниципальной услуги необходима обработка персональных данных лица, не являющегося заявителем, и если в соответствии с Законом о персональных данных такая обработка может осуществляться с согласия указанного лица, при обращении за получением государственной или муниципальной услуги заявитель дополнительно представляет документы, подтверждающие получение согласия указанного лица или его законного представителя на обработку персональных данных указанного лица.

Данное положение вносит неопределенность. В соответствии с п. 4 ч. 1 ст. 6 Федерального закона «О персональных данных» персональные данные могут обрабатываться без согласия субъекта персональных данных, если такая обработка необходима для исполнения полномочий государственных и муниципальных органов, а также функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг. При этом закон не конкретизирует, касается ли данное положение только случая, когда государственная или муниципальная услуга предоставляется самому субъекту персональных данных или третьему лицу. Следовательно, можно сделать вывод, что п. 4 ч. 1 ст. 6 Закона о персональных данных позволяет обрабатывать персональные данные без согласия субъекта персональных дан-

ных, если такая обработка необходима для предоставления государственной или муниципальной услуги кому бы то ни было.

Ч. 4 ст. 7 Федерального закона № 210-ФЗ предусматривает, что получение согласия заявителя как субъекта персональных данных не требуется для обработки органами, предоставляющими государственные услуги, органами, предоставляющими муниципальные услуги, иными государственными органами, органами местного самоуправления, подведомственными государственным органам или органам местного самоуправления организациями, участвующими в предоставлении предусмотренных государственных и муниципальных услуг, персональных данных в целях предоставления персональных данных заявителя, имеющихся в распоряжении таких органов или организаций, в орган, предоставляющий государственную услугу, орган, предоставляющий муниципальную услугу, либо подведомственную государственному органу или органу местного самоуправления организацию, участвующую в предоставлении государственных и муниципальных услуг, либо многофункциональный центр на основании межведомственных запросов таких органов или организаций для предоставления государственной или муниципальной услуги по запросу заявителя.

По сути данная норма частично конкретизирует норму п. 4 ч. 1 ст. 6 Закона о персональных данных. Если указанная норма Закона о персональных данных говорит, что получение согласия на обработку персональных данных не требуется, если такая обработка необходима для обеспечения предоставления государственных или муниципальных услуг, то положение ч. 4 ст. 7 Федерального закона № 210-ФЗ касается лишь одного частного механизма, обеспечивающего предоставление государственных или муниципальных услуг — обмена персональными данными в порядке межведомственного и межуровневого взаимодействия.

Следует отметить, что ч. 4 ст. 7 Федерального закона № 210-ФЗ, регулируя порядок обработки персональных данных при их передаче в порядке межведомственного взаимодействия, не затрагивает вопроса об обработке персональных

данных при формировании и ведении базовых государственных информационных ресурсов, которые предназначены для использования при осуществлении межведомственного информационного взаимодействия в целях предоставления государственных и муниципальных услуг (п. 1 Требований к порядку формирования, актуализации и использования базовых государственных информационных ресурсов, утверждены постановлением Правительства Российской Федерации от 14 сентября 2012 г. № 928).

Поскольку Закон о персональных данных и Федеральный закон № 210-ФЗ имеют одинаковую юридическую силу, то ч. 4 ст. 7 Федерального закона № 210-ФЗ не изменяет и не отменяет общую норму п. 4 ч. 1 ст. 6 Закона о персональных данных. Следовательно, указанные две нормы действуют параллельно. Таким образом, поскольку формирование и ведение базовых государственных информационных ресурсов необходимо для осуществления межведомственного взаимодействия и предоставления государственных и муниципальных услуг, то обработка персональных данных при их формировании и ведении в силу п. 4 ч. 1 ст. 6 Закона о персональных данных может осуществляться без согласия субъекта персональных данных.

Также необходимо обратить внимание, что, например, из ч. 2 ст. 7.1 Федерального закона № 210-ФЗ следует, что направление межведомственного запроса и представление документов и информации по межведомственным запросам допускаются только в целях, связанных с предоставлением государственных или муниципальных услуг и (или) ведением базовых государственных информационных ресурсов в целях предоставления государственных или муниципальных услуг.

Однако при планировании и реализации мероприятий по организации межведомственного и межуровневого взаимодействия (в том числе при использовании системы межведомственного электронного взаимодействия[1]) данное требование закона было учтено не полностью. Система меж-

[1] Постановление Правительства РФ от 28.11.2011 № 697 «О единой системе межведомственного электронного взаимодействия».

ведомственного электронного взаимодействия не в полной мере позволяет при получении межведомственного запроса установить наличие права у субъекта, запрашивающего данные, на получение запрашиваемой информации, а также необходимость получения данной информации для предоставления государственной или муниципальной услуги. При этом реализованные на практике взаимодействия отличаются от тех, что были спроектированы и утверждены согласно действующим правовым актам (с использованием «технологических карт межведомственного взаимодействия» — ТКМВ и соответствующей государственной информационной системы «Проектирование ТКМВ»). Также не осуществляется должный учет сведений о фактически направленных и исполненных запросов, на основании которых можно было бы установить, были запросы целевыми и законными или нет.

Подробнее рассмотренные вопросы анализируются в следующем разделе.

2. Риски и уязвимости обработки персональных данных в публичном секторе в Российской Федерации

2.1. Обзор существующих рисков и уязвимостей защиты персональных данных граждан при их обработке в публичном секторе в Российской Федерации

2.1.1. Передача персональных данных граждан в публичном секторе без получения их согласия и уведомления

Порядок обработки персональных данных физических лиц регулируется довольно сложным сводом правил. Законом предусмотрены случаи, когда получение согласия физического лица не требуется. В таких случаях операторы должны подтвердить наличие у них оснований для обработки данных. При этом в отдельных случаях получение письменного согласия все-таки требуется. Одна из сложностей заключается в том, что в публичном секторе государственные и муниципальные органы осуществляют передачу персональных данных без согласия и уведомле-

ния субъектов персональных данных, обосновывая это необходимостью предоставления государственных или муниципальных услуг (п. 4 ч. 1 ст. 6 Закона о персональных данных).

В сфере предоставления государственных и муниципальных услуг одним из примеров ситуации, когда оператор обрабатывает персональные данные, полученные не от самого субъекта персональных данных, является получение персональных данных в рамках электронного межведомственного взаимодействия. Это как раз случай, когда действует исключение из правила об уведомлении субъекта персональных данных, поскольку в рамках электронного межведомственного взаимодействия оператор получает персональные данные на основании Федерального закона № 210-ФЗ (ст. 7).

Между тем, как было отмечено выше, функционирующая в данный момент система межведомственного электронного взаимодействия не позволяет в полной мере проконтролировать целевой характер запросов персональных данных, обрабатываемых посредством этой системы. Это может означать, что в системе межведомственного электронного взаимодействия наряду с законными, могут также обрабатываться и незаконные запросы. И хотя ответственность за такую обработку в силу закона возложена на соответствующих операторов персональных данных, механизмов выявления нарушений и их пресечения в российском законодательстве и практике не предусмотрено.

При этом незаконные запросы, согласно букве п. 2 ч. 4 ст. 18 Закона о персональных данных, не подпадают под исключение из обязанности уведомления субъекта персональных данных об обработке его персональных данных, полученных у третьего лица. Однако, поскольку выявление факта незаконности запроса технически и организационно затруднено, фактически система межведомственного электронного взаимодействия позволяет в нарушение обязанности по уведомлению обрабатывать персональные данные, полученные не у самого субъекта персональных данных.

В контексте передачи персональных данных граждан при предоставлении государственных и муниципальных услуг без получения их согласия и уведомления отличается колли-

зионностью правового регулирования обработка персональных данных третьих лиц.

Например, при предоставлении государственных и муниципальных услуг, в частности услуг в сфере социальной защиты населения (выплаты пособий и компенсаций, предоставление дополнительных прав и др.), у заявителя возникает необходимость представлять в орган государственной власти или орган местного самоуправления, предоставляющий услугу (далее — уполномоченный орган), сведения о семье, в том числе имена членов семьи, даты их рождения, сведения о доходах, обучении, работе и другие сведения. При этом во взаимодействии заявителя и уполномоченного органа члены семьи заявителя выступают в качестве третьих лиц.

В соответствии со ст. 3 Федерального закона № 152-ФЗ, персональными данными лица является «любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)». Таким образом, возникает необходимость представления в уполномоченный орган персональных данных третьих лиц. Особенно актуальным это становится при переводе услуги в электронную форму, расширении дистанционных форм взаимодействия заявителя с уполномоченным органом и использовании межведомственных информационных запросов для получения сведений, необходимых для предоставления услуги и находящихся в распоряжении иных органов государственной власти и органов местного самоуправления, поскольку уполномоченный орган в этом случае самостоятельно получает персональные данные третьих лиц при предоставлении услуги заявителю. Применительно к указанным услугам источником необходимых сведений являются органы записи актов гражданского состояния.

Проблема обработки персональных данных третьих лиц при осуществлении межведомственных запросов при предоставлении государственных и муниципальных услуг в настоящее время однозначным образом не решена, и можно говорить о правовой коллизии между Федеральным законом № 210-ФЗ и Федеральным законом № 152-ФЗ. Как было указано в разделе 1, Федеральный закон № 210-ФЗ в ч. 3 ст. 7

устанавливает, что «в случае если для предоставления государственной или муниципальной услуги необходима обработка персональных данных лица, не являющегося заявителем… заявитель дополнительно представляет документы, подтверждающие получение согласия указанного лица или его законного представителя на обработку персональных данных указанного лица». Следовательно, для получения по межведомственным запросам сведений о членах семьи заявителя, уполномоченному органу необходимо предварительно удостовериться в наличии письменного согласия (на бумажном носителе или в электронной форме) этих лиц на обработку их персональных данных.

Однако Федеральный закон № 152-ФЗ хотя и устанавливает согласие субъекта персональных данных на обработку его персональных данных в качестве базового условия для начала такой обработки, в ч. 8 ст. 9 определяет, что «персональные данные могут быть получены оператором от лица, не являющегося субъектом персональных данных, при условии предоставления оператору подтверждения наличия оснований…», что предполагает возможность обработки персональных данных лица без получения его согласия, в случае если обработка персональных данных осуществляется по одному из оснований, предусмотренных, в частности, ч. 1 ст. 6 Федерального закона № 152-ФЗ.

Пункт 4 ч. 1 указанной статьи содержит следующее основание: «Обработка персональных данных необходима для исполнения полномочий федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг, предусмотренных Федеральным законом от 27 июля 2010 г. № 210-ФЗ “Об организации предоставления государственных и муниципальных услуг”, включая регистрацию субъекта персональных данных на Едином портале государственных и муниципальных услуг и (или) региональных порталах государственных и муниципальных услуг».

При разрешении данной коллизии необходимо учитывать приоритет специального законодательства при разрешении конфликтов норм права и, соответственно, определить, какой из указанных законов осуществляет общее, а какой — специальное регулирование применительно к коллизии, возникающей при межведомственном запросе персональных данных третьих лиц при предоставлении государственной услуги. Представляется, что более правильным будет рассматривать в качестве специального законодательства именно Федеральный закон № 210-ФЗ, поскольку он устанавливает регулирование одного из подмножества оснований для обработки персональных данных, общее регулирование которой, в свою очередь, осуществляется Федеральным законом № 152-ФЗ. В таком случае положения п. 4 ч. 1 относятся, прежде всего, к органам, осуществляющим обработку персональных данных (в форме их передачи) по запросам органов, предоставляющих услугу заявителю, но не распространяется на третьих лиц, не являющихся субъектом предоставления услуги.

Дополнительным аргументом за данный подход является ч. 5 ст. 9 Федерального закона № 152-ФЗ, которая устанавливает, что «порядок получения в форме электронного документа согласия субъекта персональных данных на обработку его персональных данных в целях предоставления государственных и муниципальных услуг, а также услуг, которые являются необходимыми и обязательными для предоставления государственных и муниципальных услуг, устанавливается Правительством Российской Федерации», что можно рассматривать как необходимость получения согласия любого субъекта персональных данных на обработку его персональных данных в целях предоставления государственных или муниципальных услуг.

В настоящее время такой порядок Правительством Российской Федерации не установлен, однако п. 2 Критериев определения видов электронной подписи, использование которых допускается при обращении за предоставлением государственных и муниципальных услуг, утвержденный постановлением Правительства Российской Федерации от 25 июня 2012 г. № 634, устанавливает, что согласие третьих лиц

в электронной форме на обработку их персональных данных при предоставлении государственной услуги должно удостоверяться усиленной квалифицированной электронной подписью, в том числе и в случае подтверждения своего согласия непосредственно на Едином портале государственных и муниципальных услуг (функций) или на региональных порталах государственных и муниципальных услуг (далее — порталы услуг). Таким образом, получение от членов семьи заявителя согласия на обработку персональных данных в электронной форме возможно при условии использования усиленной квалифицированной электронной подписи.

2.1.2. Возможные риски введения ограничений Федеральным законом № 242-ФЗ

Главная заявленная задача Федерального закона № 242-ФЗ («О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях») — обеспечить безопасность персональных данных граждан России. Тем не менее данную задачу документ, исходя из анализа его содержания, выполняет лишь отчасти или не выполняет ее вовсе. Прежде всего, Федеральный закон лишь говорит, что оператор обязан обеспечить обработку персональных данных граждан России на территории России. Закон не содержит слов «только» или «исключительно» и не запрещает обрабатывать такие персональные данные на зарубежных серверах. Также документ не предписывает удалить уже находящуюся на них информацию.

Таким образом, провозглашенная защита персональных данных от иностранных спецслужб или иных угроз является весьма призрачной. Федеральный закон № 242-ФЗ говорит, по сути, только о создании обязательной «копии» сведений, которая должна располагаться на территории России. Указанное требование (как и любое иное увеличение числа мест хранения любых персональных данных или увеличение числа субъектов, имеющих к ним доступ) может лишь снизить интегральную защищенность персональных данных, поскольку

на практике увеличивает число «копий» и круг лиц, имеющих доступ к персональным данным россиян (в том числе за счет сотрудников специализированных служб, операторов связи и провайдеров дата-центров), до принятия закона хранившихся исключительно за границей.

Также следует учитывать, что предложенная Федеральным законом № 242-ФЗ норма на практике невыполнима для случаев массовой обработки персональных данных (например, для сервисов электронной почты или сервисов социального общения), поскольку в таких случаях технологически невозможно отделить персональные данные именно российских граждан от персональных данных иных лиц, что порождает формальные основания для претензий к большинству интернет-сервисов, имеющих зарубежное происхождение и некоторой части интернет-сервисов, имеющих российское происхождение. Указанные ограничения могут быть сняты только полным дублированием на серверах, расположенных на территории России, всех персональных данных таких сервисов.

Федеральный закон № 242-ФЗ влечет увеличение затрат на обработку персональных данных российских граждан иностранными компаниями, которым приходится арендовать серверы в России. Также затраты повышаются и у отечественных компаний, которые используют зарубежные хостинги, например, из-за низкой цены, качественного сервиса и предпочтительных условий ведения хозяйственной деятельности.

Важно отметить, что одним из аргументов для принятия Закона была ч. 1 ст. 24 Конституции РФ. В соответствии с ней сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются. Однако в Федеральном законе № 242-ФЗ говорится не о принципиальном согласии гражданина на обработку персональных данных (его и сейчас нужно получать в соответствии со ст. 9 Закона о персональных данных). Речь идет именно о месте обработки такой информации, а именно это обстоятельство в Федеральном законе № 242-ФЗ не затрагивается: предусмотренные законом нормы принуждают операторов обрабатывать персональные данные граждан России

на территории России без учета мнения самих субъектов персональных данных и ограничивают их права распоряжаться своими персональными данными по собственному усмотрению, как это предусмотрено Конституцией и международными обязательствами России. Согласно Конвенции ETS № 108 «О защите физических лиц при автоматизированной обработке персональных данных», которую ратифицировала Россия, присоединившиеся к ней страны не должны ограничивать движение персональных данных между их территориями.

Актуальным является вопрос о трансграничном характере интернета. Специфика Федерального закона № 242-ФЗ и некоторых других ранее принятых законов (например, «закона о блоггерах») такова, что он касается, в том числе, иностранных сервисов и иностранные компании, распространяя на них свою юрисдикцию. Такой подход отпугивает зарубежные компании, которые хотят вести бизнес в России, и в целом ведет к экономическим потерям как фирм, так и потребителей, защита которых декларируется при принятии такого рода законов.

2.2. Анализ рисков, связанных с идентификацией сведений о гражданах в публичном секторе в Российской Федерации

2.2.1. Создание объединенных государственных информационных ресурсов персональных данных граждан Российской Федерации, в том числе как источников сведений для идентификации граждан в иных государственных информационных ресурсах

28 ноября 2011 г. Правительством Российской Федерации было принято Постановление № 977 «О федеральной государственной информационной системе “Единая система идентификации и аутентификации в инфраструктуре,

обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме"».

В этом Постановлении федеральным органам власти и органам внебюджетных фондов предписывается, а органам власти субъектов Федерации и органам местного самоуправления рекомендуется использовать данную единую систему идентификации, аутентификации, авторизации и регистрации физических и юридических лиц. Единая система будет включать в себя разные регистры, в том числе «регистр физических лиц».

Система должна обеспечивать санкционированный доступ к информации, содержащейся в государственных, муниципальных и иных информационных системах, не только в целях предоставления государственных и муниципальных услуг, но и для формирования «базовых государственных информационных ресурсов», для «межведомственного электронного взаимодействия» и «в иных целях, предусмотренных федеральными законами, актами Президента Российской Федерации и актами Правительства Российской Федерации». «Прозрачно» взаимодействующие друг с другом информационные хранилища являются, по сути, консолидированной базой данных.

Распоряжением Правительства Российской Федерации от 9 июня 2005 г. № 748-р была одобрена «Концепция создания системы персонального учета населения Российской Федерации». В соответствии с Концепцией, система персонального учета населения (СПУН) представляет собой территориально распределенную информационную систему, функционирующую на федеральном, региональном и муниципальном уровнях и обеспечивающую взаимодействие автоматизированных систем учета органов государственной власти, местного самоуправления, государственных и муниципальных организаций в части сбора, хранения, передачи и использования персональных данных граждан.

Важнейшие компоненты СПУН:

– государственный регистр населения (ГРН);
– информационные системы органов власти разного уровня, осуществляющие учет населения;
– метабаза по данным взаимодействующих информационных систем;
– модули взаимодействия, устанавливаемые в соответствующих информационных системах и обеспечивающие информационный контакт с системой ГРН и с метабазой СПУН.

Создание государственного регистра населения представляется рискованным действием с точки зрения защиты персональных данных граждан. При создании любых регистров населения высок риск облегчения сбора, хранения и распространения персональных данных граждан в неправовых целях, создании возможностей для коррупции в среде органов государственной власти и местного самоуправления. Создание же государственного регистра населения и комплекса взаимосвязанных информационных систем, предназначенных для единообразного учета, хранения и передачи персональных данных граждан, повышает риски незаконного распространения большого массива имеющихся в распоряжении органов государственной власти и органов местного самоуправления персональных данных граждан.

Аналогичные риски несут в себе проекты правовых актов, касающиеся порядка обработки информации, в том числе персональных данных, в государственных информационных ресурсах, готовящиеся по некоторым поручениям Правительства Российской Федерации. Например, во исполнение распоряжения Правительства Российской Федерации от 10 мая 2014 г. № 793-р «Об утверждении Концепции методологии систематизации и кодирования информации, а также совершенствования и актуализации общероссийских классификаторов, реестров и информационных ресурсов» разработан проект постановления Правительства Российской Федерации «О порядке создания, ведения, изменения и применения отдельных информационных ресурсов». Среди его целей фигурирует «формирование

правовых, технологических и организационных основ» для «обмена и сопоставления данных, содержащихся в информационных ресурсах», «доступа государственных органов и иных заинтересованных лиц к полной, достоверной и актуальной информации, содержащейся в информационных ресурсах», «создание единой информационной среды... в Российской Федерации». В числе норм предусматривается обязанность органов, ведущих государственные информационные ресурсы, «для целей внесения... данных в... информационные ресурсы... представлять оператору Системы в автоматизированном режиме эталонные данные, их обновления», автоматическая «актуализация дублирующихся данных» между различными информационными ресурсами, а также различные механизмы автоматического анализа и сопоставления данных. Представляется, что как декларируемые цели, так и конкретные нормы упомянутого проекта не соответствуют цитированной ранее Конвенции «О защите физических лиц при автоматизированной обработке персональных данных» (например, ее принципу, что автоматизированная обработка персональных данных допускается для определенных и законных целей и что сами данные не должны использоваться несовместимым с этим принципом образом или быть чрезмерными для целей их хранения).

Под влиянием процессов перевода предоставления государственных и муниципальных услуг в электронную форму, а также организации межведомственного и межуровневого взаимодействия в электронной форме (создание «электронного правительства») в публичных органах сформировался технократический взгляд на обработку персональных данных. Необходимость обеспечивать должный уровень защиты персональных данных согласно букве и духу законодательства о защите персональных данных и международным обязательствам Российской Федерации уступает необходимости выполнения публичными органами текущих поручений, создания пользователям удобства и иным задачам, связанным с формированием в стране электронного правительства.

Вопрос целесообразности создания в России ГРН, а также иных систем, обеспечивающих автоматизацию консолида-

ции и обработки персональных данных, необходимо решать только после тщательного, всестороннего и публичного анализа порождаемых их созданием рисков нарушения прав граждан на защиту их персональных данных.

2.2.2. Введение в Российской Федерации универсальных идентификаторов сведений о гражданах в государственных информационных ресурсах

Действующее российское законодательство на данный момент не регулирует правовой статус идентификатора физического лица и сведений о физическом лице.

Согласно п. 7 ст. 8 Директивы 95/46/ЕС, государства — члены ЕС определяют условия, при которых может производиться обработка национального идентификационного номера или любого другого общепринятого идентификатора.

Тот факт, что Директива 95/46/ЕС в статье, посвященной обработке специальной категории персональных данных, предписывает странам — членам ЕС определить отдельные условия, при которых возможна обработка национального идентификационного номера или другого общепринятого идентификатора, указывает на то, что:

- идентификаторы сведений о физических лицах признаются персональными данными в соответствии с Директивой;
- идентификаторы сведений о физических лицах требуют особого, повышенного режима защиты при их обработке.

В свою очередь Закон РФ о персональных данных вообще не упоминает об идентификаторе в статье 10, посвященной защите специальных категорий персональных данных, и в целом не регулирует его статус и режим обработки.

Единственное косвенное упоминание об идентификаторе сведений о физических лицах присутствует в ст. 13 Закона о персональных данных, которая посвящена особенностям обработки персональных данных в государственных или

муниципальных информационных системах персональных данных. Указанная статья предусматривает, что федеральными законами могут быть установлены особенности учета персональных данных в государственных и муниципальных информационных системах персональных данных, в том числе использование «различных способов обозначения принадлежности персональных данных, содержащихся в соответствующей государственной или муниципальной информационной системе персональных данных, конкретному субъекту персональных данных».

Данная норма фактически предусматривает использование идентификаторов сведений о субъектах персональных данных в государственных и муниципальных системах персональных данных.

При этом за исключением общего указания в ч. 3 рассматриваемой статьи на то, что права и свободы человека и гражданина не могут быть ограничены по мотивам, связанным с использованием идентификатора при обработке персональных данных, Закон о персональных данных не устанавливает никаких правил обработки идентификатора.

Возможность введения в Российской Федерации универсального идентификатора сведений о физических лицах активно обсуждаемый вопрос и, представляется, для принятия взвешенного решения по данному вопросу необходимо, чтобы все участники обсуждений одинаково понимали сущность и назначение универсального идентификатора. Для того чтобы детальнее разобраться в правовом назначении идентификаторов сведений о физических лицах, рассмотрим особенности их введения, сложившиеся в мировой практике.

В мировой практике выделяются следующие подходы к введению идентификаторов:

– вводится единый универсальный идентификатор, который используется для установления личности при получении государственных услуг в электронном виде (Швеция, Бельгия);
– единый универсальный идентификатор не вводится целенаправленно, но таковым де-факто со временем ста-

новится один из отраслевых идентификаторов. Этот отраслевой идентификатор используется при получении услуг как публичного, так и гражданского сектора в электронном виде в большинстве сфер деятельности государства (США);

– единый универсальный идентификатор не вводится из соображений защиты прав и свобод граждан, в связи с этим принимаются законодательные меры, препятствующие использование какого-либо из отраслевых идентификаторов в качестве универсального. Для целей предоставления государственных услуг в электронном виде граждане идентифицируются посредством отраслевых идентификаторов (Великобритания, Австралия, Венгрия);
– единый универсальный идентификатор не вводится, для идентификации граждан используется набор сведений о лице (имя, фамилия, дата рождения, место жительства и т.д.). Одновременно вводится универсальная электронная идентификационная карточка, на чипе которой записан определенный набор идентифицирующих гражданина персональных данных. Эта карточка используется для установления личности гражданина при получении государственных услуг в электронном виде. Формирование универсального идентификатора законодательно запрещено (ФРГ);
– единый универсальный идентификатор не вводится. Для установления личности гражданина при получении государственных услуг в электронном виде используются специальным образом сгенерированные отраслевые коды, присвоенные гражданину в отношении каждой сферы государственной деятельности. Все отраслевые идентификаторы «встроены» в единую «карту гражданина», которая не является картой в прямом смысле этого слова, а представляет собой программное решение (набор функций), которое может храниться не только на смарт-карте, но и на мобильном телефоне или USB-накопителе (Австрия).

Таким образом, сегодня можно назвать лишь три развитые страны мира, которые используют универсальный идентификатор личности (Швеция, Бельгия, США).

Рассмотрим основные плюсы и минусы введения универсальных и отраслевых идентификаторов на основе международного опыта ряда стран.

Аргументы «за».

Простота и удобство использования. Использование универсального идентификатора является наиболее простым и удобным способом обобщения информации о конкретном физическом лице, содержащейся в базах данных различных органов публичной власти, позволяющим сопоставлять и консолидировать персональные данные с наименьшими организационными и техническими издержками.

Аргументы «против».

1. Нарушение права на неприкосновенность частной жизни.

Основным и важнейшим аргументом против использования универсального идентификатора является угроза нарушения права человека на неприкосновенность частной жизни и различных правонарушений с использованием персональных данных.

Использование универсального идентификатора для консолидации и унификации информации о гражданине, содержащейся во всех базах данных органов публичной власти, включая информацию, относящуюся к деликатной категории (информация о состоянии здоровья, половой жизни, вероисповедании и т.д.), вызывает серьезные возражения в обществе. Консолидация информации о человеке на основе одного лишь идентификатора позволяет получить полную информацию о человеке. В связи с этим в двух из трех государств, в которых используется универсальный идентификатор (Бельгия и США), достаточно остро стоит вопрос о нарушении права человека на неприкосновенность частной жизни. Использование универсального идентификатора для консолидации информации о гражданине делает жизнь гражданина прозрачной для государства и имеющих доступ к этой информации государственных служащих, сужая пределы автономии гражданина. Кроме того, использование

универсального идентификатора повышает риск мошенничества с использованием персональных данных («identity fraud» или «identity theft»).

Например, в Бельгии шли обширные дебаты по поводу уместности использования универсального идентификатора. Комиссия по защите персональных данных неоднократно указывала на то, что для защиты неприкосновенности частной жизни, необходимо как минимум использовать для обобщения уязвимой информации о гражданах (информация о состоянии здоровья и судебная информация) отдельный отраслевой идентификатор[1]. Соответственно, в Бельгии наблюдается тенденция к отказу от использования универсального идентификатора. В то же время расходы на переход от универсального идентификатора к отраслевым идентификаторам слишком высоки, и такой закон не был принят[2].

В США де-факто универсальность номера социального страхования (SSN) привела к многочисленным злоупотреблениям и частым случаям мошенничества с использованием персональных данных — identity theft. По данным Федеральной комиссии по торговле, ежегодно «кража личности» происходит в отношении 9 миллионов американцев[3]. В обзоре мировой практики показано, что в настоящее время Президент США и иные органы государственной власти проводят политику активного сокращения использования SSN. Между тем в данный момент США сложно отказаться от его использования, так как отсутствует какая-либо альтернатива, позволяющая органам государственной власти обмениваться информацией о гражданах при оказании электронных государственных услуг.

Таким образом, во всех государствах, кроме Швеции, где используется универсальный идентификатор (де-юре в Бельгии и де-факто в США), есть тенденция если не к полному

[1] Исследование D 13.3 консорциума FIDIS. С. 21.

[2] Там же. С. 56.

[3] Информация с официального сайта Федеральной комиссии по торговле http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html

отказу, то как минимум к сужению сферы применения универсальных идентификаторов.

В Австралии были два раза предприняты попытки ввести универсальный идентификатор, и оба раза правительство отказалось от проектов по его введению из соображений защиты неприкосновенности частной жизни и персональных данных граждан.

В Великобритании с 2006 по 2010 г. в качестве универсального идентификатора действовали Национальные идентификационные карточки, которые впоследствии были отменены в целях восстановления нарушенных гражданских прав и свобод. Созданный для обеспечения их использования централизованный реестр граждан был уничтожен.

В Венгрии универсальный идентификатор был отменен Конституционным судом в 1991 г. также из соображений защиты права на неприкосновенность частной жизни.

Придерживаясь таких же соображений, ФРГ и Австрия изначально сделали выбор в пользу исключительно отраслевых идентификаторов.

2. Высокие издержки контроля над целевым использованием персональных данных.

При использовании как универсальных, так и отраслевых идентификаторов государства принимают технические и правовые меры, направленные на защиту персональных данных при обмене информацией между органами государственной власти. Как правило, в законодательстве четко обозначаются цели, для достижения которых такой обмен информацией может осуществляться.

Цели обработки персональных данных могут изменяться посредством изменения законодательства. Когда два или более органа государственной власти уже интегрировали свои базы данных о человеке, они, как правило, будут использовать информацию для целей отличных от тех, для которых эта информация изначально предназначалась[1]. Существует риск, что когда создана необходимая инфраструктура (в частности централизованный реестр граждан), обмен

[1] Исследование D 13.3 консорциума FIDIS. С. 32.

информацией на основе универсального идентификатора будет осуществляться в любом случае, законно или незаконно, со ссылкой на аргументы *ad hoc* или различные политические соображения[1]. Именно этот процесс в настоящее время активно идет в Российской Федерации, когда изначально консолидация персональных данных или интеграция информационных систем их обработки осуществляется с законной целью (например, для обеспечения межведомственного взаимодействия во исполнение Федерального закона № 210-ФЗ), но фактическое использование персональных данных по итогам формирования технической возможности осуществляется бесконтрольно для большего круга задач.

Проблему усугубляет то, что издержки контроля над целями использования идентификаторов всеми органами публичной власти достаточно высоки. Кроме того, издержки контроля зависят от уровня коррупции в государстве. Чем выше уровень коррупции, тем выше издержки.

Также высокими являются и издержки по переходу от универсального идентификатора к отраслевым идентификаторам даже в ситуации, когда имеют место многочисленные правонарушения с использованием персональных данных. Это было показано выше на примере Бельгии и США.

Величина риска использования консолидированных персональных данных не по назначению зависит также от возможности граждан осуществлять свои демократические права и свободы, в частности избирательные права, и таким образом осуществлять политический контроль над государственной властью и влиять на принимаемые ею решения.

Заметим, что в Великобритании отказ от национальных идентификационных карточек произошел после того, как большинство в парламенте получили консерваторы (в противовес лейбористам, имевшим большинство до них). В Австралии оба раза отказ от введения универсального идентификатора также произошел после выборов в парламент.

[1] Там же.

3. Предложения по уточнению правового регулирования обработки персональных данных в публичном секторе в Российской Федерации

3.1. Уточнение терминов «обработка данных» и «конфиденциальность персональных данных»

Под обработкой персональных данных Закон о персональных данных понимает действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Устанавливая, что обработкой персональных данных являются любые действия с этими данными от сбора до уничтожения, закон в дальнейшем оперирует исключительно понятием «обработка», что вносит дополнительную неясность во все последующие нормы и ведет к путанице в правоприменительной практике. В Российском праве нет ни одного случая объединения в одно понятийное определение такого количе-

ства принципиально различающихся юридически значимых действий.

Такие действия, как сбор персональных данных и обезличивание этих данных, имеют совершенно различную правовую природу и, соответственно, должны иметь различный порядок регулирования. Объединение этих понятий одним определением «обработка», ведет к невозможности исполнения этого закона как в части защиты прав граждан, так и в части реализации интересов государства.

Положение усугубляется еще и тем, что закон не делает различий не только по существу совершаемых с персональными данными действий, но и по существу самих данных. Например, обработкой будут называться как манипуляции с различными данными одного человека, так и действия с однородными массивами персональных данных сколь угодно большого числа граждан.

Так в разных нормах закона неоднократно приводится требование о согласии гражданина на обработку его персональных данных без уточнения того, в чем эта обработка выражается. Например, если человек дает согласие на сбор его персональных данных, это не означает, что он согласен и на дальнейшее распространение этих данных, однако, в силу рассматриваемого закона, и сбор, и распространение являются обработкой. Соответственно, соглашаясь на обработку персональных данных, человек может оказаться в зависимости от того, насколько добросовестно и разумно будет трактовать слово «обработка» тот, кто эти данные собирает.

Не вполне оправданным следует считать и определение «конфиденциальность персональных данных». В тексте закона этот термин формулируется не как определенный правовой режим, который действиями оператора и иных субъектов отношений по поводу персональных данных должен обеспечивать информационную безопасность и информационной системы, и субъекта персональных данных, а только как требование оператора персональных данных не распространять сведения о нем без его согласия или без законного на то основания.

Исходя из такого определения конфиденциальности, ситуация, когда оператор не распространяет персональные данные, но и не обеспечивает их безопасность своим бездействием, не будет считаться нарушением конфиденциальности, поскольку распространение — это активные действия, а, например, утечка информации — это действия не самого оператора, а третьих лиц.

3.2. Особый режим обработки персональных данных публичными субъектами

В отличие от частных правоотношений, где субъект персональных данных волен выбирать контрагента (оператора персональных данных), а также принимать решение о вступлении или невступлении в договорные отношения, в публичных правоотношениях субъект персональных данных, как правило, такими возможностями не обладает. Кроме того, с учетом масштабов обработки персональных данных в публичной сфере, сам факт такой обработки создает повышенные риски для субъектов персональных данных.

Для нивелирования таких рисков законодательство о персональных данных должно устанавливать более жесткие требования для операторов персональных данных в публичной сфере. Такие требования должны применяться не только к государственным и муниципальным органам, но и ко всем организациям, выполняющим публичные функции в рамках реализации Федерального закона № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг».

Такой подход реализован во многих странах с развитой системой защиты персональных данных (например, Германия, Австрия, Австралия, Великобритания), однако в действующем российском законодательстве аналогичный подход не реализуется, более того, это является одним из недостатков Закона о персональных данных, позволяющим операторам персональных данных в публичной сфере обрабатывать их без согласия и уведомления субъекта персональных данных, без соответствующего запроса с его стороны,

без уведомления уполномоченного органа в сфере защиты персональных данных (п. 4 ч. 1 ст. 6 Федерального закона «О персональных данных», см. также разделы 1 и 2 выше).

Применение данных исключений на практике приводит к тому, что основополагающие принципы обработки персональных данных, предусмотренные Конвенцией о защите персональных данных, не реализуются, а права субъектов персональных данных нарушаются.

Необходимо конкретизировать положения п. 4 ч. 1 ст. 6 Закона о персональных данных, предусматривающие обработку персональных данных без согласия субъекта персональных данных в связи с предоставлением государственных и муниципальных услуг.

Право субъекта персональных данных на получение доступа к его персональным данным фактически не реализуется в связи с тем, что субъект персональных данных может получить сведения об обработке его персональных данных только при направлении запроса. Государственные и муниципальные органы обрабатывают персональные данные субъектов персональных данных без их согласия, и обязанность по предоставлению информации об обработке персональных данных при сборе такой информации у оператора персональных данных — государственного и муниципального органа — отсутствует, возможность субъекта персональных данных узнать о самом факте обработки и об операторе, которому необходимо подать запрос, существенно ограничена. При этом правовых актов, детализирующих положения Закона о защите персональных данных, в данной сфере не утверждено. К примеру, требования к порядку формирования, актуализации и использования базовых государственных информационных ресурсов, утвержденные постановлением Правительства Российской Федерации от 14 сентября 2012 г. № 928, содержат соответствующие требования к операторам персональных данных, но на практике для подавляющего большинства базовых государственных информационных ресурсов соответствующие порядки доступа субъекта персональных данных к его персональным данным не утверждены.

Несмотря на то, что Закон о персональных данных предусматривает общее требование об уведомлении Роскомнадзора об обработке персональных данных, исключения из этого правила сформулированы в Законе о персональных данных настолько широко, что необходимость реализации этого требования в сфере предоставления государственных и муниципальных услуг фактически отпадает.

Необходимо предусмотреть на законодательном уровне гарантии защиты персональных данных в случаях, когда уведомление специализированного органа по защите персональных данных об их обработке не обязательно.

В свете возможного введения в Российской Федерации универсального идентификатора сведений о физическом лице, представляется важным определить на законодательном уровне, что любой идентификатор, в том числе отраслевой, а тем более универсальный идентификатор, должен относиться к персональным данным, причем к специальной их категории, требующей повышенную защиту от несанкционированной или нецелевой обработки.

Использование идентификаторов должно быть жестко ограничено целями их создания и не должно трактоваться расширительно, делая возможным использование сбор и хранение идентификатора иными субъектами, кроме органов государственной власти или правомочными операторами, в иных, не оговоренных заранее, целях. На идентификаторы должны распространяться все требования Закона о персональных данных по обработке, хранению, защите и передаче персональных данных, в том числе при предоставлении государственных и муниципальных услуг.

В случае введения универсального идентификатора сведений о физическом лице в Закон о персональных данных необходимо добавить норму о том, что идентификатор сведений о физическом лице является персональными данными, относится к персональным данным с особым режимом защиты и распространить на него соответствующий режим защиты персональных данных.

Конституция Российской Федерации в ч. 1 ст. 24 закрепляет норму, в соответствии с которой сбор, хранение, использо-

вание и распространение информации о частной жизни лица без его согласия не допускаются.

В соответствии с ч. 3 ст. 55 Конституции Российской Федерации права и свободы человека и гражданина могут быть ограничены федеральным законом только в той мере, в какой это необходимо в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороноспособности и безопасности государства. Таким образом, сбор персональной информации возможен только на основании федерального закона.

По этой причине в случае создания государственного реестра населения необходимо принять Федеральный закон «О системе персонального учета населения», в котором должны быть определены:

– роль и функции ГРН, перечень персональных данных, включаемых в состав ГРН;
– ответственность за создание и функционирование ГРН на всех уровнях;
– порядок функционирования ГРН и присвоения гражданам идентификатора персональных данных;
– порядок предоставления информации из ГРН органам исполнительной власти, местного самоуправления и иным пользователям;
– порядок информационного взаимодействия ГРН с системами персонального учета разных категорий населения;
– требования к обеспечению защиты персональных данных ГРН.

3.3. Облачные технологии и трансграничная передача персональных данных

Действующее регулирование создает рамочные правовые условия для использования облачных вычислений, однако оно не обеспечивает их развитие и в ряде случаев создает для такого развития необоснованные препятствия.

Прежде всего, в настоящее время нормативно не урегулированы должным образом вопросы обеспечения безопасности и конфиденциальности информации, передаваемой поставщику облачных услуг. Кроме того, не закреплены нормы, четко определяющие административную, гражданско-правовую ответственность поставщика облачных услуг, а также уголовную ответственность руководителей и работников организаций, оказывающих облачные услуги.

В этой связи для перехода на использование облачных технологий в деятельности органов государственной власти и органов местного самоуправления необходимо подготовить предложения по нормативно-правовому регулированию использования облачных технологий в деятельности органов государственной власти и органов местного самоуправления и разработать проекты соответствующих нормативных правовых актов.

В целях создания основы для будущего регулирования облачных вычислений следовало бы включить в существующий Федеральный закон, например, в Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации», а в перспективе в отдельный специальный закон об облачных технологиях, определение «провайдера облачных вычислений» как разновидности «провайдера хостинга». Данное предложение основано на исследовании технологий облачных вычислений, учитывает рекомендации экспертов, зарубежный опыт и, как представляется, позволяет корректно ввести облачные вычисления в правовое поле российского законодательства.

Также необходимо обеспечить более гибкий подход к регулированию трансграничной передачи персональных данных. Данный вывод может быть сделан с учетом положительного законодательного и правоприменительного опыта зарубежных стран с высоким уровнем защиты персональных данных, прежде всего, стран Европейского союза. Поэтому в Федеральный закон «О персональных данных» предлагается ввести помимо существующего перечня стран с адекватным уровнем защиты, также договорные гарантии защиты персональных данных при их трансграничной передаче.

3.4. Предложения по оптимизации правового регулирования деятельности органов государственной власти Российской Федерации в сфере контроля обработки персональных данных в публичном секторе

3.4.1. Правовой статус уполномоченного органа

В рамках раздела 1 исследования мы рассматривали правовой статус Уполномоченного органа по защите персональных данных в Российской Федерации и проводили сопоставление с международной практикой в данной области. Представим основные параметры сравнения в таблице 1.

Из представленной таблицы видно, что в российском законодательстве о персональных данных не реализован сформированный международной практикой (в частности стран ЕС) принцип независимости уполномоченного органа по защите персональных данных.

Контроль и надзор за обеспечением информационной безопасности субъектов персональных данных в настоящее время осуществляет сама исполнительная власть, в процессе деятельности которой в основном и создаются информационные системы с обрабатываемыми персональными данными. Однако мировой опыт показывает, что более эффективным представляется статус независимого публичного органа по защите прав субъектов персональных данных.

В качестве одного из возможных вариантов реформирования правового режима Уполномоченного органа в сфере контроля за обработкой персональных данных в публичном секторе допустимо введение нового органа государственной власти, занимающегося деятельностью исключительно по линии «контроль—надзор—защита персональных данных в РФ», либо передача функций уже сформированному и действующему органу, например, Уполномоченному по правам человека при Президенте РФ, наделенному к тому же квазисудебными полномочиями по защите и восстановлению нарушенных прав.

Таблица 1. Сопоставление правового статуса Уполномоченного органа по защите персональных данных в РФ с международной практикой

ФЗ «О персональных данных»	**международная практика**
Уполномоченный (должностное лицо) или Уполномоченный орган?	
Уполномоченный орган	В разных странах по-разному
Обладает ли независимым статусом?	
Нет	Да, независимый статус закреплен в законе
В каких рамках функционирует?	
В рамках исполнительной власти	Независимый государственный орган
Порядок формирования	
Не определен	Определен в законе
Требования к членам надзорного органа	
Не определены	Как правило, сформулированы в законе
Обладает ли правом рассматривать жалобы и проводить проверки?	
Да	Да
Обладает ли правом осуществлять административное производство и накладывать штрафы?	
Да	В большинстве стран — да
Может ли участвовать в судебных процессах и самостоятельно обращаться в суд для защиты прав граждан?	
Может	Иногда
Занимается ли приемом и регистрацией уведомлений об обработке персональных данных?	
Да	Да
Имеет ли полномочия разрабатывать рекомендации по исполнению законодательства о персональных данных?	
Не определено	Да
Ведет ли просветительскую деятельность?	
Не определено	Иногда в законах это определено, но чаще подразумевается
Участвует ли в законотворческой деятельности?	
Да	Да
Участвует ли в международном сотрудничестве?	
Да	Да
Публикует ли регулярные отчеты?	
Да	Да

При этом к основным полномочиям данного органа следовало бы отнести:

– рассматривать жалобы и иные обращения физических и юридических лиц по вопросам защиты персональных данных и принимать решения по результатам их рассмотрения;
– проводить на основании обращений или по собственной инициативе выездные и невыездные, плановые, внеплановые проверки владельцев или распорядителей персональных данных в порядке, определенном уполномоченным органом, с обеспечением в соответствии с законом доступа к помещениям, где осуществляется обработка персональных данных;
– получать по своему требованию и иметь доступ к любой информации (документам) владельцев или распорядителей персональных данных, которые необходимы для осуществления контроля за обеспечением защиты персональных данных, в том числе доступ к персональным данным, соответствующих баз данных или картотек, информации с ограниченным доступом;
– по итогам проверки, рассмотрения обращения издавать обязательные для выполнения требования (предписания) о предотвращении или устранении нарушений законодательства о защите персональных данных;
– составлять протоколы о привлечении к административной ответственности и направлять их в суд в случаях, предусмотренных законом.

В качестве альтернативного варианта передачи полномочий ныне действующего государственного органа по надзору в сфере персональных данных (Роскомнадзора) другому специализированному и независимому органу следовало бы рассматривать возможность существования наряду с Роскомнадзором системы независимых самоуправляемых отраслевых ассоциаций в сфере защиты персональных данных.

Как подчеркивается в публикациях[1], если бы требования по защите персональных данных определялись оператором и вытекали из разработанных экспертным сообществом отраслевых стандартов, а не из жестких требований регуляторов, это привело бы к совершенствованию механизма защиты прав субъектов персональных данных. Альтернативой государственным регуляторам стали бы саморегулирующиеся организации, объединившие компании по критерию сферы деятельности (операторы сотовой связи, медицинские учреждения, страховые компании и др.). Отметим, что такой подход позволяет разгрузить Роскомнадзор, который в настоящее время не способен полноценно выполнять свои функции (в силу невозможности эффективного контроля 7 миллионов операторов при лимите проверок 6 тысяч в год).

3.4.2. Полномочия надзорного органа

Полномочия надзорного органа сформулированы в Законе о персональных данных в слишком общем виде, что создает неопределенность относительно его конкретных прав и обязанностей в отношении операторов персональных данных. Это приводит к неэффективности деятельности надзорного органа, ослаблению стимулов операторов персональных данных к соблюдению требований законодательства, повышает риск возникновения коррупции при осуществлении надзорным органом полномочий.

Деятельность Роскомнадзора регулируется Положением, утвержденным Постановлением Правительства РФ от 16 марта 2009 г. № 228 «О федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций» (далее — Положение от 16 марта 2009 г.). Однако в Положении нашли отражение не все полномочия, предусмотренные статьей 23 Федерального закона «О персональных данных».

[1] См., например: *Борисенко О.В.* Институт защиты прав субъектов персональных данных в Российской Федерации // Грамота. 2012. № 1 (15): в 2-х ч. Ч. I. С. 32.

Так, несмотря на наличие в Положении бланкетной нормы, в соответствии с которой наряду с полномочиями, прямо предусмотренными Положением, Роскомнадзор осуществляет и иные полномочия, в том числе предусмотренные федеральными законами, в настоящее время отсутствуют правовые механизмы реализации органами Роскомнадзора, в частности, права вносить в Правительство Российской Федерации предложения о совершенствовании нормативного правового регулирования защиты прав субъектов персональных данных, права обращаться в суд с исковым заявлением в защиту прав субъектов персональных данных и представлять интересы субъектов персональных данных в суде, а также обязанности организовывать в соответствии с требованиями настоящего Федерального закона и других федеральных законов защиту прав субъектов персональных данных.

Задача по приведению актов, регулирующих деятельность Роскомнадзора, в строгое соответствие с положениями Федерального закона «О персональных данных», представляется достаточно значимой для повышения уровня защиты прав субъектов персональных данных в России.

3.4.3. Предварительные проверки уполномоченного надзорного органа

В отличие от Директивы 95/46/ЕС и законодательств некоторых стран — членов ЕС, Закон о персональных данных не предусматривает проведение уполномоченным органом в области защиты персональных данных предварительных проверок в отношении случаев обработки персональных данных, создающей конкретные риски для прав и свобод субъектов данных.

В отличие от Директивы 95/46/ЕС и законодательств некоторых стран — членов ЕС, Закон о персональных данных предполагает, что оператор вправе приступить к обработке персональных данных сразу после направления уведомления в Роскомнадзор. Между тем Директива 95/46/ЕС (ст. 20) предусматривает предварительные проверки надзорного органа в отношении некоторых случаев обработки персональных

данных, когда такая обработка может создавать конкретные риски для прав и свобод субъектов данных.

Например, согласно параграфу 18 Закона о защите персональных данных Австрии[1], примерами таких случаев являются обработка персональных данных в рамках «объединенной информационной системы» и обработка чувствительных категорий персональных данных.

При этом под объединенными информационными системами понимаются системы, в которых осуществляется совместная обработка или совместное использование персональных данных несколькими операторами персональных данных таким образом, что операторы персональных данных имеют доступ даже к тем персональным данным в системе, которые стали доступны в системе благодаря другим операторам персональных данных.

Такие предварительные проверки осуществляются надзорным органом вслед за получением уведомления от оператора или служащего, занимающегося защитой данных, который, в случаях сомнения, должен проконсультироваться с надзорным органом. В случае если предусмотрен предварительный контроль, обработка персональных данных может быть начата только после соответствующего решения надзорного органа.

[1] Федеральный закон о защите персональных данных 2000 г. (Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 — DSG 2000), http://www.ris.bka.gv.at/GeltendeFassung.wxe? Abfrage=bundesnormen&Gesetzesnummer=10001597

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Конституция РФ от 12 декабря 1993 г.
2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (ред. от 04 июня 2014 г.).
3. Постановление Межпарламентской Ассамблеи государств — участников Содружества Независимых Государств от 16 октября 1999 г. № 14–19 «О модельном законе «О персональных данных»».
4. Конвенция Совета Европы от 28 января 1981 г. «О защите физических лиц при автоматизированной обработке персональных данных».
5. Федеральный закон от 19 декабря 2005 г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных».
6. Федеральный закон от 20 февраля 1995 г. № 24-ФЗ «Об информации, информатизации и защите информации».
7. Указ Президента РФ от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера».
8. Указ Президента РФ от 30 мая 2005 г. № 609 «Об утверждении положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела».
9. Кодекс РФ об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ.
10. Федеральный закон от 3 декабря 2008 г. № 242-ФЗ «О государственной геномной регистрации в Российской Федерации» (с изм. от 17 декабря 2009 г.).

11. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. от 05 мая 2014 г., с изм. от 21 июля 2014 г.).
12. Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне» (ред. от 11 июля 2011 г.).
13. Федеральный закон от 1 апреля 1996 г. № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования» (ред. от 12 марта 2014 г.).
14. Федеральный закон от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг».
15. Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
16. Постановление Правительства РФ от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».
17. Постановление Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
18. Постановление Правительства Российской Федерации от 6 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных» (ред. от 27 декабря 2012 г.).
19. Постановление Правительства РФ от 8 сентября 2010 № 697 «О единой системе межведомственного электронного взаимодействия» (ред. от 19 марта 2014 г.).

20. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
21. Приказ ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489 «Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования».
22. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (утв. ФСБ России 21 февраля 2008 г. № 149/54–144).
23. Модель угроз и нарушителя безопасности персональных данных, обрабатываемых в типовых информационных системах персональных данных отрасли, согласованная Письмом ФСБ России от 10 августа 2010 г. № 149/7/2/6–1203 и Письмом ФСТЭК России от 04 июня 2010 г. № 240/2/2271.
24. Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных (утв. ФСБ России 21 февраля 2008 г. № 149/6/6–622).
25. Приказ Роскомнадзора от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных».
26. Приказ ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных».
27. Указ Президента РФ от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».

28. Конвенция «О защите физических лиц при автоматизированной обработке персональных данных» ETS № 108 (Страсбург, 28 января 1981 г.).
29. Директива 95/46/ЕС от 24 октября 1995 г. «О защите физических лиц в отношении обработки персональных данных и о свободном движении таких данных».
30. Директива 97/66/ЕС Европарламента и Европейского совета от 15 декабря 1997 г. «Об обработке персональных данных и защите конфиденциальности интересов абонентов, являющихся как физическими, так и юридическими лицами».
31. Директива № 2002/58/ЕС Европейского парламента и Совета Европейского союза «В отношении обработки персональных данных и защиты конфиденциальности в секторе электронных средств связи (Директива о конфиденциальности и электронных средствах связи)» (Принята в г. Брюсселе 12 июля 2002 г.) (с изм. и доп. от 25 ноября 2009 г.).
32. Privacy Act of 1974, Pub. L. No 93–579, 88 Stat. 1896 (Dec. 31, 1974), codified at 5 U.S.C. § 552a (1974).
33. Privacy Protection Act of 1980 (PPA), Pub. L. No. 96–440, 94 Stat. 1879 (Oct. 13, 1980), codified at 42 U.S.C. § 2000aa et seq.
34. Code of Fair Information Practices. U. S. Dep't. of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, Records, computers, and the Rights of Citizens VIII (1973).
35. Аналитическая записка к проекту Федерального закона 217346–4 О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных 2005 ноябрь. http://iam.duma.gov.ru/node/8/4740/17032.
36. Защита персональных данных за рубежом: США http://weta.ru/privacy-comments-us-law-analysis.php.
37. *Волчинская Е.К.* Некоторые правовые проблемы применения Федерального закона «О персональных данных» // Персональные данные. 2009. № 2.
38. Требования к порядку формирования, актуализации и использования базовых государственных информацион-

ных ресурсов (утв. Постановлением Правительства РФ от 14 сентября 2012 г. № 928).
39. Положение о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций (утв. Постановлением Правительства РФ от 16 марта 2009 г. № 228).
40. Распоряжение Правительства Москвы № 376-РП от 12 мая 2011 г. «О Базовом регистре информации, необходимой для предоставления государственных услуг в городе Москве».
41. Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. Official Journal of European Communities, LS/1, 12.01.2001.
42. Федеральный закон от 21 июля 2014 г. № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях».
43. Переход на использование облачных технологий в деятельности органов государственной власти и органов местного самоуправления. http://minsvyaz.ru/ru/doc/printable.php?id_4=946.
44. Проект Постановления Правительства РФ от 21 мая 2014 г. № 00/04–15149/05–14/4–13–3 «О внесении изменений в Перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами, утвержденный постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211» // http://regulation.gov.ru/project/15149.html.
45. Постановление Правительства РФ от 28 ноября 2011 г. № 977 «О федеральной государственной информационной системе «Единая система идентификации и аутенти-

фикации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме»» (ред. от 09 декабря 2013 г.).
46. Распоряжение Правительства РФ от 15 апреля 2011 г. № 654-р «О базовых государственных информационных ресурсах».
47. Концепция создания системы персонального учета населения Российской Федерации (утв. Распоряжением Правительства Российской Федерации от 9 июня 2005 г. № 748-р).
48. Федеральный закон от 19 мая 2013 г. № 99-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» и Федерального закона «О персональных данных»».
49. *Борисенко О.В.* Институт защиты прав субъектов персональных данных в Российской Федерации // Грамота. 2012. № 1 (15): в 2-х ч. Ч. I.
50. Федеральный закон Австрии о защите персональных данных (Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 — DSG 2000)) // http://www.ris.bka.gv.at/GeltendeFassung.wxe? Abfrage=bundesnormen &Gesetzesnummer=10001597).

Научная литература

Серия «Научные доклады: государство и право»

Заказное издание

Михаил Юрьевич Брауде-Золотарёв
Евгения Сергеевна Сербина
Виталий Станиславович Негородов
Иван Геннадьевич Волошкин

**Персональные данные
в государственных информационных ресурсах**

Выпускающий редактор *Е. В. Попова*
Художник *Е. В. Трушина*
Оригинал-макет *О. З. Элоева*
Верстка *Т. А. Файзуллиной*

Подписано в печать 24.12.2015. Формат 60x90 1/16
Гарнитура ПТ Сериф. Усл. печ. л. 3,5. Тираж 530 экз.
Заказ № 1394.

Издательский дом «Дело» РАНХиГС
119571, Москва, пр-т Вернадского, 82

Коммерческий центр – тел. (495) 433–25–10, (495) 433–25–02
www.ranepa.ru
delo@ranepa.ru

Отпечатано в типографии РАНХиГС
119571, Москва, пр-т Вернадского, 82