**АНАЛИТИЧЕСКИЙ ОБЗОР МЕЖДУНАРОДНОГО ОПЫТА ПО ЛОКАЛИЗАЦИИ БАЗ ДАННЫХ, СОДЕРЖАЩИХ ПЕРСОНАЛЬНЫЕ ДАННЫЕ ГРАЖДАН**

**СОДЕРЖАНИЕ**

[1. Обзор законодательства в сфере локализации персональных данных в странах мира 2](#_Toc502066549)

[2. Российская практика правоприменения в сфере обеспечения локализации баз, содержащих персональные данные граждан Российской Федерации, на территории Российской Федерации 8](#_Toc502066550)

[3. Международная практика регулирования правового статуса общедоступной информации, содержащей персональные данные граждан 13](#_Toc502066551)

# **ОБЗОР ЗАКОНОДАТЕЛЬСТВА В СФЕРЕ ЛОКАЛИЗАЦИИ ПЕРСОНАЛЬНЫХ ДАННЫХ В СТРАНАХ МИРА**

Локализация баз персональных данных характерна для многих стран. В данном обзоре внимание будет уделено таким странам, как Китай, Австралия, Индонезия, Нигерия, Вьетнам, Индия, Казахстан, Канада.

Экспертыотмечают, что в **Китае** в последние годы законы и правила все чаще содержат требования к локализации данных, поскольку правительство стремится уменьшить потенциальные барьеры для своей юрисдикции в отношении данных.

Так, в 2011 году Народный банк Китая опубликовал Уведомление, посвященное необходимости повышения уровни защиты личной финансовой информации.

Под личной финансовой информацией в Китае понимают персональную информацию (имя, пол, национальность, фотография), информацию о личной собственности, информацию о личном счете, личную кредитную информацию, информацию о транзакциях, иная производная информация (информация, полученная путем анализа первичной информации), другая личная информация, ставая известная Банку в ходе делового сотрудничества, договорных отношений.

В Уведомлении содержится запрет Банкам хранить, обрабатывать или анализировать за пределами Китая любую личную финансовую информацию, которая была собрана в Китае, или предоставлять личную финансовую информацию, собранную в Китае, оффшорному предприятию.

Нарушение требований, содержащихся в Уведомлении, дает право Народному Банку Китая приказать соответствующему Банку исправить свое несоответствие и потребовать от Банка наказать ответственных должностных лиц.

Кроме того, с 1 июня 2017 года вступил в силу Закон о кибербезопасности, который установил новые ограничения для операторов ключевой информационной инфраструктуры, операторов сетей и поставщиков сетевых продуктов и услуг.

Так, статьей 37 Закона о кибербезопасности предусмотрено, что операторы критической информационной инфраструктуры должны хранить на материковой территории КНР собранную или произведенную ими персональную информацию на материковой части Китая. Однако, когда из-за требований бизнеса действительно необходимо обеспечить хранение персональной информации за пределами материка, операторы критической информационной инфраструктуры должны следовать мерам, совместно сформулированным государственными сетевыми информационными департаментами и соответствующими департаментами Государственного совета для проведения оценки безопасности; но в тех случаях, когда законы и административные нормы предусматривают иное, необходимо следовать этим положениям.

Если операторы критической информационной инфраструктуры нарушают статью 37 Закона путем хранения данных за пределами материковой территории или предоставляют сетевые данные отдельным лицам или организациям за пределами материковой территории без проведения оценки безопасности, соответствующий компетентный отдел дает предупреждения, конфисковывает незаконно полученную выгоду, налагает штрафы в размере от 50 000 до 500 000 юаней и может вынести постановление о временном приостановлении операций, приостановлении деятельности для устранения нарушений, прекратить деятельность веб-сайтов, аннулировать соответствующие разрешения на деятельность или аннулировать лицензии на деятельность. Лица, осуществляющие контроль соблюдения требований законодательства, ответственные лица, в случае выявления нарушения могут быть оштрафованы на сумму от 10000 до 100000 юаней.

Также, требование локализации касается баз данных, содержащих медицинские сведения. Так, Мерами по управлению информацией о здоровье населения, принятыми Государственным комитеот по делам здравоохранения и планового деторождения КНР, предусмотрено, что медицинские учреждения, организации в сфере социального обеспечения (социальные службы), учреждения по планированию семьи не могут хранить информацию о здоровье населения на серверах за границей или иным образом размещать или арендовать зарубежные серверы.

Относительно деятельности иностранных компаний на территории Китая отметим, что в адрес их представительств на территории Китая периодически направляется уведомление с требованием локализовать хранение персональных данных на территории Китая. В случае отказа, интернет-сервисы указанных компаний временно блокируются на основании решения уполномоченного органа исполнительной власти.

В 2012 году в **Австралии** был принят закон, регулирующий вопросы предоставления доступа к электронным медицинским записям для соответствующих целей (Personally Controlled Electronic Health Records Act 2012 № 63), который, в том числе, определил обязанность лиц, имеющих доступ к информации, содержащейся в электронных медицинских записях граждан, обеспечить хранение такой информации на территории Австралии.

Так, согласно ч. 1 ст. 77 указанного Закона оператор системы, зарегистрированный оператор репозитория, зарегистрированный оператор портала или зарегистрированный контрактный поставщик услуг, который хранит записи для целей системы PCEHR, независимо от того, хранятся ли записи в других целях) или имеется доступ к информации в отношении таких записей, не должны:

хранить записи или записывать записи за пределами Австралии;

обрабатывать или обрабатывать информацию, относящуюся к записям за пределами Австралии;

разрешать другим лицам хранить записи или использовать записи за пределами Австралии, обрабатывать или обрабатывать информацию, относящуюся к записям, за пределами Австралии.

За нарушение указанных запретов предусмотрен штраф в размере 120 штрафных единиц.

В тоже время, ч. 2 ст. 77 Закона предусмотрено, что для целей эксплуатации или администрирования системы PCEHR Системный оператор вправе:

хранить и принимать такие документы за пределами Австралии, при условии, что эти записи не включают личную информацию в отношении потребителя или участника системы PCEHR или информацию, позволяющую идентифицировать физическое или юридическое лицо;

обрабатывать и обрабатывать такую информацию за пределами Австралии, при условии, что информация не является личной информацией в отношении потребителя или участника системы PCEHR и (или) информацией, позволяющей идентифицировать физическое или юридическое лицо.

Резюмируя изложенное: организации, в том числе иностранные, осуществляющие обработку сведений, связанных со здоровьем, должны создавать центры обработки данных на территории Австралии или поручать обработку такой информации австралийским компаниям, имеющим такие центры в Австралии. Осуществление действий, направленных на обработку сведений, содержащих информацию о состоянии граждан за пределами Австралии возможно, только при соблюдении требования по обезличиванию такой информации.

В 2012 году правительство **Индонезии** потребовало, чтобы государственные учреждения, организация, участвующие в предоставлении государственных услуг, обеспечили создание центров обработки данных на территории Индонезии.

Положением п. 82 Эксплуатации электронной системы и операций предусмотрено, что электронный системный оператор в этих целях обязан также центр аварийного восстановления на индонезийской территории.

В дальнейшем, в 2014 году Министерство связи распространило требование о нахождении центров обработки данных для аварийного восстановления для более широкого круга учреждений – любых учреждений и организаций, предоставляющих услуги с использованием информационных технологий.

Кроме того, электронный системный оператор должен обеспечить хранение данных о транзакцияхв Индонезии. Требование хранить данные, возникающие в результате электронных транзакций между поставщиками электронных систем и их клиентами в Индонезии, применяется как к частным, так и к публичным поставщикам электронных систем в рамках GR 82. В этом контексте нет определения «транзакционных данных». Однако, по мнению некоторых экспертов, транзакционные данные охватывают данные, которые приводят к юридическим последствиям.

В **Нигерии** в 2013 году Национальное агентство по развитию информационных технологий выпустило Руководство по развитию нигерийского контента в области информационных и коммуникационных технологий. Согласно положениям Руководства организации, осуществляющие действия с данными и информацией, позволяющей идентифицировать гражданина, должны обеспечить локализацию баз таких данных на территории страны.

В сентябре 2013 года во **Вьетнаме** вступил в силу Декрет об управлении, предоставлении и использовании интернет-услуг и информационном контенте в Интернет, согласно которому все компании, предоставляющие интернет-услуги должны иметь хотя бы один сервер с базами данных на территории Вьетнама.

В октябре 2013 года Министерство информации и связи распространило проект циркуляра, в котором представлены дополнительные данные о реализации Декрета, в том числе, содержащее требование, что в случае наличия требований к серверной системе, расположенной во Вьетнаме, вся серверная система, расположенная за пределами Вьетнама, должна отвечать этим требованиям.

Согласно Национальной политики обмена данными и доступности **Индии** все данные, собранные с использованием государственных ресурсов, должны храниться на территории Индии.

В феврале 2014 года Совет национальной безопасности Индии предложил обеспечить локализацию всех персональных данных граждан Индии на территории Индии.

Так, предполагалась, что всем провайдерам услуг электронной почты может быть поручено разместить свои серверы, собирающие данные индийцев на территории Индии. Также, инициатива Совета национальной безопасности запрещает создание зеркал таких серверов, если основной сервер храниться за рубежом.

Кроме того, было предложение обеспечить всем телекоммуникационным и интернет-компаниям маршрутизацию локальных данных через Национальную интернет-биржу Индии.

В настоящее время, Закон о телекоммуникациях Индии предусматривает, что вся информация о клиентах и информация о пользователях (кроме сведений о роуминге) должна храниться на территории Индии, удаленный доступ к такой информации из-за пределов Индии запрещен.

В **Казахстане** Закон о персональных данных РК был принят в 2013 г., в 2015 г. в него были внесены изменения. Изменения 2015 г. были связаны с введением требования о хранении (локализации) персональных данных в Казахстане. Требование хранить персональные данные в Казахстане вступило в силу 1 января 2016 г.

Требование локализации персональных данных требует только хранить базы данных с персональными данными на территории РК.

В законе отсутствует требование сохранить персональные данные сначала в Казахстане, а потом передавать их в другие страны. Соответственно, сбор, обработка, использование и внесение изменений в базу данных могут производиться сначала за рубежом с последующим сохранением базы данных с персональными данными на территории РК. В таком случае компании должны быть готовы предоставить доказательства того, что база данных с персональными данными была в последующем сохранена в Казахстане.

В случае первоначального сохранения данных за рубежом, важно обеспечить синхронизацию баз данных за рубежом и в Казахстане. Частота синхронизации не определена в Законе о персональных данных.

Персональные данные в Казахстане должны хранить, как владельцы баз данных, так и операторы баз данных.

В **Канаде** в системе федерального законодательства отсутствует требование по локализации баз персональных данных граждан на территории Канады. Однако, такое требование существует на уровне двух провинций – Новой Шотландии и Британской Колумбии.

До декабря 2017 года в Британской Колумбии существовал Закон о свободе информации и защите частной жизни. Согласно ст. 30.1. Закона общественный орган должен обеспечить, чтобы хранение личной информации, находящейся в распоряжении такого органа, а также доступ к ней, осуществлялись только на территории Канады. При этом, субъект данных мог дать согласие на хранении или использование личной информации в другой юрисдикции.

В Новой Шотландии вопросы хранения баз данных, содержащих персональные данные, урегулированы положениями Закона о защите личной информации. Законодательные положения об обеспечении локализации в Новой Шотландии идентичны положениям (ст. 5(1), существовавшим в Британской Колумбии. За нарушение требований ст. 5 (1) Закона о защите личной информации предусмотрена ответственность согласно ст. 12 указанного Закона.

# **РОССИЙСКАЯ ПРАКТИКА ПРАВОПРИМЕНЕНИЯ В СФЕРЕ ОБЕСПЕЧЕНИЯ ЛОКАЛИЗАЦИИ БАЗ, СОДЕРЖАЩИХ ПЕРСОНАЛЬНЫЕ ДАННЫЕ ГРАЖДАН РОССИЙСКОЙ ФЕДЕРАЦИИ, НА ТЕРРИТОРИИ РОССИЙСКОЙ ФЕДЕРАЦИИ**

Знаковым событием в регулировании сферы персональных данных стало вступление в силу в 2015 году Федерального закона от 21.07.2014  
№ 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно - телекоммуникационных сетях» (далее – Закон).

Положениями части 1 статьи 2 Закона для оператора установлена новая обязанность - осуществлять при сборе персональных данных определенные виды обработки персональных данных в базах данных, которые находятся на территории России.

Введенная норма содержит четкий закрытый перечень видов обработки персональных данных, а именно: запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации, которые оператор обязан осуществлять с использованием баз данных, находящихся на территории Российской Федерации.

Представляется необходимым обратиться к вопросу о действии нормы, введенной частью 1 статьи 2 Закона, в пространстве, во времени и по кругу лиц.

Вчасти действия Закона в пространстве отметим, что все российские нормативные правовые акты действуют на всей территории страны. При этом деятельность иностранных компаний, осуществляемая посредством сети Интернет, особым свойством которого является трансграничность, не умаляет данного положения.

Действие закона по кругу лиц означает, что Закон действует в отношении всех лиц, находящихся на этой территории России и являющихся субъектами отношений, на которые распространяется акт.

Коррелируя это положение с понятием территории России с учетом свойств трансграничности Интернета, можно сказать, что комментируемая норма распространяет свое действие на лиц (операторов персональных данных), осуществляющих свою деятельность на территории Российской Федерации, то есть распространяется как на российские компании, так и на иностранные.

В настоящее время практика ведения бизнеса посредством Интернета сформировала модель оказания услуг пользователям, при которой компания не обязана образовывать юридическое лицо на территории места нахождения пользователей компании (направленности интернет сервисов компании), то есть места фактического осуществления своей деятельности, а также не обязана вносить налоговые платежи, исполнять иные требования национального законодательства.

Однако Закон определил необходимость исполнения нормы о локализации данных иностранными компаниями, в том числе, которые осуществляют деятельность на территории России без образования официальных представительств или иных форм юридических лиц.

Важным является вопрос определения критериев направленности иностранных сайтов, посредством которых компании осуществляют коммерческую деятельность на территории России.

Говорить о наличии направленности Интернет-сайта на территорию Российской Федерации могут, в том числе следующие обстоятельства:

1) использование делегированного доменного имени, связанного с Российской Федерацией (.ru, .рф., .su) и/или

2) наличие русскоязычной версии Интернет-сайта, созданной владельцем такого сайта или по его поручению иным лицом (использование на сайте или самим пользователем плагинов, предоставляющих функционал автоматизированных переводчиков с различных языков, не должно приниматься во внимание);

3) возможности исполнения заключенного на таком Интернет-сайте договора на территории Российской Федерации (доставки товара, оказания услуги или пользования цифровым контентом на территории России).

Более подробно разберем содержание вводимой нормы.

При определении понятия«база данных» следует учитывать, что в законодательстве Российской Федерации существует много понятий баз данных, тем не менее все они сводятся к одному общему значению, согласно которому база данных - это упорядоченный массив данных, независимый от вида материального носителя информации и используемых средств его обработки (архивы, картотеки, электронные базы данных). Так, например, базой данных можно считать таблицу в формате Excel, word, в которой содержатся персональные данные граждан.

При этом, единственным законным признаком, которым должна обладать база данных, является ее место нахождения – территория Российской Федерации.

Долгое время существовал спор можно ли считать предметом регулирования комментируемого закона базу данных, сформированную на бумажных носителях, при последующем внесении указанных сведений в информационную систему персональных данных.

Существующая позиция основывается на принципе, согласно которому обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. В связи с этим внесение персональных данных в информационную систему персональных данных, используемую в целях, аналогичных сбору данных на бумажных носителях, следует рассматривать как единый процесс, реализация которого должна осуществляться в строгом соответствии с требованиями части 5 статьи 18 Федерального закона №152-ФЗ. Разделение указанного единого процесса на отдельные действия законодательством Российской Федерации в области персональных данных не предусмотрено. Таким образом, отдельные виды обработки персональных данных, предусмотренные частью 5 статьи 18 Федерального закона №152-ФЗ, в том числе сбор персональных данных на бумажных носителях с последующим их внесением в электронную базу данных, должны осуществляться как единый процесс в правовом поле законодательной нормы, обязывающей хранить персональные данные на территории Российской Федерации.

Понятие «оператор» содержится в статье 3 Федерального закона  
№ 152-ФЗ, под которым понимается государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными. Таким образом, в свете применения комментируемой нормы, оператором является лицо, осуществляющее сбор персональных данных, либо поручившее его третьему лицу на основании договора поручения.

В отношении отнесения той или иной информации к персональным данным следует руководствоваться статьей 3 Федерального закона № 152-ФЗ, согласно которому персональные данные – это любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). Таким образом, отнесение указанного перечня информации к персональным данным возможно при условии соответствия данной информации положениям Федерального закона № 152-ФЗ.

Реализация обязанности «при сборе данных» означает, что оператор должен их получать непосредственно у первоисточника, то есть у субъекта персональных данных или его представителя. В таком случае речь идет о сборе информации, а не о случаях передачи данных третьему лицу для обработки в каких-либо целях.

Так, оператор, получив данные субъекта, обязан обеспечить их запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение с использованием баз данных, находящихся в России.

Указанные виды обработки данных представляют собой единый процесс формирования и поддержания базы данных в актуальном состоянии. Образно говоря, можно сказать, что законодатель вводит правило, согласно которому формирование и актуализация баз персональных данных российских граждан должны осуществляться на территории России.

Так, база данных, сформированная посредством сбора персональных данных, должна находиться на территории России и актуализироваться также на территории России.

При этом комментируемый закон не запрещает передавать данные из этой базы на территорию иностранного государства. Но обновление данных во всех случаях будет осуществляться в базе данных, расположенной на территории России, и, при необходимости, обновленные данные могут быть переданы на территорию иностранного государства.

Необходимо отметить, что параллельный ввод собранных персональных данных в российскую информационную систему и систему, находящуюся на территории иностранного государства, не отвечает требованиям комментируемой нормы, поскольку после сбора посредством российской информационной системы указанные сведения могут быть переданы в иностранную информационную систему только посредством трансграничной передачи.

Следует обратить внимание на возможность поручения иностранным лицом российскому юридическому лицу осуществить сбор персональных данных в России, однако необходимо учесть, что такие правоотношения возможны при условии неукоснительного соблюдения требований части 3 статьи 6 Федерального закона № 152-ФЗ.

В отношении использования международных территориально распределенных систем, в том числе при оказании услуг по кадровому и бухгалтерскому учету в рамках аутсорсинга следует отметить, что при сборе персональных данных российских пользователей в рамках территориально распределенной системы указанные действия должны быть обеспечены с использованием баз данных, расположенных на территории Российской Федерации.

При реализации деятельности по кадровому учету и расчету заработной платы, в том числе с участием аффилированного лица, оператор в соответствии с требованиями комментируемой нормы обязан обеспечить сбор указанных данных с использованием баз данных, расположенных на территории Российской Федерации. Последующая трансграничная передача в иную базу должна осуществляться согласно требованиям статьи 12 Федерального закона №152-ФЗ.

По вопросу копирования персональных данных следует заметить, что «копирование» представляет собой процесс, характеризующийся созданием дубликата документа или информации. То есть основным свойством данного действия является создание дубликата вне зависимости от способа и цели его создания или места нахождения дублирующей информации. Таким образом, скопированные персональные данные подлежат хранению и последующему использованию в соответствии с требованиями Федерального закона № 152-ФЗ.

Хранение персональных данных должно быть ограничено достижением цели обработки. Федеральным законом № 152-ФЗ (часть 4 статьи 21) предусмотрено, что в случае достижения цели обработки персональных данных оператор обязан прекратить обработку персональных данных или обеспечить ее прекращение и уничтожить персональные данные в срок, не превышающий 30 дней с даты достижения цели обработки персональных данных.

В случае отсутствия возможности уничтожения персональных данных в течение указанного срока оператор осуществляет блокирование персональных данных и обеспечивает уничтожение персональных данных в срок не более чем 6 месяцев.

Необходимо отметить, что в норме отсутствуют понятия «временное хранение», «постоянное хранение», в связи с чем использование подобной терминологии, в том числе в согласиях на обработку персональных данных, является недопустимым.

Относительно применения требований локализации баз персональных данных к обработке общедоступных сведений необходимо отметить, что статьей 2 указанного закона не установлены исключения применительно к пункту 10 части 1 статьи 6 Федерального закона № 152-ФЗ. Таким образом, при осуществлении сбора общедоступных персональных данных на деятельность оператора требования комментируемой нормы распространяются в полном объеме.

# **МЕЖДУНАРОДНАЯ ПРАКТИКА РЕГУЛИРОВАНИЯ ПРАВОВОГО СТАТУСА ОБЩЕДОСТУПНОЙ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙ ПЕРСОНАЛЬНЫЕ ДАННЫЕ ГРАЖДАН**

Ключевым принципом защиты данных, согласно Директиве Европейского Союза об открытой информации, принятой в 2003 году, является ограничение цели использования персональных данных и требуя, чтобы личные данные, которые были собраны для определенной цели, далее не использовались для другой, несовместимой цели. Этот принцип в равной степени относится к личным данным, которые общедоступны. Простой факт того, что личные данные общедоступны для определенной цели, не означает, что такие личные данные открыты для повторного использования для любой другой цели.

Соответствующие положения гармонично трансформировались в национальное законодательство, в том числе и российское, согласно которому вторичная обработка персональных данных должна коррелироваться с первоначальными целями сбора персональных данных.

Так, согласно ч. 2 ст. 5 Закона № 152-ФЗ, обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных. В соответствии с ч. 4 ст. 5 указанного закона, обработке подлежат только персональные данные, которые отвечают целям их обработки.

Кроме того, правовая конструкция ст. 7 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее-Закон №149-ФЗ) в части указания на возможность распространения общедоступной информации, размещенной в формате «открытых данных» предполагает взаимосвязанность понятий «размещение» и «распространение» общедоступной информации, размещаемой в формате открытых данных, в том числе в контексте ограничений ее распространения.

В частности, согласно ч. 6 ст. 7 Закона №149-ФЗ в случае, если размещение информации в форме открытых данных осуществляется с нарушением требований Закона № 152-ФЗ, размещение информации в форме открытых данных должно быть приостановлено или прекращено по требованию уполномоченного органа по защите прав субъектов персональных данных. Применительно к положениям Федерального закона «О персональных данных» нарушением в данном случае может быть распространение открытых данных, содержащих персональные данные, в случаях, предусматривающих получение согласия субъекта и соответствие целям их первоначального сбора.

Таким образом, дальнейшее распространение персональных данных граждан, содержащихся на основании законов без согласия субъектов персональных данных в общедоступных реестрах, в целях, отличных от заявленных на этапе их сбора, будет нарушать требования законодательства в области персональных данных.

Аналогичной точки зрения придерживаются иностранные государства, в структуре органов власти которых существуют уполномоченные органы по защите прав субъектов персональных данных.

Так, на национальном уровне иностранных государств, за исключением Республики Сингапур, имеются созданные в соответствии с законодательством открытые регистры, содержащие персональные данные.

При этом, вторичное использование персональных данных, содержащихся в публичных регистрах, возможно только с учетом первичных законно установленных целей, ради которых они были размещены (собраны) (Гонконг, Королевство Дания, Королевство Нидерландов, Словацкая Республика, Республика Словения, Республика Албания, Республика Хорватия, Австрийская Республика, Республика Мальта, Мексика), в исключительных случаях, предусмотренных законом (официальный запрос полиции, суда) (Венгрия, Республика Албания, Республика Хорватия, Мексика), а также в статистических или научных исследованиях в случае обезличивания персональных данных (Королевство Дания, Республика Словения, Республика Албания, Румыния).

В частности, по информации, представленной уполномоченным органом Словацкой Республикой, оператор, намеревающийся обрабатывать персональные данные, которые были раскрыты в соответствии с законом, должен доказать, что обрабатываемые персональные данные данные были ранее раскрыты по закону, а также, что он использует их исключительно в целях ради которых данные были собраны и раскрыты.

Таким образом, международный опыт нормативного правового регулирования, в том числе правоприменения, распространения общедоступной информации, содержащей персональные данные, показал, что для вторичного использования персональных данных, должны быть правовые основания, а также цель обработки должна коррелироваться с целью, ради которой личные данные были собраны.

На несоблюдение вышеуказанных условий в иностранных государствах существует система санкций за нарушение порядка и условий ведения публичных регистров, установлены административная, гражданская или уголовная ответственность. В качестве меры ответственности применяются в основном штрафы, а также приостановление обработки персональных данных и аресты (1-3 лет).

Заслуживает внимания административно-пресекательная практика уполномоченного органа Гонконга. Так, комиссар по защите персональных данных Гонконга имеет право издавать уведомление для правоохранительных органов в отношении нарушителя с требованием пресечь деятельность и принять меры по исправлению положения дел.

В качестве примера представлена информация о результатах расследования в отношении разработчиков мобильного приложения под названием «не делай зла». Разработчик мобильных приложений собирал и сопоставлял различные персональные данные из открытых источников (в том числе открытых регистров). Таким образом, была построена всеобъемлющая база данных, касающаяся большого числа граждан. По результатам принятых уполномоченным органом Гонконга мер реагирования деятельность указанного мобильного приложения была пресечена.

Уполномоченные по защите прав субъектов персональных данных в в целях усиления защиты персональных данных, включенных в открытые регистры, разрабатывают соответствующие предложения по внесению в действующее законодательство положений, направленных на защиту от неправомерного использования персональных данных из открытых регистров, законодательного закрепления использования открытых данных в конкретных целях, не противоречащих целям создания публичного регистра.

Иными словами, обработка персональных данных исключительно в целях, которые определены законом и известны субъекту персональных данных, является одним из основополагающих принципов деятельности как российского, так и иностранных уполномоченных органов, а также необходимым условием защиты прав и законных интересов субъекта персональных данных.

Кроме того, что в соответствии с ч. 9 ст. 23 Закона № 152-ФЗ при Роскомнадзоре в 2009 году создан Консультативный совет, являющийся общественной площадкой, объединяющей представителей государственных органов, представителей профессиональных объединений операторов, научного и экспертного сообщества.

Консультативный совет уделяет большое значение развитию и совершенствованию деятельности в области персональных данных, основными задачами Консультативного совета являются подготовка предложений и рекомендаций по вопросам гармонизации законодательства Российской Федерации в области защиты персональных данных с учетом общественного мнения и опыта правоприменительной практики; методическое обеспечение правоприменительной деятельности в области защиты персональных данных; создание условий для повышения правового уровня и активной гражданской позиции общества.

На заседании Консультативного совета, состоявшемся 19 мая 2016 года, членами Консультативного совета был обсужден вопрос о возможности распространения неограниченным кругом лиц сведений, относящихся к персональным данным, содержащихся в открытых реестрах в форме открытых данных, в целях, отличных от их первоначального размещения.

Согласно единогласно принятой позиции членов Консультативного совета, принявших участие в указанном заседании, распространение неограниченным кругом лиц сведений, относящихся к персональным данным, содержащихся в открытых реестрах в формате открытых данных, в целях, отличных от их первоначального размещения, является недопустимым и противоречит Закону № 152-ФЗ.

Факт размещения персональных данных в открытых реестрах в форме открытых данных не выводит их из-под режима обработки, предусмотренного Законом № 152-ФЗ. Следовательно, к обработке таких персональных данных продолжают применяться общие принципы, установленные ст. 5 Закона № 152-ФЗ.

Создание любых прецедентов, не регулируемых в рамках правового поля Закона №152-ФЗ, по мнению членов Консультативного совета, может привести к необратимым негативным последствиям для субъекта персональных данных в части нарушения его прав и законных интересов.