ИНСТИТУТ ИССЛЕДОВАНИЙ ИНТЕРНЕТА

АНАЛИЗ

возможных последствий и влияния Регламента Global Data Protection Regulation (GDPR) Европейского Союза на бизнес российских операторов персональных данных (телекоммуникационные компании, интернет-компании) предоставляющих услуги через интернет для лиц в странах ЕС в контексте действующего и вступающего с силу регулирования в Российской Федерации

Москва, 2017

Содержание

Введение

В настоящее время на развитие отрасли связи, в том числе ниши интернет-провайдеров в Российской Федерации оказывает существенное влияние разработка и применение законодательства в области сбора и хранения данных пользователей услуг связи, прежде всего – телекоммуникационных услуг, в том числе передачи данных в сети Интернет.

Принятый 6 июля 2016 г. «Пакет Яровой» (ФЗ №374, ФЗ №375) обязывает операторов связи и организаторов распространения информации хранить не только метаданные, но и (до 6 месяцев) непосредственно данные, передаваемые пользователями в рамках телекоммуникационных услуг, - существенная часть таких данных является персональными данными.

В рамках выполненной Институтом исследований интернета НИР по теме «Зарубежный опыт нормативно-правового регулирования деятельности операторов связи в области сбора и хранения данных пользователей телекоммуникационных услуг (Telecommunications Data Retention Legislation) в контексте деятельности государственных правоохранительных органов» эксперты Института исследований интернета отметили, что принятый Регламент GDPR является одним из весомых оснований для отмены или корректировки странами Евросоюза нормативно-правового регулирования деятельности операторов связи и интернет-компаний в области сбора и хранения данных пользователей телекоммуникационных услуг (Telecommunications Data Retention Legislation).

При этом, в результате проведённого анализа было установлено, что регулирование деятельности операторов связи и интернет-компаний в области сбора и хранения данных пользователей телекоммуникационных услуг и интернет-сервисов в Российской Федерации является наиболее непроработанным и потенциально нарушает нормы международного права, в

частности принятый Регламент Global Data Protection Regulation (GDPR) Европейского Союза.

Настоящая работа направлена на анализ и моделирование возможных последствий вступления в силу в мае 2018 года Регламента Global Data Protection Regulation (GDPR) Европейского Союза для российских операторов персональных данных (телекоммуникационных компаний, интернет-компаний) предоставляющих услуги через интернет для лиц в странах ЕС, в контексте действующего и вступающего с силу регулирования в Российской Федерации.

1. Общие положения

Правовое регулирование защиты персональных данных в Европейском Союзе фактически насчитывает более 20 лет и правомерно связывается с соответствующей «европейской моделью», формирование и использование которой стало возможным в рамках европейского регионального интеграционного объединения, обладающего «наднациональными» характеристиками. Система «европейской модели» основана на нормативно-правовом и организационном (институциональном) механизмах порядка и процедур защиты персональных данных.

Нормативно-правовой механизм, с одной стороны, охватывает документы руководящих органов Европейского Союза (директивы, регламенты), набор базовых принципов основных прав субъектов данных и т.д., с другой стороны, имплементирована в национальное право стран-членов Европейского Союза. Основу нормативно-правового механизма порядка и процедур защиты персональных данных составляют документы, принимаемые Европейским Парламентом и Европейским Советом – директивы (*Directive*) и регламенты (*Regulation*). Правовая природа и формально-юридический порядок применения директив и регламентов Европейского Парламента и Совета, различны. Так, нормативные документы Европейского Союза, принятые в форме регламента, в отличие от директив, *непосредственно* применяются в государствах-членах Европейского Союза и не требуют имплементации в национальное право государств-членов.

Сказанное делает понятным, что правовое регулирование защиты персональных данных в Европейском Союзе, начиная с 2016 г. получило новый импульс развития. Это связано с принятием в апреле 2016 г. Регламента (ЕС) 2016/679 Европейского Парламента и Совета «О защите физических лиц в отношении обработки персональных данных и о

свободном перемещении таких данных и отмене Директивы 95/46/ ЕС (Общие положения о защите данных)»[1].

Регламент (ЕС) 2016/679 (далее – «Регламент GDPR»), *de facto* и *de facto jure* является документом прямого действия, что означает в практическом плане следующее.

Во-первых, Регламент GDPR выступает не только как регулирующий механизм для государств-членов Евросоюза, непосредственно влияющий и на уровень правотворчества и на уровень правоприменения. В связи с тем, что Регламент GDPR направлен на гармонизацию защиты основных прав и свобод физических лиц в отношении обработки данных и обеспечения свободного перемещения персональных данных между государствами-членами Евросоюза, Регламент GDPR обязывает государства-членов гармонизировать и уровень правотворчества, и уровень правоприменения.

На уровне правотворчества государства-члены Евросоюза обязаны гармонизировать с Регламентом GDPR свое национальное право посредством принятия, изменения, дополнения своего национального права.

На уровне правоприменения в рамках юрисдикции государств-членов Евросоюза Регламент GDPR непосредственно применяется национальными судами государств-членов. Более того, Регламент GDPR закрепляет номы о том, что государства-члены обязаны гармонизировать воздействие административных наказаний за нарушения Регламента GDPR.

Во-вторых, Регламент GDPR непосредственно применяется Судом справедливости Евросоюза (*European Court of Justic*), решения которого обладают прецедентным характером.

[1] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).*

2. Территориальная применимость Регламента (Global Data Protection Regulation, GDPR), начало действия Регламента GDPR, основные требования Регламента GDPR к защите персональных данных

В соответствии со Статьей 99 Регламента GDPR, он вступил в силу в мае 2016 г., а его применение начнется с 25 мая 2018 г., как обязательный нормативно-правовой документ, подлежащий прямому применению в государствах-членах Евросоюза. Основные положения и требования Регламента GDPR закреплены в преамбуле, содержащей 173 пункта, и в 99 статьях.

Регламент GDPR устанавливает цели, принципы, общие правила защиты физических лиц в отношении обработки персональных данных, их свободного перемещения в рамках Евросоюза, включая трансграничную передачу данных. Регламент GDPR закрепляет в том числе следующие принципы обработки персональных данных. Персональные данные должны:

– быть обработаны правомерно, справедливо и прозрачно в отношении субъекта данных («принцип законности, справедливости и прозрачности»);

– быть собраны для определенных, четких и законных целей и в дальнейшем не обрабатываться способом, несовместимым с этими целями; дальнейшая обработка данных для архивных целей, в интересах общества, научных и исторических исследований или статистических целей, не рассматривается как несовместимая с первоначальным целям («принцип целевого сбора данных»);

– быть обработаны адекватно и ограничиваться целями, для которых они обрабатываются (принцип «минимизации данных»);

– быть обработаны точно и там, где это необходимо, а также должны обновляться; должны приниматься все разумные меры для гарантии того, что персональные данные, которые являются неточными, с учетом целей, для которых они обрабатываются, будут удалены или исправлены без задержки (принцип «точности»);

– храниться в форме, позволяющей идентифицировать субъекта данных, не дольше, чем это необходимо для целей, для которых персональные данные обрабатываются; персональные данные могут храниться в течение более длительных периодов, т.к. персональные данные могут обрабатываться только для архивных целей в интересах общества, научных или исторических исследовательских целей или для целей статистики, с учетом осуществления соответствующих технических и организационных мер («принцип ограничения хранения данных»);

– быть обработаны таким образом, чтобы обеспечить надлежащую сохранность персональных данных, включая защиту от несанкционированной или незаконной обработки и случайной потери, уничтожения или повреждения, с использованием соответствующих технических или организационных мер («принцип целостности и конфиденциальности»).

Правомерность обработки данных оценивается исходя из следующих требований и условий:

– субъект данных дал согласие на обработку его персональных данных для одного или более конкретных целей;

– обработка необходима для исполнения договора, стороной которого субъект данных является стороной или для принятия мер по просьбе субъекта данных до заключения контракта;

– обработка необходима для соблюдения соответствующих обязательств контроллера;

– обработка необходима для защиты жизненных интересов субъекта данных или другого физического лица;

– обработка необходима для выполнения определенных задач и осуществляется в общественных интересах или для исполнении функций контроллера;

– обработка необходима для законных целей и интересов регулятора третьих лиц.

Регламент GDPR отменяет действующую в настоящее время Директиву 95/46/ЕС Европейского Парламента и Совета от 24 октября 1995 об обеспечении отдельных лиц в отношении обработки их персональных данных и свободном перемещении таких данных[2] и заменяет ее.

Согласно Статье 29 названной Директивы 95/46/ ЕС была учреждена Рабочая группа по защите физических лиц при обработке персональных данных (*Data Protection Working Party, WP29*)[3]. Рабочая группа по защите физических лиц при обработке персональных данных (далее – «Рабочая группа *WP29*») действует в настоящее время, разрабатывая разъяснения и рекомендации по различным аспектам будущего применения Регламента GDPR[4].

Деятельность Рабочей группы *WP29* прекратится 25 мая 2018 г., в связи с отменой Директивы 95/46/ ЕС. При этом с этой даты, т.е. с 25 мая 2018 г., начинает функционировать вновь созданный орган Евросоюза – Европейский совет по защите данных (*European Data Protection Board, EDPB*), который учрежден в соответствии с Регламентом GDPR. В организационном плане этот орган будет включать руководителя Европейской службы по защите данных и старших представителей Национальных органов по защите данных (*Data Protection Authorities*) стран-участниц Евросоюза (Статья 94 Регламента GDPR).

Компетенция Европейского совета по защите данных будут связаны с:

– подготовкой заключений и руководящих положений относительно единообразного применения Регламента GDPR;

– подготовкой заключений и отчетов в сфере защиты данных для Европейской Комиссии;

---

[2] *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.*

[3] См. например, URL:https://www.iabeurope.eu/policy/data-protection/the-wp29-will-become-the-edpb-but-what-does-that-mean/

[4] В числе первых подобных разъяснений можно назвать документы, принятые в апреле 2017 г., который касались, в частности, Европейского инспектора по защите данных (*European Data Protection Supervisor*), механизма «единого окна» (*one-stop-shop mechanism*). О последующих документах см., например, http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

– осуществлением ключевой роли в реализации «механизма единого окна» (*находится в стадии уточнения регулирования*).

В контексте содержания Регламента GDPR к субъектам, осуществляющим «обработку» «персональных данных», относятся «контролер» и «обработчик».

«Персональные данные» (*personal data*) – означают любую информацию, относящуюся к идентифицированному или идентифицируемому физическому лицу («субъект данных»); идентифицируемое физическое лицо является лицом, которое может быть идентифицировано прямо или косвенно, в частности, на основе идентификационной информации, такой как имя, идентификационный номер, данные о местоположении, идентификатор в интернете (онлайн-идентификатор) или посредством одного или нескольких показателей, характерных для физической, физиологической, генетической, умственной, экономической, культурной или социальной идентичности данного физического лица;

«Обработка» (*processing*) означает любую операцию или набор операций, которые совершаются с персональными данными или набором персональных данных, с использованием автоматизированных средств и без таковых, в числе которых сбор, запись, организация, структурирование, хранение, переработка или изменение, поиск и выборка, экспертиза, использование, раскрытие посредством передачи, рассылка или иной способ предоставления для доступа, группировка или комбинирование, отбор, стирание или уничтожение (Статья 4 Регламента GDPR).

«Контролер» (*controller*) – это физическое или юридическое лицо, государственный орган, агентство или иной орган, который самостоятельно или совместно с другими, определяет цели и средства обработки персональных данных (Статья 4 Регламента GDPR).

Регламент GDPR закрепляет, что контролёр обязан: в определенных случаях сотрудничать с обработчиками данных; вести учетную

документацию; осуществлять оценку воздействия обработки персональных данных на права субъектов данных для некоторых видов обработки данных; внедрять механизмы защиты данных; в момент сбора персональных данных предоставлять субъектам данных полную информацию о целях сбора персональных данных, о правах субъектов данных и т.д.; обязаны, по возможности, в течение 72 часов уведомлять национальные органы по защите данных (*Data Protection Authorities*) об обнаружении утечек персональных данных, и соответствующих субъектов персональных данных[5].

«Обработчик» (*processor*) – это физическое или юридическое лицо, государственный орган, агентство или иной орган, который обрабатывает персональные данные от имени и по поручению контролёра. Обработчик обязан: вести письменный реестр операций по обработке персональных данных, выполненных от имени и по поручению каждого контролёра; если у обработчика нет представителя в Евросоюзе, он обязан назначить такое лицо в определенных случаях; без задержек уведомлять контролёра об утечках персональных данных; участвовать в деятельности по трансграничной передаче данных.

Кроме того, контролёры и обработчики, в рамках своих программ отчетности обязаны назначить инспектора по защите данных (*Data Protection Officer*). Согласно Регламенту GDPR, инспектор по защите данных в обязательном порядке назначается в следующих случаях:

– обработка данных осуществляется государственным органом;

– основная деятельность контролёра или обработчика связана с такой обработкой данных, которая по своему охвату, целям и сути, требует крупномасштабного, регулярного и систематического мониторинга субъектов данных; при обработке специальной категории данных.

Территориальная сфера применения непосредственно закреплена в Статье 3 Регламента GDPR. Территориальная сфера применения

[5] В настоящее время находится в стадии уточнения регулирования Рабочей группы WP29.

ограничивается переделами Европейского Союза, однако юрисдикционно действие Регламента GDPR распространяется на субъектов за пределами Европейского Союза.

В целях обеспечения того, чтобы физические лица не были лишены защиты, на которую они имеют право в соответствии с Регламентом GDPR, обработка персональных данных субъектов данных в Евросоюзе контролёром или обработчиком, которые не учреждены в Евросоюзе, подпадает под действие Регламента GDPR в случаях, когда:

а) обработка персональных данных субъектов данных в Евросоюзе связана с предложением товаров или услуг субъектам данных в Евросоюзе, независимо от того, связано это с их с оплатой или нет. При этом Регламент GDPR устанавливает, что признаками, которые с очевидностью свидетельствуют о намерении предлагать товары или услуги субъектам данных в Евросоюзе, являются:

– использование языка или валюты, обычно используемой в одном или нескольких государствах-членах, с возможностью заказывать товары и услуги на этом языке;

– упоминание потребителей или пользователей, которые находятся в Евросоюзе (пункт (23) Преамбулы Регламента GDPR);

б) обработка персональных данных субъектов данных, находящихся в Евросоюзе также является предметом регулирования Регламента GDPR, когда это связано с мониторингом действий/поведения субъектов данных в Евросоюзе, постольку, поскольку их действия совершаются на территории Евросоюза. Для того, чтобы определить, подпадает ли деятельность по обработке данных для целей мониторинга действий субъекта данных, устанавливается факт того, осуществляют ли физические лица деятельность в интернете, в том числе потенциальную возможность последовательного использования технологии обработки персональных данных и т.д. (пункт (24) Преамбулы Регламента GDPR).

3. Соотношение норм Регламента GDPR и Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных (ETS-108), иных международных соглашений в области защиты ПД

Соотношение норм Регламента GDPR, Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных (ETS-108) и иных международных соглашений в области защиты персональных данных.

Регламент GDPR согласован с положениями целого ряда международно-правовых актов и документов как универсального, так и регионального и билатерального характера, речь в том числе идет о:

– Хартии Европейского Евросоюза об основных правах;

– Конвенции Совета Европы от 28 января 1981 г. о защите физических лиц при автоматизированной обработке персональных данных и Дополнительного протокола к Конвенции;

– Европейской Конвенции о защите прав человека и основных свобод;

– Женевских Конвенциях, связанные с соблюдением международного гуманитарного права, применяемого в период вооружённых конфликтов

– действующих договорах государств-членов Европейского Союза о взаимной правовой помощи и правовых отношениях по гражданским, семейным и уголовным делам.

Регламент GDPR исходит из того, что в отношении защиты персональных данных, трансграничной передачи данных в третью страну, международную организацию, Европейская Комиссия должна принимать во внимание, не только, к примеру, участие, присоединение третьей страны к Конвенции Совета Европы от 28 января 1981 г. о защите физических лиц при автоматизированной обработке персональных данных и к Дополнительному протокол, а также участие третьей страны или международной организации в многосторонних или региональных системах в отношении защиты

персональных данных, а также исполнение таких международных обязательств. Международные обязательства третьих стран или международных организаций принимаются во внимание Европейской Комиссией, в том числе для приятия решения о трансграничной передаче персональных данных в третью страну (пункт (105) Преамбулы Регламента GDPR).

4. Нормы Регламента GDPR, распространяющиеся на российских операторов персональных данных (телекоммуникационные компании, интернет-компании) предоставляющих услуги через интернет для лиц в странах ЕС

Регламент GDPR распространяется на российских операторов персональных данных (телекоммуникационные компании, интернет-компании) как на компании, не учреждённые в Евросоюзе, но обрабатывающие персональные данные находящихся в Евросоюзе субъектов данных, если их деятельность по обработке данных связана с предложением товаров и услуг таким субъектам данных в Евросоюзе, вне зависимости от того, требуется ли оплата от субъекта данных, либо связана с мониторингом деятельности субъектов данных постольку, поскольку она осуществляется в Евросоюзе.

В практическом плане сказанное означает, во-первых, что на российские компании, «ориентированные» на субъектов в Евросоюзе (потребители Евросоюза), после 26 мая 2018 г. окажутся в сфере действия Регламента GDPR. В этой связи, согласно требованиям Регламента GDPR, во-вторых, такие компании должны назначить своего представителя в Евросоюзе (пункт (80) Преамбулы Регламента GDPR).

Представитель (*representative*) – это физическое или юридическое лицо, созданное в Евросоюзе, которое специально уполномочено в письменной форме контролёром или обработчиком и представляет контролёра или обработчика, в отношении их соответствующих обязательств, предусмотренных Регламентом (Статья 4 Регламента GDPR). Порядок и основные функции представителя регулируются Статьей 27 Регламента GDPR.

Представитель может не назначаться, в частности, когда обработка носит случайный характер, не включает в себя масштабную обработку конкретных категорий персональных данных, либо обработка персональных

данных, связана с уголовными приговорами и правонарушениями, или если контролёр является органом или учреждением государственной власти.

Представитель должен действовать от имени контролёра или обработчика, может взаимодействовать с любыми компетентными органами Евросоюза, государства-члена, включая надзорные органы. Представитель должен быть специально уполномочен, посредством письменного предписания контролёра или обработчика, действовать от их имени в отношении их обязательств, вытекающих из Регламента GDPR. Назначение такого представителя не влияет на ответственность или обязанности контролёра или обработчика вытекающие из Регламента GDPR.

Представитель должен выполнять свои задачи согласно предписанию, полученному от контролёра или обработчика, и осуществлять любые действия в целях обеспечения соблюдения Регламента GDPR. Представитель подпадает под действие исполнительного производства в случае несоблюдения требований Регламента GDPR контролёром или обработчиком.

Если у российских операторов персональных данных (телекоммуникационных компаний, интернет-компаний), к примеру, предоставляющие услуги через интернет для лиц в странах Евросоюза, есть представительства и филиалы в странах Евросоюза, то функции представителя могут быть возложены на них.

Регламент GDPR при регулировании отношений, связанных со сбором и хранением персональных данных субъектов данных исходит из обязательного требования получения «согласия» (*consent*) субъекта на обработку персональных данных. Согласие должно быть настолько же легко отозвать, как и предоставить, а для специальных категорий данных согласие должно быть явно выраженным. В Преамбуле Регламента GDPR разъясняется, что согласие не считается добровольным, если субъект данных не имеет подлинного и свободного выбора либо возможности отказать в предоставлении согласия или отозвать согласие без ущерба для себя.

Контролёр данных обязан быть в состоянии предоставить доказательства получения согласия.

5. Нормативные требования действующего российского законодательства, в контексте возможных коллизий с нормами Регламента GDPR

Представляется, что настоящее время преждевременно анализировать возможные коллизии между нормативными требованиями действующего российского законодательства, и нормами Регламента GDPR. Это связано, прежде всего, с отмеченными ранее факторами.

Во-первых, предполагается принятие целого ряда разъяснительных и директивных документов применения Регламента GDPR Рабочей группой *WP29*. Во-вторых, несмотря на непосредственное действие Регламента GDPR в государствах-членах Евросоюза, на государства-члены возложена обязанность «трансформировать» национальное право к требованиям Регламента GDPR, включая «переходные положения»[6].

Во-вторых, после мая 2018 г. начнет формироваться национальная правоприменительная (судебная, административная) практика. Кроме того, т.к. Регламент GDPR непосредственно будет применяться Судом справедливости Евросоюза (*European Court of Justic*), после мая 2018 г. также начнет формироваться практика Суда справедливости.

В действующем российском законодательстве в регулировании отношений в сфере персональных данных системообразующим актом является Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ, с поправками Федерального закон № 242-ФЗ 2015 г. (далее – «ФЗ РФ о персональных данных»). В этой связи целесообразно обратить внимание на то, что Регламент GDPR и ФЗ РФ о персональных данных имеют различное действие в пространстве, по кругу лиц, и во времени.

[6] Первые законодательные акты приняты в таких странах-членах Евросоюза как Германия, Польша, Нидерланды. См., например, URL: https://www.datastax.com/resources/whitepapers/eu-gdpr-a-pocket-guide-a-clear-concise-primer-on-the-eu-gdpr-German?utm_campaign=GDPR_DACH_connectcom&utm_medium=cpc&utm_source=Google&utm_content=gdpr&gclid=CjwKEAjwruPNBRCKkbL9zqKcrHwSJABGDVyI_LtgAW9GE6IC4rXYELZE_fUqetX-fSp_0ijMK1Z9vBoCWUbw_wcB; URL: http://www.eversheds-sutherland.com/global/en/where/europe/ireland/services/data_protection/gdpr.page

ФЗ РФ о персональных данных не обладает экстерриториальным действием, не распространяется на нерезидентов, собирающих персональные данные российских граждан за границей, в случае, если они не осуществляют деятельность в интернете, направленную на Российскую Федерацию.

В контексте содержания Регламента GDPR субъектами, осуществляющим обработку персональных данных являются «контролер» и «обработчик», а в терминологии ФЗ РФ о персональных данных – «оператор». «Оператор» – 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 (пункт 2 Статьи 3 ФЗ № 152-ФЗ «О персональных данных»).

«Европейская модель» защищает персональные данные как основное право человека, является нейтральной к «национальному признаку». Право на защиту персональных данных, согласно Регламенту GDPR, осуществляется на территории Евросоюза и в государствах-членах независимо от гражданства или проживания, тем самым не ограничивается сфера действия права о персональных данных по «национальному принципу»[7].

ФЗ РФ о персональных данных распространяется на граждан Российской Федерации, что в том числе следует из нормативных положений Федерального закона от 21.07.2014 № 242-ФЗ (в редакции от 31.12.2014) «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях».

[7] См., к примеру, см. материалы Рабочей группы *WP29* о приемлемости защиты лиц, проживающих в ЕС. https://www.google.ru/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0ahUKEwiQoarl_qjWAhUsCZoKHRiDCIUQFggxMAE&url=http%3A%2F%2Fec.europa.eu%2Fnewsroom%2Fdocument.cfm%3Fdoc_id%3D43823&usg=AFQjCNEmByOWl_41poQ-zIX4TWGpzxqhMA

1) ФЗ №149-ФЗ (в редакции от 31.12.2014) «Об информации, информационных технологиях и о защите информации» дополнено нормой части 4 Статьи 16: «нахождение на территории Российской Федерации баз данных информации, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение *персональных данных граждан Российской Федерации*».

2) ФЗ № 152-ФЗ «О персональных данных» дополнено, в частности:

– частью 5 Статьи 18: «При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети «Интернет», оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных *данных граждан Российской Федерации* с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в пунктах 2, 3, 4, 8 части 1 статьи 6 настоящего Федерального закона»;

– частью 3 Статьи 22: «сведения о месте нахождения базы данных информации, содержащей персональные данные граждан Российской Федерации» (пункт 10.1).

Таким образом, сбор персональных данных и их защита связана с гражданами России, т.е. сфера применения законов о персональных данных в российском праве ограничена «по национальному принципу». При этом на практике сложно, а порой невозможно, российскому оператору данных, в частности при обработке персональных, полученных через интернет, определить гражданство субъекта данных. Как правило, интернет-услуги не предоставляются «по национальному признаку», даже если регистрационные формы могут содержать графу о гражданстве пользователя, проверить достоверность предоставленной информации по общему правилу не представляется возможным.

Роскомнадзор *de facto* «переложил» бремя идентификации гражданства субъекта данных на обработчиков данных. Поскольку

определение способов идентификации гражданства субъекта данных может быть различным, скорее всего российские операторы данных будут собирать все персональные данные субъектов данных на территории России с тем, чтобы выполнить требования российского права.

ФЗ № 242-ФЗ 2015 г. (в редакции от 29.07.2017 г.) предусматривает новые требования защиты персональных данных, связанные с локализацией данных[8]. Требования к регулированию сферы защиты персональных данных, связанные с локализацией данных относятся к следующему кругу лиц:

– российские юридические лица;

– иностранные компании, у которых есть филиалы/представительства в Российской Федерации;

– иностранные компании, осуществляющие деятельность в интернете, направленную на Российскую Федерацию, если они, к примеру, используют доменные имена в зоне .ru, .рф; имеют русскоязычный сайт; используют рекламу на русском языке и т.д.).

Временн***о***е требование ФЗ о персональных данных о локализации персональных данных распространяется на персональные данные, собранные или обрабатываемые после 1 сентября 2015 г. При этом, исходя из нормативных требований российского законодательства о персональных данных, связывающие защиту с принципом гражданства, достаточно сложно однозначно ответить на вопрос: распространяются ли требования к локализации данных к персональным данным российских граждан, собранных за пределами Российской Федерации. Представляется, что ответ на этот вопрос будет зависеть от вида обработки персональных данных.

По смыслу нормативных положений части 5 Статьи 18, объем обязательств по локализации данных «ограничен» тем, что при сборе персональных данных, в том числе посредством информационно-

[8] В общем плане требования локализации персональных данных согласуются с нормативными положениями Конвенции Совета Европы (№108) о защите частных лиц в отношении автоматической обработки персональных данных 1981 г. участником которой является Российская Федерация. См. также информацию URL:http://www.minsvyaz.ru/ru/personaldata

телекоммуникационной сети «Интернет», оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации…». Соответственно, в объем обязательств по локализации данных не подпадают, к примеру, такие виды обработки, как удаление, использование, распространение, псевдонимизация. Таким образом, формально-юридически обозначенные операции обработки могут осуществляться и быть локализованы вне пределов Российской Федерации.

Кроме того, в интересах оператора по обработке персональных данных могут действовать на договорно-правовой основе обработчики, которые не являются российскими лицами. В этих случаях лишь российский оператор обязан соблюдать требования о локализации, и требования локализации не распространяются на обработчиков данных, именно оператор данных, вне зависимости от области его деятельности, несет ответственность за локализацию[9].

Требования локализации данных, закрепленные ФЗ РФ о персональных данных, непосредственно связываются с таким важным аспектом как трансграничная передача персональных данных российских граждан. В контексте сопоставления ФЗ РФ о персональных данных и Регламента GDPR следует отметить следующее.

Регламент GDPR закрепляет понятие трансграничная обработка» (*cross-border processing*), которое означает: а) обработку персональных данных, которая имеет место в контексте деятельности учреждений в более чем одном государстве-члене контролёра или обработчика в Евросоюзе, в случае, если этот контролёр или обработчик учреждены в более чем одном государстве-члене; или б) обработку персональных данных, которая имеет

[9] Министерство связи и массовых коммуникаций Российской Федерации разъясняет вопросы, связанные с регулированием персональных данных и их локализацией, подготовленные на основании информации, полученной от представителей бизнеса, научного сообщества и органов государственной власти РФ (Совет Федерации РФ, Минкомсвязи РФ, Роскомнадзор). URL: http://minsvyaz.ru/ru/personaldata/

место в контексте деятельности единственного учреждения контролёра или обработчика в Евросоюзе, но которая существенно влияет или может существенно повлиять на субъектов данных в более чем одном государстве-члене.

Регламент GDPR регулирует порядок трансграничного перемещения персональных данных за пределы Евросоюза в Главе V «Передача персональных данных третьим странам или международным организациям».

В связи с тем, что о, что это может передача персональных данных может подвергнуть повышенному риску способность физических лиц осуществлять права на защиту данных, в том числе, защитить себя от неправомерного использования или разглашения информации, Регламент GDPR предусматривает, что в соответствии с ним, а также на основе взаимности применяются, в частности:

– механизм согласования;

– механизм сотрудничества между надзорными органами государств-членов и надзорными органами третьих государств;

– механизм взаимной помощи и совместные операции между соответствующими контролирующими органами на двусторонней или многосторонней основе.

С учетом того, что надзорные органы могут быть не в состоянии рассмотреть жалобу субъекта данных или провести расследование в отношении деятельности, осуществляемой за пределами границ своего государства-члена, их попытки сотрудничать в трансграничном контексте также могут быть затруднены недостаточными превентивными или полномочиями, связанными с исправлением ситуации, противоречивым режимом правового регулирования, а также препятствиями практического характера, например, ограничением источников сведений.

Передача персональных данных третьей стране или международной организации может иметь место, когда Европейская Комиссия приняла решение, что третья страна, территория, или один или несколько особых

секторов третьей страны, либо соответствующая международная организация обеспечивают надлежащий уровень гарантий. При этом Регламент GDPR закрепляет критерии оценки надлежащего уровня защиты, из которых должна исходить Европейская Комиссия при принятии решения (Статья 45 Регламента GDPR).

Если Европейская Комиссия будет обладать соответствующей информацией, что третья страна (территория, или один или несколько особых секторов третьей страны) либо международная организация не обеспечивают надлежащий уровень защиты, она вправе отменить, изменить или приостановить решение о передаче данных. Европейская Комиссия должна опубликовать в Официальном Журнале Европейского Союза[10], а также на своем веб-сайте список третьих стран (территорий и особых секторов третьей страны), а также международных организаций, в отношении которых она приняла решение о том, что надлежащий уровень защиты существует, либо не обеспечивается (пункт 8 Статьи 45 Регламента GDPR).

Согласно ФЗ РФ о персональных данных, в частности Статьи 12 ФЗ № 152, трансграничная передача персональных данных осуществляется в иностранные государства, которые являются сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, а также в иные иностранные государства, обеспечивающие адекватную защиту прав субъектов персональных данных. При том трансграничная передача персональных данных в иностранные государства может быть запрещена или ограничена в целях защиты основ конституционного строя Российской Федерации, нравственности, здоровья, прав и законных интересов граждан, обеспечения обороны страны и безопасности государства.

[10] *Official Journal of the European Union*

Роскомнадзор (уполномоченный орган РФ по защите прав субъектов персональных данных) утверждает перечень[11] иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных. Государство, не являющееся стороной Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, может быть включено в перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, при условии соответствия положениям указанной Конвенции действующих в соответствующем государстве норм права и применяемых мер безопасности персональных данных[12].

Один из наиболее важных аспектов требований российского законодательства локализации данных, в контексте трансграничной передачи персональных данных в иностранные государства связано с тем, что хранение данных (граждан РФ) должно быть локализовано на территории РФ, а при трансграничной передаче данные так или иначе будут храниться на сервере, расположенном за границей. При трансграничной передаче персональных данных он «не могут не подвергаться обработке», однако, с позиции официальных российских регуляторов, российские нормы локализации данных предназначены для предотвращения злоупотребления

[11] Приказ Роскомнадзора от 15.03.2013 № 274 (в редакции от 15.06.2017) «Об утверждении перечня иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных».

[12] В соответствии с Приказом Роскомнадзора № 274 от 15 марта 2013 года (в редакции 15.06.2017) среди таких стран: Австралия (Австралийский союз), Аргентинская Республика, Габонская Республика, Государство Израиль, Государство Катар, Канада, Королевство Марокко, Малайзия, Мексиканские Соединенные Штаты, Монголия, Новая Зеландия, Республика Ангола, Республика Бенин, Республика Кабо-Верде, Республика Казахстан, Республика Коста-Рика, Республика Корея, Республика Мали, Республика Перу, Республика Сингапур, Тунисская Республика, Республика Чили, Южно-Африканская Республика. Критерии, которые Роскомнадзор использует для оценки, формально-юридически не закреплены, к примеру, А. Савельев указывает на следующие: 1) наличие законодательства, основанного на тех же принципах, которые отражены в Конвенции СЕ № 108; 2) наличие специальной государственной администрации, ответственной за обеспечение безопасности, которая сотрудничает с Роскомнадзором, и 3) наличие ответственности за нарушение законодательства о персональных данных. См. Savelyev A. Russia's new personal data localization regulations: A step forward or a self-imposed sanction? https://pravo.hse.ru/data/2017/03/22/1169832328/2015%20Savelyev%20AI%20Russian%20New%20Personal%20Da..ward%20or%20a%20Self-Imposed%20Sanction.pdf

персональными данными российских граждан иностранными операторами данных и защиты российских граждан от надзора в иностранных государствах»[13].

Как отмечали некоторые российские эксперты, Роскомнадзору удалось найти решение, позволяющее осуществлять локализацию данных и трансграничную передачу персональных данных. Суть решения состоит в том, чтобы разделить все базы данных, которые могут содержать персональные данные, на две группы: первичные базы данных и другие базы данных»[14]. Так, персональные данные должны быть первоначально записаны, а также сохранены и обновлены на более позднем этапе, должны быть расположены в России («первичная база данных»); после этого информация из таких «первичных баз данных» может быть перенесена в базы данных, расположенные за пределами России («вторичные базы данных»), при условии соблюдения российского законодательства о персональных данных, связанных с трансграничной передачей. «Другими словами, главная копия личных данных российских граждан, собранных в России, должна быть расположена в России, а также как последующие обновления и дополнения к этим личным данным. Технические решения, в которых первичная база данных находится за рубежом, и создается только русская копия («копия» или «зеркало») такой зарубежной базы данных, не соответствуют закону»[15].

За несоблюдение российского законодательства о персональных данных, включая требования о локализации данных, предусматривается административная ответственность, которая с 1 июля 2017 г. существенно

[13] См. например, URL:http://tass.ru/obschestvo/2223739

[14] См., например, Savelyev A. Russia's new personal data localization regulations: A step forward or a self-imposed sanction? https://pravo.hse.ru/data/2017/03/22/1169832328/2015%20Savelyev%20AI%20Russian%20New%20Personal%20Da..ward%20or%20a%20Self-Imposed%20Sanction.pdf

[15] Savelyev A. Указ. Работа. Russia's new personal data localization regulations: A step forward or a self-imposed sanction? https://pravo.hse.ru/data/2017/03/22/1169832328/2015%20Savelyev%20AI%20Russian%20New%20Personal%20Da..ward%20or%20a%20Self-Imposed%20Sanction.pdf

изменена[16]. Статья 13.11. «Нарушение законодательства Российской Федерации в области персональных данных» Кодекса об административных правонарушениях предусматривает следующее:

1. Обработка персональных данных в случаях, не предусмотренных законодательством РФ в области персональных данных, либо обработка персональных данных, несовместимая с целями сбора персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи, если эти действия не содержат уголовно наказуемого деяния, влечет предупреждение или наложение административного штрафа на граждан в размере от 1 до 3 рублей; на должностных лиц – от 5 до 10 000 рублей; на юридических лиц – 30 000 до 50 000 рублей.

2. Обработка персональных данных без согласия в письменной форме субъекта персональных данных на обработку его персональных данных в случаях, когда такое согласие должно быть получено в соответствии с законодательством РФ в области персональных данных, если эти действия не содержат уголовно наказуемого деяния, либо обработка персональных данных с нарушением установленных законодательством РФ в области персональных данных требований к составу сведений, включаемых в согласие в письменной форме субъекта персональных данных на обработку его персональных данных, влечет наложение административного штрафа на граждан в размере от 3000 до 5000 рублей; на должностных лиц – 10000 до 20 000 рублей; на юридических лиц – 15 000 до 75 000 рублей.

3. Невыполнение оператором предусмотренной законодательством РФ в области персональных данных обязанности по опубликованию или обеспечению иным образом неограниченного доступа к документу, определяющему политику оператора в отношении обработки персональных данных, или сведениям о реализуемых требованиях к защите персональных данных, влечет предупреждение или наложение административного штрафа

[16] Федеральный закон от 07.02.2017 № 13-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях».

на граждан в размере от 700 до 1 000 пятисот рублей; на должностных лиц – от 3000 до 6 000 рублей; на индивидуальных предпринимателей – 5000 до 10 000 рублей; на юридических лиц – 15 000 до 30 000 рублей.

4. Невыполнение оператором предусмотренной законодательством РФ в области персональных данных обязанности по предоставлению субъекту персональных данных информации, касающейся обработки его персональных данных, влечет предупреждение или наложение административного штрафа на граждан в размере от 1 000 до 2 000 рублей; на должностных лиц – 4 000 до 6 000 рублей; на индивидуальных предпринимателей – 10 000 до 15 000 рублей; на юридических лиц – 20 000 до 40 000 рублей.

5. Невыполнение оператором в сроки, установленные законодательством РФ в области персональных данных, требования субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных об уточнении персональных данных, их блокировании или уничтожении в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, влечет предупреждение или наложение административного штрафа на граждан в размере от 1000 до 2 000 рублей; на должностных лиц – от 4 000 до 10 000 рублей; на индивидуальных предпринимателей – 10 000 до 20 000 рублей; на юридических лиц – 25 000 до 45 000 рублей.

6. Невыполнение оператором при обработке персональных данных без использования средств автоматизации обязанности по соблюдению условий, обеспечивающих в соответствии с законодательством РФ в области персональных данных сохранность персональных данных при хранении материальных носителей персональных данных и исключающих несанкционированный к ним доступ, если это повлекло неправомерный или случайный доступ к персональным данным, их уничтожение, изменение, блокирование, копирование, предоставление, распространение либо иные

неправомерные действия в отношении персональных данных, при отсутствии признаков уголовно наказуемого деяния влечет наложение административного штрафа на граждан в размере от 700 до 2 000 рублей; на должностных лиц – 4 000 до 10 000 рублей; на индивидуальных предпринимателей – 10 000 до 20 000 рублей; на юридических лиц – 25 000 до 50 000 рублей.

Таким образом, в российском законодательстве расширены и изменены виды правонарушений. Правонарушением является «незаконная обработка данных» (т.е. обработка не предусмотрена законом или не соответствующая целям сбора информации). В качестве подобного правонарушения может стать передача данных о сотрудниках третьим организациям в рекламных целях. Правонарушением считается «обработка данных без письменного согласия сотрудника». Самостоятельным видом правонарушения является «доступ к информации о политике компании в области обработки персональных данных». Правонарушением считается «сокрытие данных» (физическое лицо вправе запросить и получить информацию, связанную с обработкой его персональных данных, а если запрос лица не удовлетворен, это может квалифицироваться как правонарушение). Правонарушением является несоблюдение своевременной «корректировки данных», которая коррелирует нормативным положениям статьи 21 ФЗ о персональных данных. Обработчик данных обязан уточнять, уничтожать и т.д. данные о физических лицах. Неполная или устаревшей информация должна быть скорректирована в определенный срок. Обработчик данных обязан обеспечить «сохранность персональных данных», а в случае нарушения (получение несанкционированного доступа, уничтожение информации и т.д.) – это считается правонарушением

С 1 июля 2017 г. изменилась подведомственность дел при нарушении ФЗ о персональных данных: ранее дело, связанное с персональными данными, мог возбудить только прокурор, теперь дела об административных

правонарушениях могут быть инициированы в том числе должностными лицами Роскомнадзора.

Регламент GDPR закрепляет нормативные положения, предусматривающие принятие мер юридического характера компетентными надзорными органами Евросоюза и государств-членов, включая наложение административных штрафов. Административные штрафы и потенциальные санкции государств-членов (соответствующее законодательство в ряде государств ЕС формируется) за нарушение Регламента GDPR, выше, чем санкции за нарушения российского законодательства о персональных данных. Меры юридического характера принимаются компетентными надзорными органами Евросоюза и государств-членов в том числе на основании жалобы/заявления субъекта персональных данных (Преамбула (130) Регламент GDPR).

Для того, чтобы усилить обязательность соблюдения норм Регламент GDPR, санкции, в том числе административные штрафы, должны налагаться за любое его нарушение, в дополнение или вместо соответствующих мер, налагаемых надзорным органом государства-члена. В случае если нарушение незначительное или если вероятное наложение штраф может повлечь несоразмерную нагрузку для физического лица, вместо штрафа может быть объявлен выговор. При это принимается во внимание характер, тяжесть и продолжительность нарушения, преднамеренный характер нарушения, меры, принятые для смягчения нанесенного ущерба, степень ответственности или любые другие ранее совершенные нарушения, способ, посредством которого надзорному органу стало известно о нарушении, соблюдение мер, принятых в отношении контролёра или обработчика, соблюдение кодексов поведения, а также любые иные отягчающие или смягчающие вину обстоятельства. Для назначения наказаний, в том числе для наложения административных штрафов, необходимо наличие соответствующих процессуальных гарантий в соответствии с общими принципами права Евросоюза и Хартии Европейского Евросоюза об основных правах, включая эффективную

судебную защиту и надлежащую правовую процедуру. Государства-члены Евросоюза могут предусматривать уголовную ответственность за нарушение настоящего Регламента GDPR, включая нарушения национальных норм, принятых согласно и в соответствии Регламентом GDPR Регламента. (Преамбула (148)-(151), Статьи 58, 70, 83 Регламента GDPR).

Изложенное выше обобщенно свидетельствует о том, что Регламент GDPR и российское законодательство, регулирующее сферу персональных данных, имеют самостоятельную территориальную и «юрисдикционную» сферу применения; при этом некоторая общность подходов регулирования не дает основания сделать вывод относительно их «гармонизации». В практическом плане для российских компаний, деятельность которых связана со сферой персональных данных, ориентированных на пользователей в Евросоюзе, имеющих договорно-правовые обязательства с контрагентами Евросоюза, – это означает «двойное обременение».

5.1. Возможные риски и последствия нарушения норм Регламента GDPR для российских операторов персональных данных (интернет-компании и телекоммуникационные компании), предоставляющих услуги через интернет для лиц в странах ЕС

Возможные риски и последствия нарушения норм Регламента GDPR для российских операторов персональных данных (интернет-компании и телекоммуникационные компании), предоставляющих услуги через интернет для лиц в странах Евросоюза непосредственно связаны с тем, что Регламент GDPR закрепляет обязанности обработчиков данных. К числу прямых обязанностей относятся, к примеру:

– ведение письменного реестра операций по обработке персональных данных, осуществляемых от имени и по поручению каждого контролера;

– назначение своего представителя в Европейском Союзе (о котором было сказано ранее);

– представление уведомления об утечках персональных данных, по возможности 72 часов после обнаружения утечки[17];

– соблюдение целого ряда закрепленных механизмов, включая механизм сертификации[18];

– предоставление субъектам данных в момент сбора персональных данных транспарентную (прозрачную) информацию об обработке и о целях такой обработки;

– соблюдение норм, предусмотренных Статьей 83, которые подпадают под административные штрафы; при этом при наложении штрафов в порядке Статьи 83, всегда берется та сумма, которая больше (из двух сумм);

[17] В последней декаде 2017 г. ожидается принятие Рабочей группой по защите физических лиц при обработке персональных данных (*Data Protection Working Party, WP29*) Руководящих положений *WP29* по уведомлению об утечках данных.

[18] См. например, *Certifications, Seals and Marks under the GDPR and Their Roles as Accountability Tools and Cross-Border Data Transfer Mechanisms*
URL:https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_certifications_discussion_paper_12_april_2017.pdf

– представление доказательств о правомерности деятельности, связанной по обработке (т.е. бремя доказывания возлагается, по смыслу Регламента GDPR, на лиц, обрабатывающих персональные данные субъектов данных).

Избежать возможных рисков и последствий нарушения норм Регламента GDPR компания может посредством своевременного принятия мер, которые способны продемонстрировать соблюдение требований Регламента GDPR.

В их числе могут быть следующие:

1. Необходимо проанализировать операции по обработке данных на предмет добросовестности их осуществления, а также пересмотреть существующие формы уведомления субъекта данных. Это связано с тем, что Регламент GDPR обязывает предоставлять субъекту данных детализированную информацию: об обработке данных в момент ее сбора; целях обработки; о правах субъекта данных (необходимо, к примеру, указать право на отзыв согласия на обработку); о сроке хранения данных и др.

2. Разработать внутренние регламенты, определяющие политику компании в сфере обработки персональных данных, включая назначение инспектора по защите данных.

3. Осуществить «аудит», в случае наличия, действующих договоров с компаниями из Европейского Союза, на предмет правовых оснований обработки, использования, хранения и т.д. персональных данных. Это связано с тем, что Регламент GDPR предусматривает, наряду с согласием субъекта персональных данных на обработку, и иные правовые основания обработки. Правомерность обработки, к примеру, может вытекать из контрактных обязательств. Контрагенты из Европейского Союза могут потребовать внести изменения в существующие договоры для соблюдения требований Регламента GDPR. В этой связи следует, в том числе, решить вопрос: когда и как изменить (дополнить, отменить) условия действующих

договоров, кто будет нести бремя расходов, связанных с такими изменениями и проч.

4. Регламент GDPR предусматривает и регулирует порядок осуществления трансграничной (международной) передачи данных, включая условия и порядок перемещения персональных данных в третьи государства, в международные организации, а также в рамках группы компаний, осуществляющих совместную экономическую деятельность. При этом такая трансграничная передача данных не исключает портативности данных, «права на забвение» и иных прав субъектов данных. Соответственно, целесообразно проанализировать правомерность хранения персональных данных для обоснования того, что интересы компании (обрабатывающих персональные данные) обладают правомерной преимущественной силой по сравнению с правами субъектов данных, поскольку нередко субъекты данных обладают «завышенным пониманием» своих прав.

5. Регламент GDPR признает обязательный характер (в правовом значении) корпоративных кодексов поведения (*Binding corporate rules*), как регулирующий нормативный механизм «законной/правомерной» трансграничной передачи данных в рамках группы компаний/предприятий, осуществляющих совместную экономическую деятельность. Целесообразно проанализировать существующие (и утвержденные в будущем корпоративные кодексы поведения). Нередко корпоративные кодексы поведения (*Binding corporate rules*) рассматривают как «золотой стандарт» регулирования передачи данных в рамках трансграничной передачи данных в рамках группы компаний/предприятий.

5.2 Возможные риски последствия реализации Пакета Яровой (№374-ФЗ) для российских операторов персональных данных

Российское законодательство о персональных данных, в том числе, Федеральный закон от 06.07.2016 № 374-ФЗ и Федеральный закона от 06.07.2016 № 375-ФЗ, – имеют разную предметную сферу регулирования, самостоятельное действие в пространстве, по кругу лиц и во времени. При этом Федеральный закон от 06.07.2016 № 374-ФЗ и Федеральный закона от 06.07.2016 № 375-ФЗ (далее – «Пакет Яровой») относится к публично-правовой сфере; Регламент GDPR, преимущественно – к частноправовой сфере.

Российские операторы связи и организаторы распространения информации оказываются в условиях «двойного обременения»: исполнение требований российского права, с одной стороны, и исполнение норм тех юрисдикций, в рамках которых, в том числе, осуществляется их коммерческая деятельность – с другой.

Российские операторы связи и организаторы распространения информации обязаны выполнять требования законодательства, вытекающие из Федерального закона от 06.07.2016 N 374-ФЗ "О внесении изменений в Федеральный закон "О противодействии терроризму" и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности" (*Далее – «Пакет Яровой» (общеупотребимое*), которое вступит в силу с 1 июля 2018 г., постольку, поскольку его предметная сфера связана исключительно публично-правовой сферой, и касается реализации мер противодействия терроризму и обеспечения общественной безопасности в Российской Федерации. Нормы Пакета Яровой являются императивными, и их несоблюдение может повлечь применение соответствующих санкций.

Напомним, согласно Пакету Яровой, ФЗ «О связи» изменен и дополнен следующими нормами:

1) оператор связи обязан прекратить при поступлении соответствующего запроса

от органа, осуществляющего оперативно-розыскную деятельность, оказание услуг связи в случае неподтверждения в течение пятнадцати суток соответствия персональных данных фактических пользователей сведениям, заявленным в абонентских договорах. (Статья 46 пункт 1);

2) операторы связи обязаны хранить на территории Российской Федерации:

– информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, текстовых сообщений, изображений, звуков, видео- или иных сообщений пользователей услугами связи - в течение трех лет с момента окончания осуществления таких действий;

– текстовые сообщения пользователей услугами связи, голосовую информацию, изображения, звуки, видео-, иные сообщения пользователей услугами связи - до шести месяцев с момента окончания их приема, передачи, доставки и (или) обработки. Порядок, сроки и объем хранения указанной в настоящем подпункте информации устанавливаются Правительством Российской Федерации (пункт 1 Статьи 64);

– операторы связи обязаны предоставлять уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации, указанную информацию, информацию о пользователях услугами связи и об оказанных им услугах связи и иную информацию, необходимую для выполнения возложенных на эти органы задач, в случаях, установленных федеральными законами (пункт 1.1. Статьи 64).

Пакет Яровой внес изменения и дополнения в ФЗ №149-ФЗ «Об информации, информационных технологиях и о защите информации», а именно в Статью 10.1 следующего содержания:

1) организатор распространения информации в сети «Интернет» обязан хранить на территории Российской Федерации:

– информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков, видео- или иных электронных сообщений пользователей сети «Интернет» и информацию об этих пользователях в течение одного года с момента окончания осуществления таких действий;

– текстовые сообщения пользователей сети «Интернет», голосовую информацию, изображения, звуки, видео-, иные электронные сообщения пользователей сети «Интернет» до шести месяцев с момента окончания их приема, передачи, доставки и (или) обработки. Порядок, сроки и объем хранения указанной в настоящем подпункте информации устанавливаются Правительством Российской Федерации (пункт 3);

2) организатор распространения информации в сети «Интернет» обязан предоставлять указанную в пункте 3 настоящей статьи информацию уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации, в случаях, установленных федеральными законами (пункт 3.1);

3) организатор распространения информации в сети «Интернет» обязан при использовании для приема, передачи, доставки и (или) обработки электронных сообщений пользователей сети «Интернет» дополнительного кодирования электронных сообщений и (или) при предоставлении пользователям сети «Интернет» возможности дополнительного кодирования электронных сообщений представлять в федеральный орган исполнительной власти в области обеспечения безопасности информацию, необходимую для декодирования принимаемых, передаваемых, доставляемых и (или) обрабатываемых электронных сообщений (пункт 4.1).

В той редакции Пакета Яровой, в которой приняты изменения и дополнения, связанные с деятельностью операторов связи и организаторов распространения информации, не ограничивается круг лиц, на который распространяются обозначенные выше нормы. В практическом плане это означает, что Пакет Яровой «по умолчанию» распространяется и на иностранные физические лица (иностранные граждане; граждане, проживающие на территории иностранных государств, иные лица, проживающие на территории иностранных государств).

В контексте императивного действия норм Пакета Яровой, российские операторы связи и организаторы распространения информации должны, в том числе, обеспечить сбор, обработку сообщений, хранение и т.д. на территории Российской Федерации соответствующей информации («локализация»), а также обязаны предоставить соответствующую информацию уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность или обеспечивающим безопасность Российской Федерации по их запросу.

При этом деятельность российских операторов связи и организаторов распространения информации, нередко связана с обработкой и хранением персональных данных физических лиц Европейского Союза. Поскольку Регламент GDPR не регулирует отношения, и не применяется к отношениям, связанным с защитой физических лиц при обработке персональных данных компетентными органами в целях «…предотвращения угроз общественной безопасности». (Преамбула (19) Регламента GDPR). В этой связи одновременно с Регламентом GDPR, в целях предупреждения, расследования, выявления или судебного рассмотрения уголовных преступлений, либо приведения в исполнение уголовных наказаний, включая обеспечение защиты и предотвращения угроз общественной безопасности, в Европейском Союзе принят специальный нормативно-правовой акт, а именно: Директива (ЕС) 2016/680 Европейского парламента и Совета от 27

апреля 2016 г. «О защите физических лиц в отношении обработки персональных данных компетентными органами в целях предотвращения, расследования, обнаружения или преследования уголовных наказаний и о свободном перемещении таких данных и отмене Рамочного Решения Совета ЕС 2008/977/ JHA»[19] (далее – «Директива (ЕС) 2016/680»).

Как было отмечено ранее, правовая природа директивы (*Directive*) предполагает принятие государствами-членами соответствующих имплементирующих национальных актов. При этом, в значении Директивы (ЕС) 2016/680, такие национальные акты должны быть приняты к 25 мая 2018 г. Какие акты примут государства-члены в настоящее время сказать определенно достаточно сложно, но именно Директива (ЕС) 2016/680 предметно в большей степени связана с предметной сферой «пакета Яровой».

Вместе с тем, Регламент GDPR закрепляет достаточно определенные параметры критериев обработки персональных данных, в случае если они в том числе, связаны с мерами безопасности.

Во-первых, Регламент GDPR содержит нормы, предусматривающие, что обработка персональных данных связанных «…с мерами безопасности», осуществляется только под контролем официального органа, либо когда обработка разрешена правом Евросоюза или государства-члена, предусматривающим соответствующие гарантии для прав и свобод субъектов данных (Статья 10 Регламента GDPR).

Во-вторых, Регламент GDPR исходит из того, что когда обработка персональных данных частными организациями попадает под его действие, должна существовать возможность для государств-членов ЕС ограничивать по закону осуществление отдельных обязанностей и прав, если такое ограничение представляет собой необходимую и соразмерную меру в демократическом обществе для защиты конкретных жизненных интересов,

[19] *Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data and repealing Council Framework Decision 2008/977/JHA*

включая общественную безопасность, … в том числе защиту и предотвращение угроз общественной безопасности, к примеру, в рамках борьбы с отмыванием доходов. (Преамбула (19) Регламента GDPR).

В-третьих, Регламент GDPR также предусматривает, что обработка персональных данных органами государственной власти, центрами реагирования на компьютерные чрезвычайные происшествия (*CERTs*), центрами реагирования на инциденты, связанные с компьютерной безопасностью (*CSIRTs*), поставщиками сетей электронных коммуникаций и услуг, а также поставщиками технологий и услуг по обеспечению безопасности является законным интересом соответствующего контролёра данных в той мере, в какой она необходима и соразмерна целям обеспечения сетевой и информационной безопасности, то есть способности сети или информационной системы противостоять, на заданном уровне достоверности, случайным событиям, незаконным или преднамеренным действиям, которые компрометируют доступность, подлинность, целостность и конфиденциальность сохранённых или переданных персональных данных, а также безопасность соответствующих услуг, переданных через указанные сети или системы. Такой законный интерес может включать в себя, к примеру, предотвращение несанкционированного доступа к сетям электронных коммуникаций и распространение вредоносного кода, а также пресечение сетевых атак и угроз для компьютерных и электронных систем связи. (Преамбула (49) Регламента GDPR).

Вышеизложенное дает основание сделать вывод о том, что государства-члены ЕС, при принятии ими соответствующих национальных актов, имплементирующих Директиву (ЕС) 2016/680, будут как минимум, исходить из тех норм, которые предусмотрены Регламентом GDPR, т.е. не «пойдут по пути» установления требований, аналогичных установленным «Пакетом Яровой», предусматривающего избыточное ужесточение регулирования порядка хранения данных с декларируемой целью обеспечения безопасности.

Минимизация рисков в «правовом поле», как коммерческих, так и некоммерческих (политических) российских операторов связи и организаторов распространения информации в контексте Пакета Яровой ФЗ практически невозможна[20], однако, потенциально в «правовом поле» влияние окажут:

– то, каким образом Правительство РФ определит порядок, сроки и объем хранения информации в подзаконных актах, которые еще не приняты, т.к. реализация Пакета Яровой увязана с рядом поручений Правительству в «целях минимизации возможных негативных последствий и рисков»;

– оспаривание в Конституционном Суде Пакета Яровой, с учетом того, каким образом будет формироваться правоприменительная практика, которая в настоящее время отсутствует.

Пакет Яровой, как отмечено ранее, изменяет и дополняет ФЗ № 149-Ф «*Об информации, информационных технологиях и о защите информации*», соответственно, требования по хранению данных распространяется на всех организаторов распространения информации, потенциально включая и иностранных операторов. С одной стороны, иностранные операторы (участвующие, к примеру, в обеспечении приема, передачи, доставки и/или обработки данных), будут обязаны соблюдать императивные требования Пакета Яровой, а это может привести к нарушению ими соответствующих норм иностранного права, прежде всего касающихся конфиденциальности персональных данных, получения согласия субъекта данных на обработку, целевую обработку данных и т.д. Такая ситуация, в свою очередь, может повлиять на сокращение присутствия иностранных компаний на российском рынке телекоммуникационных услуг (если не к полному их уходу).

С другой стороны, сети ряда российских операторов расположены за рубежом и российские компании находятся в договорно-правовых

[20] Реализация Пакета Яровой потребует от российских операторов связи и организаторов распространения информации сокращения прямых затрат, запуск новых сетей и сервисов, модернизацию существующих оборудования и т.д. В свою очередь, принятие мер экономического характера, могут оказаться непосильными для целого ряда компаний, что приведет, если не к «самоубийству» отрасли, то, несомненно, к сокращению интернет-компаний, увеличению тарифов.

отношениях с европейскими компаниями. Соблюдение российскими операторами требований Пакета Яровой о хранении данных (данные переписки, данные разговора между пользователями и т.д.) может привести к нарушению российским оператором не только условий заключенных договоров, но и законодательных норм, действующих в иностранном государстве, к примеру, тех же требований о конфиденциальности, которые значительно расширены в Регламенте GDPR. Как следствие, на российских операторов в юрисдикции государств-членов Евросоюза могут быть наложены значительные штрафные санкции, согласно Регламенту GDPR; иные меры юридического характера в соответствии с правом государств-членов, не говоря уже об ответственности, вытекающей из условий заключенных договоров. В итоге, это может привести к прекращению договорно-правовых отношений российских операторов с их иностранными контрагентами, сокращению их коммерческих возможностей и присутствия российских операторов в юрисдикции государств-членов Евросоюза[21].

В этой связи российским операторам связи и организаторам распространения информации для минимизации возможных рисков потребуется:

1. Осуществить аудит заключенных договоров (если таковые есть) с компаниями из государств-членов Евросоюза для приведения в соответствие условий договоров с требованиями Регламента GDPR, а также с учетом императивных требований норм Пакета Яровой;

[21] Помимо Пакета Яровой Российская Федерация может оказаться первой страной, которая избыточно ужесточает регулирование порядка «обмена сообщениями», т.к. инициировано внесение соответствующих изменений и поправок в ФЗ № 149-Ф «Об информации, информационных технологиях и о защите информации». При прохождении всех законодательных процедур, согласно изменениям и поправкам ФЗ № 149-Ф, с 1 января 2018 г. приложения обмена сообщениями, которые пока позволяют пользователям регистрироваться анонимно, будут, в том числе связаны с идентификацией пользователей См. подробнее, например, URL:http://www.globalprivacyblog.com/legislative-regulatory-developments/messaging-apps-may-face-new-obligations-in-russia/

2. Внести соответствующие изменения в действующие договоры с компаниями-контрагентами из стран Европейского Союза и распределить возможные финансовые затраты;
3. Назначить в рамках компании компетентное лицо (группу лиц), ответственных за мониторинг разъясняющих норм применения Регламента GDPR, включая подзаконные и имплементирующие акты, принятые в соответствии с настоящим Регламентом и с правом государств-членов Евросоюза для уточнения положений Регламента GDPR, которые в перспективе могут быть приняты государствами-членами Евросоюза и Комиссией Европейского Союза;
4. Назначить своего представителя в соответствующем государстве-члене Евросоюза для взаимодействия с национальными надзорными органами.

Отметим, что Регламент GDPR предусматривает, что в соответствии с правом государства-члена ответственность за его нарушения может быть соразмерно распределена в отношении ущерба, причинённого обработкой, контролёр или обработчик, которые заплатили полную компенсацию, может обратиться в суд с регрессным требованием относительно других контролёров или обработчиков, участвовавших в одной и той же обработке. (Преамбула (146) Регламента GDPR).

Как отмечалось ранее, Регламент GDPR юрисдикционно расширен и может применяться к российским операторам связи и организаторам распространения информации, которые не учреждены в Евросоюзе, но обрабатывают персональные данные находящихся в Евросоюзе субъектов данных, если их деятельность по обработке данных связана с предложением товаров и услуг таким субъектам данных в Евросоюзе, вне зависимости от того, требуется ли оплата от субъекта данных, либо связана с мониторингом деятельности субъектов данных постольку, поскольку она осуществляется в Евросоюзе.

Можно смоделировать следующую ситуацию. Субъект персональных данных из стран-членов Евросоюза, в соответствии с Регламентом GDPR хочет обжаловать действия российской компании-обработчика, связанные с обработкой его персональных данных, т.к. они обработаны без его согласия и такая обработка нанесла ему ущерб. Субъект данных вправе обратиться в соответствующий компетентный орган. Но даже если такой компетентный орган вынесет решений, оно не будет исполнимо на территории Российской Федерации, поскольку отсутствуют адекватных правовых механизмов, в том числе из-за отсутствия правовых договоров о правовой помощи.

Важным аспектом является то, что Регламент GDPR регулирует трансграничную передачу данных за пределы Евросоюза, что может подвергнуть повышенному риску способность физических лиц осуществлять права на защиту данных, в том числе, защитить себя от неправомерного использования или нарушение конфиденциальности. Надзорные органы Евросоюза могут быть не в состоянии рассмотреть жалобу или провести расследование в отношении деятельности, осуществляемой за пределами границ своего государства-члена. Их попытки сотрудничать в трансграничном контексте также могут быть затруднены недостаточными превентивными или полномочиями, связанными с исправлением ситуации, противоречивым режимом правового регулирования, а также препятствиями практического характера, например, ограничением источников сведений. Вследствие этого Регламент GDPR исходит из необходимости содействовать тесному сотрудничеству между надзорными органами по защите персональных данных для того, чтобы они могли обмениваться информацией и проводить расследования с надзорными органами других стран. В целях разработки механизмов международного сотрудничества для содействия и обеспечения международной взаимной помощи при исполнении законодательства о защите персональных данных, Европейская Комиссия и надзорные органы обмениваются информацией и сотрудничают в рамках

своей компетенции с компетентными органами в третьих странах на основе взаимности и в соответствии с Регламентом GDPR.

Европейская Комиссия, согласно Регламенту GDPR, вправе оценивать уровень защиты персональных данных в третьих странах, учитывать то, каким образом третья страна соблюдает принципы правового государства, обеспечивает доступность правосудия, так же, как и соблюдает нормы и стандарты международного права прав человека. Европейская Комиссия, согласно Регламенту GDPR, может принять решение о недостаточности мер защиты персональных данных в отношении третьей страны, если третья страна не предоставляет гарантии, обеспечивающие соответствующий уровень защиты, соразмерный уровню, гарантированному в Евросоюзе, эффективный независимый мониторинг защиты данных, не предусматривает механизмы сотрудничества с органами защиты данных государств-членов Евросоюза по защите данных, а субъектам данных должны не предоставляет административные и судебные средства защиты. В этом случае трансграничная передача данных такой третьей стране может быть запрещена. Статья 70 (s) Регламента GDPR возлагает определенные полномочия по этим вопросам на новый орган – Европейский совет по защите данных (*European Data Protection Board, EDPB*).

Пакет Яровой, а также предлагаемые изменения и дополнения действующего российского законодательства в сфере персональных данных могут потенциально привести к принятию решения о недостаточности мер защиты персональных данных в России. Если подобное решение будет принято в отношении России, минимизировать подобные риски российским операторам связи и организаторам распространения информации не удастся.