Информация для клиентов
Россия 2016: Персональные Данные и Кибербезопасность

МОСКВА
Дмитрий Никифоров
dvnikiforov@debevoise.com

Анна Максименко
avmaximenko@debevoise.com

Николай Киселев
nskiselev@debevoise.com

Елена Ключарева
emklutchareva@debevoise.com

В 2016 г. в России усилился контроль над исполнением требований о локализации персональных данных, появились дальнейшие разъяснения в этой сфере[1], была разработана стратегия дальнейшего развития законодательства о защите персональных данных и уделено внимание вопросам кибербезопасности.

ЛОКАЛИЗАЦИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ: ПЕРВЫЕ РЕЗУЛЬТАТЫ

1 сентября 2016 г. Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций Российской Федерации («Роскомнадзор») были опубликованы первые результаты практики применения требования о локализации персональных данных. Было отмечено, в частности, следующее:

- в Реестр нарушителей прав субъектов персональных данных («Реестр») внесен и заблокирован 161 Интернет-ресурс;
- нарушения требований о локализации составили 1,3% от всех нарушений, выявленных Роскомнадзором в ходе проверок (23 нарушения из 1822).

Основной мерой ответственности, которую Роскомнадзор применял за нарушения требования о локализации персональных данных, являлись предупреждения с требованием устранить нарушения.

[1] Требования о локализации хранения персональных данных были введены Федеральным законом от 21 июля 2014 г. № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-коммуникационных сетях» («Закон № 242») и вступили в силу 1 сентября 2015 г. В нем предусмотрено, что запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан России может осуществляться только с использованием баз данных, находящихся на территории Российской Федерации («локализация персональных данных»).

После получения предупреждения Роскомнадзора ряд компаний устранил нарушения.

ЛОКАЛИЗАЦИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ: РАЗЪЯСНЕНИЯ

9 ноября 2016 г. Роскомнадзор опубликовал разъяснения по некоторым вопросам локализации персональных данных. Разъяснения не имеют обязательной силы, однако Роскомнадзор может опираться на них при проведении проверок и принятии решений о наличии нарушений в данной сфере.

Ограничение доступа к Интернет-ресурсам, используемым для обработки персональных данных

В соответствии с Законом о персональных данных[2] ограничение доступа к Интернет-ресурсам вводится на основании решения суда. Это предоставляет оператору персональных данных возможность представить доказательства того, что обработка персональных данных осуществляется на законных основаниях.

Меры по ограничению доступа к Интернет-ресурсам могут быть приняты вследствие следующих нарушений[3] Закона о персональных данных:

- сбор персональных данных в базах данных, находящихся за рубежом;
- обработка персональных данных без согласия субъекта персональных данных;
- предоставление открытого доступа к находящимся в открытом доступе персональным данным в ином объеме и в иных целях, чем объем и цели первоначального сбора персональных данных;
- неопубликование оператором персональных данных положения о порядке обработки им персональных данных в сети Интернет.

Для установления компании-ответчика в спорах по ограничению доступа к Интернет-ресурсам Роскомнадзор использует сервис WHOIS[4].

---

[2] Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» («Закон о персональных данных»).

[3] Перечень не является исчерпывающим.

[4] Сервис WHOIS позволяет установить лицо, являющееся владельцем доменного имени. Определение ответчика в спорах по ограничению доступа к Интернет-ресурсам путем использования сервиса WHOIS было признано законным в нескольких судебных актах судов апелляционной и кассационной инстанций.

Роскомнадзор отметил, что прекращение работы Интернет-ресурса не является основанием для его исключения из Реестра. Интернет-ресурс может быть исключен из Реестра в случае, если были приняты меры по устранению нарушений или в случае, если суд принял решение об отмене соответствующего решения Роскомнадзора о включении Интернет-ресурса в Реестр.

Разъяснение значения терминов

Роскомнадзор разъяснил значение некоторых терминов, используемых в Законе о персональных данных, включая следующие:

- «*база данных*» означает систематизацию персональных данных независимо от материальных носителей и средств обработки (например, архивы, электронные базы данных, документы в формате MS Word и MS Excel и т.п.); перенос персональных данных из бумажных документов в электронную базу данных считается единым процессом, который должен осуществляться в России (например, если оператор персональных данных производит сбор персональных данных в бумажной форме в России, а затем переводит их в электронную базу за пределами России, оператор нарушает Закон о персональных данных);
- «*сбор персональных данных*» означает получение персональных данных непосредственно от субъекта персональных данных; данный процесс следует отличать от передачи персональных данных для дальнейшей обработки;
- законодательство не разделяет «*хранение персональных данных*» на постоянное и временное; использование подобных формулировок в согласии на обработку персональных данных является нарушением закона.

Трансграничная передача персональных данных

Требование о локализации персональных данных не устанавливает дополнительных ограничений на трансграничную передачу персональных данных, находящихся в России. Тем не менее, обновление персональных данных сначала должно осуществляться в базах данных, расположенных в России, и только затем данные могут быть переданы за рубеж. Параллельный ввод персональных данных в российскую и зарубежную базу данных противоречит требованиям Закона о персональных данных.

ОГРАНИЧЕНИЕ ДОСТУПА К САЙТАМ LINKEDIN

В 2016 г. доступ к сайтам LinkedIn[5] [6] был заблокирован для лиц, использующих российские IP-адреса[7]. Основанием для блокировки Сайтов LinkedIn стало, среди прочего, неисполнение со стороны LinkedIn требования о локализации хранения персональных данных и отсутствие согласия граждан на обработку LinkedIn их персональных данных.

Более подробные сведения о данном деле приведены в Приложении 1.

СТРАТЕГИЯ В ОБЛАСТИ ЗАЩИТЫ ПРАВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

31 марта 2016 г. Роскомнадзор принял Стратегию институционального развития и информационно-публичной деятельности в области защиты прав субъектов персональных данных на период до 2020 г. («Стратегия»). Положения Стратегии не имеют обязательной силы, и ее основной целью является определение направлений дальнейшей законотворческой и правоприменительной деятельности Роскомнадзора.

Стратегия предусматривает:

- развитие саморегулирования в сфере обработки персональных данных;
- учет отраслевой специфики, влияющей на обработку персональных данных;
- расширение деятельности Роскомнадзора в публичной сфере (например, реализация совместных проектов с профессиональными сообществами операторов персональных данных); и
- информационную прозрачность деятельности, имеющей целью усиление защиты персональных данных.

К числу приоритетных задач, предусмотренных Стратегией, отнесены, среди прочего:

---

5 LinkedIn Corporation («LinkedIn»).

6 Доменные имена, унифицированные локаторы ресурса (URL) и сетевые адреса следующих сайтов: http://www.linkedin.com и http://linkedin.com («Сайты LinkedIn»).

7 По имеющейся в открытом доступе информации, представители LinkedIn провели встречу с Роскомнадзором 8 декабря 2016 г. для обсуждения требований Роскомнадзора о локализации, в частности, разумных сроков осуществления локализации. В январе 2017 г. по требованию Роскомнадзора компании Apple и Google убрали приложение LinkedIn из своего российского магазина приложений.

- стимулирование соблюдения законодательства о персональных данных и совершенствование имеющихся механизмов регулирования (что должно привести к уменьшению нарушений в области обработки персональных данных на 30%); и
- совершенствование правоприменительного и методического инструментария (что должно привести к ежегодному уменьшению числа выявляемых нарушений на 2%).

ЗАКОНОПРОЕКТЫ О БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ В РОССИИ

6 декабря 2016 г. на рассмотрение в Государственную Думу РФ были внесены Законопроект № 47571-7 «О безопасности критической информационной инфраструктуры Российской Федерации» и сопутствующие Законопроекты № 47591-7 и № 47579-7 о внесении изменений в отдельные законодательные акты Российской Федерации в соответствии с Законопроектом № 47571-7 («Законопроекты»)[8].

В Законопроектах установлены основные принципы обеспечения безопасности критической информационной инфраструктуры («КИИ»)[9] России и определены права, обязанности и ответственность лиц, владеющих на праве собственности (ином законном основании) объектами КИИ, операторов связи и информационных систем, обеспечивающих взаимодействие этих объектов.

В Законопроектах имеются, помимо прочего, следующие предложения:

- создать для обеспечения безопасности объектов КИИ специальный реестр значимых объектов КИИ;
- обязать субъектов КИИ (в том числе юридических лиц-владельцев КИИ) информировать о компьютерных инцидентах и оказывать содействие соответствующим федеральным органам в обнаружении и предупреждении

---

8 С дополнительной информацией по Законопроектам можно ознакомиться по адресу: http://asozd2.duma.gov.ru/main.nsf/%28SpravkaNew%29?OpenAgent&RN=47571-7&02, http://asozd2.duma.gov.ru/main.nsf/%28SpravkaNew%29?OpenAgent&RN=47579-7&02, http://asozd2.duma.gov.ru/main.nsf/%28SpravkaNew%29?OpenAgent&RN=47591-7&02.

9 В соответствии с Законопроектом № 47571-7 в состав объектов КИИ входят, среди прочего, информационно-телекоммуникационные сети и системы государственных органов и информационно-телекоммуникационные сети и системы, действующие в оборонной отрасли, здравоохранении, на транспорте, в банковской сфере, в энергетике, топливной, атомной, горнодобывающей, металлургической, химической, ракетно-космической промышленности.

компьютерных атак, ликвидации их последствий, установлении причин и условий возникновения компьютерных инцидентов;

- дополнить главу 28 Уголовного кодекса РФ (*Преступления в сфере компьютерной информации*) новой статьей,
  - устанавливающей уголовную ответственность за неправомерное воздействие на КИИ России (в том числе за создание/распространение компьютерных программ или компьютерной информации, заведомо предназначенных для неправомерного воздействия на КИИ России, за неправомерный доступ к охраняемой компьютерной информации, содержащейся в КИИ России), и
  - предусматривающей наказание в зависимости от конкретного правонарушения в виде штрафа до 2 млн. рублей или лишения свободы на срок до 10 лет; и
- дополнить перечень сведений, составляющих государственную тайну, сведениями о мерах по обеспечению безопасности объектов КИИ, отнесенных к одной из категорий значимости, и сведениями об оценке степени защищенности КИИ России.

27 января 2017 г. Государственная Дума РФ приняла Законопроекты в первом чтении.

ДЕЯТЕЛЬНОСТЬ БАНКА РОССИИ

11 апреля 2016 г. Банк России выпустил Рекомендации в области стандартизации «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Предотвращение утечек информации».

В документе изложены, помимо прочего:

- предлагаемые к принятию меры для предотвращения возможных утечек конфиденциальной информации и рекомендации по реализации данных мер;
- рекомендации по поддержанию необходимого и достаточного уровня зрелости мониторинга и контроля возможных каналов утечки; и
- виды данных, рекомендуемых для включения в класс «информация конфиденциального характера».

Кроме того, в 2016 г. Банк России выступил с двумя важными инициативами:

- разработать меры воздействия на банки с низким уровнем информационной безопасности (конкретные меры в разработке); и,

- начиная с 2017 г., провести проверку и разработать регулирование в сфере дистанционных банковских сервисов, в частности:

  - провести тотальную проверку безопасности онлайн-банкинга для физических лиц и дистанционных платежных сервисов для юридических лиц;

  - ввести сертификацию таких дистанционных сервисов на соответствие требованиям информационной безопасности; и

  - закрепить требования, которым должны соответствовать дистанционные банковские сервисы, и оформить указанные требования в формате национальных стандартов.

Конкретные документы по реализации данных инициатив Банка России находятся в разработке.

Мы также ожидаем дальнейшего развития в сфере защиты персональных данных и локализации персональных данных, а также инициатив банковского сообщества в сфере кибербезопасности.

* * *

Если у вас возникнут какие-либо вопросы, просим вас обращаться к нам за разъяснениями.

ПРИЛОЖЕНИЕ 1

ДЕЛО LINKEDIN

Иск Роскомнадзора

16 июня 2016 году Роскомнадзор обратился в Таганский районный суд г. Москва с иском к LinkedIn в связи с ведением Сайтами LinkedIn незаконной деятельности по сбору, использованию и хранению персональных данных российских граждан. Роскомнадзор также ходатайствовал о включении Сайтов LinkedIn в Реестр.

Роскомнадзор привел следующие доводы:

- LinkedIn не осуществил локализации обработки персональных данных в соответствии с требованиями Закона о персональных данных[10], которым предусмотрено, что по общему правилу при сборе персональных данных (в том числе через сеть Интернет) оператор персональных данных обязан обеспечить запись, систематизацию, сбор, хранение, уточнение и извлечение персональных данных граждан России с использованием баз данных, находящихся на территории России;
- LinkedIn не получал согласия отдельных физических лиц на обработку их персональных данных в нарушение Закона о персональных данных[11], поскольку при синхронизации электронной почты и устройств пользователей LinkedIn также собирал и обрабатывал данные физических лиц, которые не являлись ни «участниками», ни «посетителями» соответствующих сайтов, и с точки зрения Роскомнадзора, не подпадали под действие пользовательского соглашения LinkedIn и других документов; и
- в соответствии с информацией, приведенной на Сайтах LinkedIn, ответственность за оказание услуг на сайте «linkedin.com» несет LinkedIn, находящийся за пределами России; кроме того, данное юридическое лицо является администратором доменного имени сайта «linkedin.com», в связи с чем данное лицо было признано ответчиком.

На этом этапе LinkedIn не участвовал в судебных заседаниях и не направил отзыва на иск.

---

[10] П. 5 ст. 18 Закона о персональных данных.

[11] П. 1 ст. 6 Закона о персональных данных.

4 августа 2016 г. Таганский районный суд г. Москвы, приняв во внимание преднамеренный характер деятельности LinkedIn по организации сбора персональных данных, вынес решение, которым признал факт нарушения LinkedIn Закона о персональных данных и соответствующих прав российских граждан на неприкосновенность частной жизни.

На основании этого Роскомнадзор внес Сайты LinkedIn в Реестр, вследствие чего доступ к Сайтам LinkedIn был ограничен.

Обжалование решения компанией LinkedIn

LinkedIn направил жалобу в Московский городской суд на решение Таганского районного суда г. Москва, в которой, помимо прочего, заявила, что:

- иск Роскомнадзора был предъявлен ненадлежащему юридическому лицу, поскольку обработкой персональных данных лиц, проживающих за пределами США, занимается не LinkedIn Corporation, а LinkedIn Ireland Unlimited Company[12];
- действие российского законодательства не распространяется на иностранные компании;
- факт нарушения прав субъектов персональных данных не доказан, поскольку жалобы российских граждан в отношении Сайтов LinkedIn представлены не были; и
- LinkedIn не был надлежащим образом уведомлен о времени и месте проведения заседания суда первой инстанции.

10 ноября 2016 г. Московский городской суд отказал в удовлетворении жалобы LinkedIn и оставил без изменений решение Таганского районного суда г. Москвы.

Позиция Роскомнадзора, поддержанная решением Московского городского суда, была основана, в частности, на следующих доводах:

- LinkedIn является оператором персональных данных, несущим ответственность за соблюдение Закона о персональных данных:

[12] В п. 1.2 Пользовательского соглашения LinkedIn от 23 октября 2014 г. указано, что в случае проживания физического лица за пределами США соглашение заключается между компанией LinkedIn Ireland Unlimited Company и соответствующим физическим лицом (https://www.linkedin.com/legal/user-agreement?trk=hb_ft_userag).

- в соответствии с информацией, приведенной на Сайтах LinkedIn, ответственность за оказание услуг на сайте «linkedin.com» несет LinkedIn и данное юридическое лицо является администратором доменного имени сайта «linkedin.com»;
- сайт «linkedin.com» размещен на технической платформе, расположенной в США и принадлежащей LinkedIn; и
- в соответствии с Законом о персональных данных[13] оператором персональных данных также является и юридическое лицо, среди прочего, организующее и (или) осуществляющее обработку персональных данных совместно с другими лицами.

- действие российского законодательства распространяется на LinkedIn:
  - в соответствии с Законом о защите информации[14] использование информационно-коммуникационных сетей на территории России осуществляется с соблюдением требований российского законодательства;
  - в соответствии с ГК РФ[15] выбор права, подлежащего применению к договору, не может повлечь за собой лишение потребителя защиты его прав, предоставляемой императивными нормами права страны места жительства потребителя, если контрагент потребителя (профессиональная сторона) любыми способами направляет свою деятельность на территорию страны места жительства потребителя;
  - LinkedIn направлял свою деятельность на территорию России, поскольку, в частности, (a) Сайты LinkedIn имеют версию на русском языке и предоставляют услуги по размещению рекламы на русском языке; (b) LinkedIn, являясь организацией, ведущей хозяйственную деятельность, понимает, что ограничение доступа к Сайтам LinkedIn в России затронет его интересы.

---

[13] В соответствии с п. 2 ст. 3 Закона о персональных данных оператором персональных данных является 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.

[14] П. 1 ст. 15 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» («Закон о защите информации»).

[15] П. 1 ст. 1212 Гражданского кодекса Российской Федерации (часть 3) от 26 ноября 2001 г. № 146-ФЗ («ГК РФ»).

На дату настоящей информации для клиентов доступ к Сайтам LinkedIn в России ограничен.