Эпоха нелегального бизнеса – торговля базами с паспортными данными россиян, их телефонами, номерами автомобилей, а также семейным, имущественным положением, доходами и историями болезни – в России, похоже, заканчивается.

.

«РГ» публикует поправки к Закону «О персональных данных».

Теперь граждане имеют право требовать возмещения морального вреда и убытков в случае потери, утечки, передачи персональной информации или нарушения правил ее обработки.

Документ ужесточает ответственность организаций за соблюдение защиты личной информации россиян. Напомним, принятый в 2006 году Федеральный закон «О персональных данных» предоставлял отсрочку по введению этой нормы до 1 января 2010 года. Впоследствии Госдума дважды продлевала этот срок, и в последний раз – до 1 июля 2011 года. В мае депутаты решили не откладывать срок еще раз.

Как пояснил «РГ» руководитель одной из крупных российских компаний, специализирующейся на проблемах информационной безопасности, Павел Шибков, новый закон напрямую затрагивает десятки тысяч российских компаний и организаций (кроме, разве что, архивов), которые сегодня регистрируют приватные, контактные сведения о людях в компьютерных базах данных. Речь идет в первую очередь о поликлиниках и медицинских центрах, операторах мобильной связи, банках, страховых компаниях, пенсионных и инвестиционных фондах, отелях и гостиницах, туристических агентствах.

Операторы должны установить правила доступа к персональным данным, регистрацию всех действий, совершаемых с информацией. Фиксировать факты несанкционированного доступа, а также восстановления потерянной информации, которая может быть повреждена или уничтожена в результате взлома или хакерской атаки. При этом они должны оценить вред, который может быть причинен гражданам.

И соблюдать установленные правительством технические требования по защите информации. И при этом использовать только определенные сертифицированные приборы и программы, одобренные уполномоченными на то силовыми структурами: Федеральной службой безопасности и Федеральной службой по техническому и экспортному контролю (ФСТЭК). Эти же организации будут контролировать выполнение новых требований.

«Первые головы могут «полететь» уже осенью», – прогнозирует эксперт. Те компании, которые не выполнят жестких требований закона, не внедрят необходимое оборудование (системы ограничения доступа, криптографическую и антивирусную защиту, программы по отслеживанию несанкционированных вторжений), будут не только выплачивать административные штрафы, но и лишаться лицензий.

Кстати, многие компании, уже имеющие такое оборудование – а это, как правило, крупные операторы-банки, страховые компании, операторы мобильной связи, – должны будут вновь аттестовать его.

В итоге, по оценкам участников рынка, расходы на установку систем обработки персональных данных для разных компаний могут составить от 10 до 200 процентов годового оборота плюс затраты на обслуживание и техническую поддержку. К примеру, чтобы лицензировать и сертифицировать защитные устройства, надо дополнительно выложить от 150 до 200 тысяч рублей. Эксперт «РГ» спрогнозировал, что большинство небольших компаний, не имеющих соответствующего оборудования, вынуждены будут для его установки и консультаций обращаться к профессионалам-посредникам, оплачивая их услуги.

Теперь правительство будет классифицировать уровни защиты информации, а требования к защите установят ФСБ и ФСТЭК. По словам Павла Шибкова, закон закрепляет позиции этих ведомств, поскольку аккредитованные при них лаборатории и центры будут получать стабильный доход от сертификации систем обработки персональных данных. Впрочем, Шибков считает, что организация такого рода фильтров позволит реально предотвращать утечки информации, защищать сведения от случайного доступа, уничтожения, изменения, блокирования, копирования, распространения.

Для граждан наиболее существенным является то, что их согласие на обработку

информации персональных данных о них может быть дано теперь в произвольной форме. Достаточно в анкете поставить галочку на сайте оператора в графе «согласен», и это будет считаться положительным ответом. Исключения касаются государственных ведомств и их ресурсов.

Вторым важным изменением является то, что вопрос, какими способами и технологиями осуществлять сохранность данных, выбирает оператор. Раннее уполномоченными органами, которые определяли технологии сохранности данных, были спецслужбы, которые рекомендовали использование дорогостоящих методов. В результате операторы просто не ставили защиту на персональные данные, и этим грешили практически все.

Кроме того, закон вводит понятие биометрических персональных данных. Но прерогатива их хранения и использования отдана в основном государственным службам, которые смогут к ним обратиться в случае необходимости установления личности. При этом обязательно письменное согласие человека на сбор и дальнейшее использование его биометрических данных, к которым относятся индивидуальные рисунки на пальцах рук и сетчатке глаза. Однако если человека подозревают в нарушении закона, причастности к терактам, то согласия, понятно, не требуется.

Важным является раздел по трансграничной передаче персональных данных, то есть о передаче их операторам других стран. Теперь туроператоры и транспортные компании должны иметь в виду, что если правила другой страны противоречат основным нашим законам, в том числе Конституции, то передача данных может быть даже запрещена. Кроме того, оператора обязывают убедиться в том, что иностранным государством, на территорию которого осуществляется передача данных, обеспечивается защита их обладателя. Причем сделать это надо до начала их передачи. Сама же передача персональной информации за рубеж не может осуществляться без письменного согласия субъекта.

Закон также определяет право гражданина на получение сведений о своих персональных данных. Он имеет право потребовать убрать информацию о себе из базы коммерческого оператора. В случае если этого по техническим причинам сделать нельзя, информация должна быть заблокирована. На то, чтобы стереть данные, оператору дается семь дней.

Официально

Новая редакция Закона «О персональных данных», пояснили «РГ» в минкомсвязи, учитывает европейский опыт регулирования обработки персональной информации.

Положения европейских документов нашли отражение в понятии персональных данных, которое стало более конкретным. В законе определены условия передачи персональных данных в другие страны и обеспечение их защиты при этом в рамках европейской конвенции. Согласие субъекта персональных данных поставлено в один ряд с другими возможными случаями обработки его данных, если он не в состоянии этого сделать в ряде ситуаций при защите его жизни, здоровья или иных жизненно важных интересов субъекта персональных данных.

Перечень случаев обработки персональных данных без согласия субъекта дополнен пунктом, который дает возможность заключить с ним договор, по которому в качестве поручителя выступает тот, кто осуществляет функции оператора, согласно законодательству. Подробно описан правовой режим деятельности лиц, которым обработка персональных данных передается оператором на аутсорсинг, то есть тем, кто обрабатывает их, если у компании нет на это собственных ресурсов.

Источник: Российская газета, № 162, 27.07.11

Авторы: Зыкова Т., Шадрина Т.