Методические рекомендации для образовательных учреждений по соблюдению законодательства в области персональных данных

В настоящее время объективной реальностью является необходимость обеспечения безопасности личной информации, поскольку информация о человеке сегодня превратилась в дорогой товар. Защита личной информации может приравниваться к защите личности, при этом степень угрозы безопасности личности (частная жизнь, личная, семейная тайна, жизнь и здоровье личности, собственность и пр.) может определяться в каждом конкретном случае незаконного использования информации о личности.

В этой связи вопросы защиты персональных данных получили в последние годы особое звучание - развитие Интернет технологий, широкое распространение персональных гаджетов с разнообразными функциями, в том числе геолокационными, выдвинули эту проблематику в разряд наиболее злободневных.

Среди нововведений можно выделить усиление контроля граждан за своими персональными данными, означающее, что передача данных гражданина должна осуществляться только с его согласия. В развитие данного положения было введено понятие «Право быть забытым», означающее, что персональные данные гражданина по его запросу должны быть полностью удалены из регистров поисковых систем.

В Федеральном законе от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – ФЗ «О персональных данных») указано, что субъект персональных данных вправе требовать от оператора прекратить обработку его персональных данных, уточнить и актуализировать сведения о себе. Данное право может рассматриваться в разрезе удаления информации не только из поисковиков, но и из социальных сетей и иных информационных ресурсов. Ведь человек, предоставив свое согласие на обработку личной информации какому-то ресурсу, должен иметь возможность стереть страницу глупых историй о себе, нелепостей молодости и иметь право на развитие личности без оглядки на прошлое.

Полноценная реализация гражданами России «права на забвение» осложняется тем, что иностранные интернет-гиганты не имеют на территории РФ полноценных представительств с правом принимать юридически значимые решения. Также следует учитывать, что сам институт защиты персональных данных в сети Интернет в России довольно молодой и мы только выстраиваем механизмы защиты персональных данных и удаления личной информации в сети Интернет, зачастую используя правила работы интернет отрасли и механизмы саморегулирования. Вместе с тем, как правило, выложенную личную информацию довольно часто по формальным признакам нельзя отнести к персональным данным, поэтому Роскомнадзор не может не тревожить уровень информированности как лиц, принимающих участие в образовательном процессе, так и самих детей, о последствиях бездумного и свободного распространения личной информации о себе и своих «подопечных».

В силу своей незрелости дети подвержены различным угрозам со стороны злоумышленников, более того дети порой сами могут причинить себе вред, не отдавая отчет тем последствиям, которые могут наступить в результате их собственных поступков и действий. Так, многочисленные исследования свидетельствуют о том, что чрезмерное увлечение общением в информационно-телекоммуникационных сетях крайне негативно сказывается на психологическом и физическом состоянии подрастающего поколения. А ведь, помимо прочего, это еще и этические проблемы, то есть правила хорошего тона, культурного поведения в Сети. Сегодняшним детям нужно объяснять, что размещать фотографии друзей в Интернете без их разрешения так же нехорошо, как и читать чужие письма, что свою личную информацию нужно защищать от посягательств со стороны третьих лиц. Так, выкладывание личной информации о друзьях или о себе может привести к ужасным последствиям, когда репутация ребенка будет неисправима. Например, недавнее происшествие с выложенными сценами изнасилования и издевательств над несовершеннолетней девочкой в Новосибирске, менее чем за сутки эта информация была

распространена в рамках одной социальной сети более чем по 70 ссылкам. Ведь подобные случаи не редкость и те только, когда речь идет об откровенной уголовщине, выкладывание в Интернете нелицеприятных фотографий с вечеринок подростков, драк или компромата в целях мести стало обыденным делом среди подростков. В таких ситуациях жертвы практически не имеют шансов начать новую жизнь без оглядки на прошлые проступки. Современная жизнь в век информационных технологий диктует нам новые угрозы, о которых мы ранее не задумывались. Мы живем в век информационного общества и не может не замечать, что стираются границы между абстрактной категорией «информация» и носителем этой информации. Виртуальный мир в современных реалиях представляет угрозу личности, собственности, общественному порядку и государственной безопасности. Так, защита той или иной информации может быть приравнена к защите её материального эквивалента.

Сегодня государственные и общественные организации стремятся создать благоприятные условия для детей в информационном пространстве. Существуют специальные программные средства, обеспечивающие родительский контроль, т.е. ограждение ребёнка от нежелательного контента в Интернете. Есть горячая линия помощи для детей, оказавшихся в тяжелой ситуации. Создана детская доменная зона .ДЕТИ для заведомо безопасных ресурсов.

Государство, со своей стороны, блокирует незаконный контент, осуществляет контроль за информационной продукцией, систематически мониторит Интернет на предмет нарушения законодательства, и привлекает нарушителей к ответственности. Но речь пойдёт не об этом, а об обучении детей правилам сетевой безопасности.

Беда в том, что дети беспечны, они не видят угроз, от которых их пытаются оградить взрослые. Школьники в России прекрасно умеют использовать современные технологии, но очень часто не понимают всех опасностей виртуального мира. Из-за этого они становятся самыми незащищенными пользователями всемирной паутины и оказываются жертвами злоумышленников именно в силу своей доверчивости.

Опасности, которые подстерегают людей в Интернете, часто связаны с нарушением прав субъектов персональных данных. А дети сами выкладывают в Сеть огромное количество личной информации, не подозревая, к каким бедам это может привести.

Как только информация попадает в Сеть, контролировать ее дальнейшее использование невозможно. Кто, когда и в каких целях может воспользоваться такими данными, не угадаешь. К нам обращались родители ребят-школьников, которых доводили до суицидальных состояний, шантажируя распространением личной информации, оказавшейся в Сети.

Драматические сюжеты развивались вокруг ситуаций, когда девушки доверчиво знакомились в социальных сетях с молодыми людьми, не зная их в реальной жизни, и высылали им личные, зачастую интимные фотографии и видео. Представьте себе состояние подростков, когда такие данные либо распространяются впоследствии в открытом доступе, либо создаётся угроза их распространения среди друзей, знакомых их родителей, соседей, учителей, родственников.

Утрата контроля над личными данными может повлиять не только на репутацию и психологическое состояние подростков. Цели злоумышленников различны - это и интернет-мошенничество, и кража денег с банковских карточек, и шантаж детей и родителей, продажа баз персональных данных для агрессивного маркетинга, насилие, кибербуллинг, установление слежки и пр.

Избежать распространения персональных данных в Интернете невозможно. Мы покупаем билеты на поезда и самолеты, совершаем покупки в онлайн пространстве, общаемся в социальных сетях под подлинными именами. Но разумная осторожность, соблюдение правил личной информационной гигиены предотвращают неприятности. Привить детям навыки безопасного поведения в киберпространстве, однако, непросто, коль скоро ими обладают далеко не все взрослые.

В мае 2014 года впервые Роскомнадзором, как уполномоченным органом в сфере защиты прав субъектов персональных данных, был применен дифференцированный подход к защите данных в Интернете. Критерием исследования информации мы поставили в зависимость от

категории лиц, которые являются субъектами персональных данных. Так, специалисты Роскомнадзора решили начать с самой незащищенной категории - с детей, в самом опасном для неокрепшей детской психики и самом свободном для кибермошенников информационном пространстве - во всемирной паутине.

При этом осознавая, что нарушения требований законодательства вызваны не злым умыслом, а недоразумением, возникшим в связи с неверной трактовкой определенных положений ФЗ «О персональных данных», было принято решение не задействовать весь спектр имеющихся механизмов воздействия на нарушителей, и воспользоваться исключительно правом Уполномоченного органа требовать удаления незаконно размещенной информации.

Зачастую возникает недопонимание правил обработки персональных данных у органов, непосредственно участвующих в образовательном процессе, в результате чего сайты, разместившие информацию о детях, как правило, принадлежат школам, детским садам, интернатам, а также муниципальным образованиям и администрациям ряда субъектов Российской Федерации.

Обнаруженные данные содержали списки не только самих воспитанников детских садов, учеников школ, с указанием их ФИО, даты рождения, места проживания, а также сведения о социальном статусе родителей и их принадлежности к той или иной льготной категории граждан. Речь идет о многодетных семьях, матерях-одиночках, безработных родителях, детях сотрудников правоохранительных органов, детях судей, детях, оставшихся без попечения родителей. На одном из сайтов образовательного учреждения даже был опубликован список детей, направляемых на психоневрологическую комиссию.

В соответствии с требованиями ст. 7 ФЗ «О персональных данных» операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Требованиями действующего законодательства Российской Федерации не предусмотрено размещение персональных данных образовательными учреждениями персональных данных обучающихся в информационно-телекоммуникационной сети «Интернет».

Согласно требованиям ч. 4 ст. 9 ФЗ «О персональных данных», согласие на обработку персональных данных должно включать в себя, в частности, цель обработки персональных данных и перечень действий с персональными данными, на совершение которых дается согласие.

В соответствии с требованиями ч. 2 ст. 5 ФЗ «О персональных данных», обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей.

Таким образом, образовательные учреждения не имеют законных целей, предусмотренных требованиями действующего законодательства Российской Федерации, для размещения персональных данных несовершеннолетних обучающихся в информационно-телекоммуникационной сети «Интернет».

Размещение подобной и не обезличенной информации не соответствует цели её обработки. Роскомнадзор неоднократно обращал внимание операторов персональных данных на то, что их обработка не должна быть избыточной по отношению к цели обработки. Следует всегда задаваться вопросом «ради чего данные о детях и их родителях собирались?»

Следует отметить, что ключевой принцип международного и российского законодательства в области персональных данных формулируется так: «Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных».

Например, в случае, когда данные собираются для информирования родителей, выкладывание данных о детях в Сети не будет соотноситься с целью обработки, ради которой эти данные собирались, даже при наличии отдельного согласия родителей на такую обработку.

К тому же размещение данной информации в сети Интернет квалифицируется как распространение информации неограниченному кругу лиц в публичном информационном

источнике. Так, следует разграничивать понятия предоставления доступа к той или иной информации и распространение данных. После того, как данные о детях будут выложены в Сеть, вы уже не сможете контролировать их обработку третьими лицами, эти данные могут быть скопированы, трансформированы, в том числе дополнены лживыми комментариями, домыслами и далее распространены в Сети. Они могут храниться в различных регистрах, базах, серверах из которых удалить данные будет практически невозможно. Таким образом, оператор, выложив персональные данные граждан в глобальную сеть Интернет, которые он собрал в определенных целях, уже не сможет проконтролировать и обеспечить обещанные субъекту данных условия обработки.

Роскомнадзором было выявлено, что в ряде случаев услуги хостинга сайтам образовательных учреждений, на которых были размещены персональные данные детей, предоставлялись иностранными компаниями, расположенными на территории США, Британских Виргинских островов, которые не являются участниками Конвенции Совета Европы в сфере защиты персональных данных, а также не обеспечивающими адекватной защиты прав субъектов персональных данных.

Следует заметить, что трансграничная передача данных на территорию таких государств возможна только в исключительных случаях, указанных в Законе о персональных данных. Информация о законности трансграничной передачи данных в Роскомнадзор до настоящего времени не поступила.

Роскомнадзор осуществляет свою контрольно-надзорную деятельность, в том числе путем проведения мероприятий систематического наблюдения в информационно-телекоммуникационной сети Интернет. Так, Управлением Роскомнадзора по Республике Дагестанежемесячно проводятся мероприятия систематического наблюдения (мониторинга) в сети «Интернет» в отношении различных категорий операторов, в том числе в отношении учреждений высшего, среднего, начального и общего образования, по результатам которых выявляются факты распространения персональных данных обучающихся на сайтах школ. В адрес образовательных учреждений направляются информационные письма для устранения выявленных нарушений.

Также ФЗ «О персональных данных» установлен ряд обязанностей для операторов, осуществляющих обработку персональных данных, в том числе:

1) направление уведомления об обработке (о намерении осуществлять обработку) персональных данных (в случае отсутствия образовательного учреждения в Реестре операторов, осуществляющих обработку персональных данных);

2) направление информационного письма (в случае отсутствия в Реестре операторов, осуществляющих обработку персональных данных, сведений о местах нахождения баз данных, содержащих персональные данные граждан)

3) назначение ответственного за организацию обработки персональных данных;

4) ознакомление работников, осуществляющих обработку персональных данных, с положениями законодательства в области персональных данных и (или) обучение указанных работников.

5) издание локальных актов по вопросам обработки персональных данных;

6) размещение на официальном сайте документа, определяющего политику оператора в отношении обработки персональных данных;

7) принятие правовых, организационных и технических мер по обеспечению безопасности персональных данных при обработке в информационных системах, в том числе внедрение средств защиты информации и контролем за принимаемыми мерами.

Необходимая работа с сайтами образовательных учреждений:

1) размещения на сайте ссылки на Портал «Персональные данные. Дети» (сайт http://персональныеданные.дети);

2) размещения документа, определяющего политику в отношении обработки персональных данных;

3) удаления сведений, содержащих персональные данные детей без законного основания;

4) **закрепления официальных сайтов непосредственно за организациями.**

Управлением Роскомнадзора по Республике Дагестан по результатам мероприятий систематического наблюдения в сети Интернет в отношении сайтов образовательных учреждений выявляются следующие виды нарушений:

1. Неразмещение на сайте документа, определяющего политику в отношении обработки персональных данных.
2. Незаконное размещение персональных данных несовершеннолетних на сайтах образовательных учреждений

Также были установлены отдельные случаи, когда сайт образовательного учреждения зарегистрирован не на организацию, а на физическое лицо (учитель информатики, системный администратор и т.д.).Это может негативно сказаться на администрировании сайта в дальнейшем, в случае увольнения указанного сотрудника у образовательного учреждения отсутствует возможность перерегистрации сайта, продления договора хостинга на сайт и т.д.