

Новое законодательство, принятое в Казахстане, вызывает беспокойство как в отношении доступа к онлайн-информации, так и в отношении безопасности данных в интернете.

Ряд законов, вступивших в силу 1 января 2016 года, закрепляет за государством функцию посредника всего онлайн-трафика. Один из законов предусматривает ответственность информационного провайдера за отказ предоставить государству информацию, считающуюся подозрительной.

Новая система потребует от всех пользователей интернета в Казахстане установить "национальный сертификат безопасности", который позволит государству быть посредником между пользователями и всеми веб-сайтами в Интернете.

Правительство уверяет, что сертификат обеспечивает шифрование каждого соединения, что позволяет защитить казахстанских граждан от террористической пропаганды, детской порнографии и интернет-мошенничества.

Но оппозиционный журналист Сергей Дуванов отмечает, что данные мотивы крайне сомнительны.

«Теперь любая информация, попадающая в интернет, станет достоянием людей в погонах, формально стоящих на страже нашей национальной безопасности, а фактически превратившихся в надзирателей за интернетом», - сказал он в интервью IWPR.

Министерство по развитию и инвестициям будет выдавать сертификат через Комитет по связи, информатизации и информации.

Это означает, что поставщик услуг будет иметь доступ ко всему зашифрованному интернет-трафику, имея возможность не только хранить и просматривать запросы пользователей, но даже потенциально редактировать входящие и исходящие данные.

Несмотря на то, что закон должен был вступить в силу с 1 января, все еще остаются вопросы по его реализации.

Впервые об этом шаге было объявлено в ноябре 2015 года в пресс-релизе казахстанского коммуникационного провайдера «Казахтелеком». В нем говорилось, что национальный сертификат безопасности будет обязательным, и что будет предоставлена пошаговая инструкция по его установке.

Впоследствии данный пресс-релиз был удален с веб-сайта, а 4 декабря «Казахтелеком» сообщил новостному сайту "Digital Report", специализирующемуся на вопросах ИКТ на постсоветском пространстве, что пользователи могут отказаться от установки данного сертификата безопасности и никаких санкций за это не будет.

Тем не менее, никто из представителей «Казакхтелеком» не смог прокомментировать IWPR, каково текущее положение дел с сертификатом.

Специалисты ИКТ отмечают, что факт добровольности можно поставить под сомнение, так как те, кто не установит сертификат, вероятнее всего, столкнутся с трудностями при доступе таким сервисам, как электронная почта, интернет-магазины и банкинг.

Gmail и Amazon, например, используют свой собственный сертификат безопасности, поэтому любая попытка доступа к ним из Казахстана будет заблокирована по причине установления защищенного соединения, пока их браузер не примет новый национальный сертификат.

Несмотря на потенциальные последствия, связанные с возможностью доступа государственных органов ко всем онлайн-транзакциям, по мнению эксперта в области цифровых технологий Адила Нурмакова, в Казахстане вряд ли будет много споров по поводу нового законодательства.

«Люди, как на уровне рядовых пользователей, так и в журналистской среде, не очень хорошо разбираются в вопросах информационной безопасности. Поэтому новость больше обсуждалась на российских профессиональных IT-порталах и в международной прессе. Люди не совсем понимают, что для них означает инициатива с национальным сертификатом безопасности», - сказал в интервью IWPR Нурмаков.

«Многие пользователи порой автоматически нажимают “да” и “согласен”», - говорит Шавкат Сабилов, руководитель Интернет-Ассоциации Казахстана. Он считает, что большинство жителей Казахстана примут новый национальный сертификат, не понимая всей его сути.

Наравне с вопросом конфиденциальности, новый шаг вызывает озабоченность по поводу безопасного хранения данных.

После ввода сертификата безопасности, личные данные, включая банковские операции, пароли и личные фотографии, хранящиеся в сети, станут доступными киберпреступникам, а также государственным органам, говорит адвокат Ерлан Кемешев.

Очевидно, что бизнес-сообщество находится в неведении относительно возможных последствий для частных пользователей интернета.

Сотрудница банка в Алматы, пожелавшая не называть свое имя, рассказала IWPR, что ее руководство до сих пор не знает, как сертификат безопасности повлияет на их работу.

«Мы находимся в том же положении, что и наши клиенты», - сказала она.

IT-специалист Артем Тихонов предупредил, что новая система делает пользователей более уязвимыми для мошенничества.

По его словам, третий участник, вклинившийся между банком и каждым клиентом, даст мошенникам дополнительные возможности для кражи данных.

В случаях мошенничества, по словам Тихонова, скорее всего, основное бремя будет нести потребитель.

«Если случится инцидент, и пользователь банка потеряет вследствие внедрения сертификата и утечки пользовательских идентификационных данных свои деньги, пострадает только сам пользователь, а банк “умоет руки”», - сказал он.

Помимо этого, вступивший 1 января в силу закон дополнительно увеличивает полномочия государственных органов по доступу к личным данным.

«Владельцам сети и операторам связи придется улучшить качество взаимодействия [с государством] во избежание новых административных санкций», - объяснил Кемешев.

Одна из новых статей предусматривает административное правонарушение, если провайдер коммуникационных услуг откажется предоставить доступ к якобы «незаконной информации».

«Мы живем в полицейском государстве, где спецслужбы... не особо беспокоятся о соблюдении различных процедурных гарантий, особенно когда речь идет об оперативно-розыскной работе и предупреждении экстремизма и радикализма», - сказал Евгений Жовтис, председатель Совета Казахстанского международного бюро по правам человека и соблюдению законности.

«Сама процедура, при которой будет использоваться новый сертификат безопасности, четко не прописана, что порождает неопределенность и опять же дает широкие полномочия спецслужбам», - согласилась с ним Айна Шорманбаева, президент общественного фонда «Международная правовая инициатива».

В Казахстане самый высокий уровень проникновения интернета в Центральной Азии, составляющий 55%. Но при этом, по данным “Freedom House”, страна считается «несвободной» и занимает низкий рейтинг в Индексе свободы Интернета.

В 2015 была введена уголовная ответственность за распространение слухов и ужесточены штрафы за клевету.

Кроме того, по данным “Freedom House”, правительство неоднократно запрещало транслировать онлайн-контент, освещавший как участие казахстанцев в боевых действиях на стороне Исламского государства, так и политическую критику.

Газиза Байтуова - контрибьютор IWPR в Алматы. Василина Атоянц-Ларина - журналист из Алматы. Сотрудники IWPR в Центральной Азии также приняли участие в подготовке материала.

Данная публикация была подготовлена в рамках проекта IWPR «Усиление потенциала и налаживание мостов между народами Центральной Азии», осуществляемого при финансовой помощи Министерства иностранных дел Норвегии.