Права человека в офлайне должны также защищаться и в онлайне

Сергей Швакин о цифровизации и защите персональных данных

Директор Института экономических и правовых исследований Сергей Швакин специально для «Регионов России» рассказал о цифровизации в России.

– Сергей Владимирович, как Вы оцениваете темпы цифровизации в России?

– Зачастую, для того чтобы как-то охарактеризовать процесс цифровизации, используется термин «темпы» с сочетанием различных эпитетов: «высокие темпы», «низкие темпы», «медленные темпы», «быстрые темпы». Как правило, это все оценочные суждения. Очевидно, что цифровизация – это динамический процесс и при его оценке нужно использовать как качественные, так и количественные показатели. Сложность заключается в том, что собираемые формальные данные явно недостаточны для комплексного анализа. Существуют различные методики, которые направлены на повышение презентативности, валидности, нормализации данных, их анализа на основе разного рода индексов, и некоторые из них вызывают большое доверие, но из-за отсутствия общепринятой методологии и ее нормативного закрепления все еще нельзя оценить процесс цифровизации в целом с достаточной степенью эффективности и точности.

Что касается международного аспекта, то существует так называемый глобальный рейтинг ООН по развитию электронного правительства (E-Government Development Index – EGDI). В 2020 г. Россия заняла 36-е место, что на четыре строчки ниже, чем двумя годами ранее.

Все вышесказанное справедливо и для оценки эффективности правового регулирования цифровой среды. Однозначно, пожалуй, можно говорить только об одном: мы можем наблюдать одновременно два параллельных нормотворческих процесса – появление одних нормативно-правовых актов буквально формирует новые социально-экономические отношения в цифровой среде, способствует их прогрессивному развитию; принятие или непринятие других – тормозит их развитие. Любая оценка этого процесса будет являться субъективной, даже в силу того, что очень сложно спрогнозировать, как повлияет на общество существующий сегодня подход законодательного регулирования цифровой среды в долгосрочной перспективе. Риски построить конструкт, описанный Иеремией Бентамом («Паноптикум») или Мишелем Фуко («Око Власти»), достаточно велики.

– Как отечественные компании заботятся о защите персональных данных своих сотрудников?

– Как минимум российские организации в вопросах защиты персональных данных обязаны соблюдать требования российского законодательства. В некоторых случаях необходимо также соблюдение требований норм права Европейского Союза, например, Общего Регламента о защите персональных данных (General Data Protection Regulation – GDPR). Это может произойти, если организация физически присутствует (в виде локального лица или подразделения) на территории одного из государств, входящих в состав

Европейского Союза; если организация предлагает товары или услуги лицам, проживающим на территории Европейского Союза, в том числе посредством своего сайта; или же проводит мониторинг лиц, находящихся на территории Европейского Союза, с использованием файлов cookies, трекинга, CCTV; если российское лицо осуществляет обработку персональных данных в интересах оператора, на которого распространяются требования GDPR, а также в некоторых других случаях. Подробное рассмотрение применимости GDPR – это тема для отдельного обсуждения в силу ее объемности.

В 2020 г. Россия заняла **36**-е место в глобальном рейтинге ООН по развитию электронного правительства (E-Government Development Index – EGDI)

– Может ли сегодня россиянин чувствовать себя безопасно в цифровой реальности?

– Вопрос безопасности человека в цифровой реальности – многоаспектный. Для того чтобы ответить на него, необходимо сначала определиться с самим понятием «безопасность». Если сильно упрощать и не приводить сложных доктринальных определений, то безопасность можно понимать как «отсутствие опасности» или «состояние защищенности» от различных угроз – внешних и внутренних. Кроме того, безопасность человека (личности), так же как и личную безопасность, невозможно рассматривать изолированно, не учитывая интересы общества и государства. О безопасности личности не может идти и речи, если не обеспечивается безопасность на более высоких, глобальных уровнях – на уровне общества и государства. Таким образом, безопасность личности всегда следует рассматривать через призму своеобразной триады: «безопасность личности», «безопасность общества» и «безопасность государства». При этом нужно разграничивать также смежные, не тождественные понятия – «личная безопасность», «общественная безопасность», «государственная безопасность». На первый взгляд, может показаться, что такая теоретизация уводит фокус внимания от реальности, однако это далеко не так. Дело в том, что определяющее значение имеет даже не сама «безопасность», как некое субъективное чувство отдельно взятого человека, на самом деле намного важнее «обеспечение безопасности» в виде государственной политики, реализации государственной функции, и для эффективного осуществления этой деятельности нужно четко понимать, какие объекты безопасности подлежат защите на уровне государства, на уровне общества, а также на уровне личности.

Особой сложности не возникает, когда речь идет о защите «традиционных прав» (имущественных или неимущественных), даже если общественные отношения реализуются не в офлайн, а в онлайн среде. Например, при совершении преступления против собственности сама суть хищения не меняется от того, что оно было совершено с использованием информационных технологий. При этом институциональные механизмы, призванные обеспечивать безопасность граждан в этой сфере, давно закреплены на законодательном уровне. Вопрос об эффективности этих механизмов – это отдельная тема для обсуждения.

Несколько иначе обстоит дело с правами человека, которые появились в результате цифровизации социальной среды, которые являются продуктом четвертой промышленной революции, речь уже идет о так называемых «цифровых правах»: праве на доступ к информации (право на подключение, право не быть отключенным, право на поиск информации, право на безопасное использование информации), о праве на забвение, праве на «цифровую смерть» (цифровое наследование), праве на информационное самоопределение, праве на обеспечение конфиденциальности информационных систем (в т.ч. защита от онлайн обысков), праве на изображение, праве на информационную частную жизнь, праве на равенство, праве не быть субъектом компьютеризированных решений, праве на анонимность в контексте обработки больших данных, праве на нейтральность и т.д. Приведенный перечень – не закрытый.

В 2012 г. Совет по правам человека ООН в резолюции 20/8 «Поощрение, защита и осуществление прав человека в Интернете» сформулировал фундаментальный принцип, согласно которому «те же права, которые человек имеет в офлайновой среде, должны также защищаться и в онлайновой среде». Несмотря на это в разных юрисдикциях вопрос о защите таких прав решается по-разному, и в целом проблема обеспечения прав граждан в цифровой среде все еще остается достаточной сложной.

– Чего не хватает российскому законодательству для защиты персональных данных россиян?

– В целом российское законодательство охватывает необходимые сферы регулирования и в принципе основано на международно-правовых нормах. Однако можно обозначить две основных проблемы. Первая касается фактического правоприменения и связана с ненадлежащим исполнением законодательных норм соответствующими субъектами на разных уровнях. Вторая проблема связана с трансграничной передачей данных, в этой сфере желательна унификация норм российского права с правом Европейского Союза (по аналогии с фреймворком EU-U.S. Privacy Shield). ■