УДК 346

ПРОБЛЕМАТИКА ПРАВОВОГО ВЗАИМОДЕЙСТВИЯ СУБЪЕКТОВ ХОЗЯЙСТВОВАНИЯ В РАМКАХ ОБЩЕГО РЕГЛАМЕНТА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Н.В. КОЗЛОВ
(Представлено: Т.В. СЕМЁНОВА)

Рассматриваются проблемы национального законодательства Республики Беларусь и Общего регламента защиты персональных данных, области их применения среди субъектов хозяйствования. Предлагаются способы разрешения исследуемой проблематики.

Вопросы сбора, обработки и передачи персональных данных и их правовая регламентация давно являются массово обсуждаемым явлением в мировой практике. Начиная от точечных законопроектов отдельных государств и заканчивая нормативным правовым актом «Общий регламент защиты персональных данных»/General Data Protection Regulation (далее – GDPR), который действует не только на территории всех стран Европейского союза (далее – ЕС), но и на субъектов хозяйствования, которые реализуют товары и услуги потребителям ЕС. Для последнего признака не является обязательным наличие гражданства ЕС, достаточно фактического местонахождения на территории одной из стран-участниц.

Для Республики Беларусь приведённая сфера является крайне спорной с наличием многих острых вопросов. Начать стоит с того, что в белорусском законодательстве не существует какой-либо нормы, не только регулирующей сферу защиты персональных данных, но и вовсе не вводит такого понятия, как «персональные данные». Определение данного понятия не закреплено на законодательном уровне, но, например, используется в статье 32 Закона Республики Беларусь «Об информации, информатизации и защите информации» [1]. Такая коллизия послужила основой для создания модели законопроекта «О персональных данных», принятие и одобрение которого Советом Республики растянулось на несколько лет и на сегодняшний день по-прежнему оставляет вопрос открытым.

Если детально исследовать GDPR, то за время действия данного законопроекта можно также выделить значительный список проблемных аспектов как для Республики Беларусь, так и для остальных стран, не членов ЕС. Автор выделяет следующие элементы, требующие значительных изменений:

1) недостаточные технические меры защиты персональных данных;
2) отсутствие социально-коммуникабельной транспарентности;
3) нарушение прав пользователей;
4) неограниченный срок хранения данных;
5) недостаточное правовое основание для обработки данных.

Дабы соответствовать требованиям GDPR, субъекты хозяйствования (если таковые имеют собственную политику, тесно связанную с различными действиями в области персональных данных пользователя) должны принять организационные и технические меры защиты персональных данных. Организационные меры касаются внедрения определённой документации и политики. Техническая сторона подразумевает наличие мощного и дорогостоящего оборудования для возможности хранения и обработки объёмных массивов информации пользователей, поэтому компании часто их игнорируют и получают большие штрафы. В качестве примера можно привести случай с авиакомпанией British Airways, получили самый большой в истории GDPR штраф – более 200 миллионов евро за отсутствие надлежащих технических мер. Через год по той же причине Marriott International, Inc оштрафовали на 100 миллионов евро. В обоих случаях из-за уязвимости в системе защиты злоумышленники получили доступ к персональным данным [2].

Исследуя отсутствие социально-коммуникабельной транспарентности, мы пришли к выводу, что основной проблемой является нежелание субъектов хозяйствования информировать пользователя о том, как и кем, будут использоваться его персональные данные. Такая информация должна быть легкодоступна и написана не юридическим и техническим языком, а понятным для пользователя. Самый яркий пример – компания Google была оштрафована правительством Франции на 50 миллионов евро за различные нарушения в области защиты персональных данных, в том числе, за форму подачи информации [2]. Чтобы узнать всю информацию о том, как используются персональные данные пользователя, достаточно было открыть 5–6 разных ссылок.

На взгляд автора, детально проработанное содержание политики конфиденциальности (privacy policy), с максимально полной и актуальной информацией о том, как компания использует персональные данные пользователей, может раз и навсегда решить данную проблему. В таком случае, у потребителя не должно возникать проблем в том, чтобы найти, где она размещена, и понять, что в ней написано.

Складывающиеся отношения в области нарушения прав пользователей, как показывают различные новостные заголовки, наводят на вывод о том, что если компания получила персональные данные пользователя на законном основании, это не значит, что теперь она может распоряжаться ими по своему усмотрению. У пользователей есть права по отношению к своим персональным данным, которые компания обязана

соблюдать. Например, если основанием для обработки данных служит согласие пользователя, то он имеет право его отозвать. Автор утверждает, что проработка на сайтах субъектов хозяйствования таких элементов как: «страница регистрации», «страница профиля пользователя» и «дополнительная функциональность» будет являться решением обозначенной проблемы, а также сэкономит время пользователя.

Самым главным недостатком GDPR является неограниченный срок хранения данных, и он не устанавливает конкретных сроков хранения каждой категории данных [3]. Каждая компания определяет их самостоятельно исходя из анализа целей, для которых эти данные обрабатываются. Даже если субъект хозяйствования обрабатывает персональные данные с соблюдением требований GDPR, он может хранить их только на протяжении определенного периода времени, а именно, пока данные нужны для достижения целей их обработки. Автор полагает, что решение исследуемой, в данном случае, проблемы заключается в определении, перед началом обработки данных, срока, в течение которого будут храниться, обрабатываться и удаляться персональные данные пользователей.

Последний приведённый проблемный аспект, а именно, недостаточное правовое основание для обработки данных, всегда упирается в некорректном использовании списка оснований для обработки персональных данных. GDPR предусматривает 6 оснований [3]:

1) субъект персональных данных дал согласие на обработку своих персональных данных для одной или нескольких конкретных целей;

2) обработка необходима для исполнения договора, в котором субъект данных является стороной, или для реализации по поручению субъекта данных шагов, предшествующих заключению договора;

3) обработка необходима для выполнения правового обязательства, возложенного на контролёра;

4) обработка необходима для защиты жизненно важных интересов субъекта данных или другого лица;

5) обработка необходима для выполнения задачи в публичных интересах или в рамках осуществления государственной власти, доверенной контролёру;

6) обработка необходима для целей, вытекающих из легитимных интересов, преследуемых контролёром или третьим лицом, за исключением случаев, когда преимущество над такими интересами имеют интересы или фундаментальные права и свободы субъекта данных, требующие защиты персональных данных, в частности, когда субъектом данных является ребёнок.

Автор, как и многие деятели науки, считает, что при грамотном и точном выборе оснований сбора персональных данных субъектом хозяйствования, данная проблема будет решена. Также, в совокупности необходимо проводить анализ всех внутренних процессов обработки данных, а после соотношение их с применимыми основаниями обработки. Если для обработки данных как основание должно использоваться согласие пользователя, необходимо учитывать, что согласие должно быть явно выраженным, свободным, конкретным и информированным.

Систематизируя всё выше изложенное, можно выделить несколько проблемных частей законодательства Республики Беларусь и ЕС в лице GDPR. Главный минус национального законодательства – отсутствие точных и конкретных норм в области защиты персональных данных. Самой главной проблемой белорусского законодательства, порождающей все пять проблемных аспектов, выделенных нами, в GDPR, является, также отсутствие какого-либо механизма исполнения требований GDPR. Данное упущение, на взгляд автора, снизило бы количество нарушений в области взаимодействия между субъектами хозяйствования Республики Беларусь и пользователями ЕС и наоборот – между компаниями ЕС с белорусскими пользователями.

Необходимо создать государственный орган, который бы занимался проверкой и разрешением различных жалоб и судебных решений в области защиты персональных данных. Не исключено, что наделение данной компетенцией возможно для органов прокуратуры, либо путём создания в них специализированных подразделений, выполняющих данную функцию.

ЛИТЕРАТУРА

1. Об информации, информатизации и защите информации [Электронный ресурс] : Закон Респ. Беларусь, 10 нояб. 2008 г. № 455-З // КонсультантПлюс. Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2020.
2. Чурилов, А. Ю. Принципы Общего регламента Европейского Союза о защите персональных данных (GDPR): проблемы и перспективы имплементации [Электронный ресурс] / А. Ю. Чурилов, // Научная электронная библиотека КиберЛенинка. – Режим доступа: https://cyberleninka.ru/article/n/printsipy-obschego-reglamenta-evropeyskogo-soyuza-o-zaschite-personalnyh-dannyh-gdpr-problemy-i-perspektivy-implementatsii/viewer. – Дата доступа: 20.09. 2020.
3. Общий регламент защиты персональных данных (GDPR) Европейского Союза // Data Privacy Office [Электронный ресурс]. – 2020. – Режим доступа: https://gdpr-text.com/ru/. – Дата доступа: 20.09.2020.