TID «Today I decide»). Создание электронных сервисов и «местных» порталов находит успешное развитие в Российской Федерации, Южной Корее, Латвии и Литве. В Республике Болгария действует система «машинного», т. е. электронного голосования, порталы для внесения предложений граждан и взаимодействия с органами.

Таким образом, анализируя зарубежный опыт, можно отметить, что осуществление электронной демократии на уровне местного управления и самоуправления в Республике Беларусь только начинает развиваться. Между тем использование ИКТ для коммуникации органов местного управления и граждан помогает глубже изучить проблемы регионов и находить подходы к их устранению, учитывая мнение населения, снижает финансовые издержки для государства в осуществлении процесса выборов в органы местного самоуправления.

Лазута Л. В.

ПРЕДЕЛЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ЕВРОПЕЙСКОМ СОЮЗЕ

Лазута Любовь Витальевна, студент 4 курса Международного университета «МИТСО», г. Минск, Беларусь, llv3381@gmail.com

Научный руководитель: старший преподаватель Ходакова А. А.

Основой правового регулирования защиты персональных данных в Европейском союзе является регламент о защите персональных данных (*General Data Protection Regulation,* далее – GDPR). В п. 26 Преамбулы регламента выделяется два вида обезличенных данных: анонимизированные данные и псевдонимизированные данные. Под анонимизированными данными понимается любые данные, которые необратимо обезличены и в отношении которых реидентификация невозможна, поскольку утрачена всякая связь с физическим лицом. Однако в регламенте GDPR отсутствует правовое закрепление понятия псевдонимизированных данных. Указанный документ определяет, что под псевдонимизацией подразумевается особенный процесс, который включает в себя обработку персональных данных, в том случае, когда персональные данные не могут быть соотнесены с конкретным лицом без использования дополнительной информации, при этом дополнительная информация хранится отдельно и для нее были предприняты организационно-технические меры обеспечения невозможности соотношения с идентифицируемым физическим лицом (ст. 4(5) GDPR). В связи с этим представляется возможным закрепление указанной дефиниции в регламенте GDPR, поскольку псевдонимизированные данные сохраняют определенную связь с физическим лицом и с учетом данного фактора, могут быть использованы для идентификации лица. Такого рода подход в GDPR основан на

практике Международной организации по стандартизации, в базисе которой имеют различия анонимизирования данных, в качестве не сохраняющих возможности установления связи с физическим лицом при использовании различных массивов данных, и обезличенные данные, в качестве информации, из которой устранена связь между физическим лицом в определенном массиве данных.

К анонимизированным данным сегодня не применяются Положения регламента GDPR, в то время как псевдонимизированные данные остаются персональными данными, однако их обработка осуществляется с особенностями, которые предусмотрены в GDPR. Псевдонимация также рассматривается одним из возможных средств защиты персональных данных. Категория анонимизированных данных, в соответствии с GDPR, зависит от технологического контекста и других объективных условий. В п. 26 Преамбулы к GDPR указывается, что невозможность идентификации субъекта непосредственно зависит от объективных факторов, которые необходимы для идентификации, доступных технологий и уровня технологического развития на момент обработки данных. Таким образом нет возможности нарушить анонимность данных исходя из фундаментальных технологий, а также данная категория не будет относиться к персональным данным в связи с использованием более современных технологий вычисления, таких как квантовые, что подразумевает под собой перспективу квалификации тех самых данных в качестве псевдонимизированных, т. е. персональных.

Причина подобного разграничения данных в GDPR и отнесение псевдонимизированных данных к числу персональных связывается с доступностью использования технологии «Больших данных», что дает возможность идентифицировать личность при помощи установления корреляционной зависимости между различными фрагментами данных. Любая информация об относительно уникальном качестве субъекта, например, посещения конкретных мест сможет стать основанием для «распознания» данной личности в иных базах данных.

Исходя из этого, проблемой представляется тот факт, что обезличенные данные уже не могут выполнять функцию действенного средства защиты личной жизни граждан, на тот момент пока они сохраняют какую-либо связь с физическим лицом и должны использоваться иные механизмы защиты, установленные в законодательстве о персональных данных. Следует отметить, что в качестве обезличенных данных рассматриваются все персональные данные, лишь за исключением редких случаев, когда с использованием таких данных не может быть произведена реидентификация лица.

В Европейском союзе немало внимания уделяют выработке методик обезличивания персональных данных. Наиболее подробным документом, описывающим методы, является позиция рабочей группы ст. 29 «О методологиях обезличивания данных». Данный документ разделяет все

методы обезличивания на две большие группы, основанные на: введении случайных данных в исходный массив информации и обобщенные значения некоторых параметров исходного массива информации.

Таким образом, на наш взгляд пределы защиты персональных данных будут заключаться в следующем категориях: 1) персональные данные должны обрабатываться законно и прозрачно; 2) данные должны собираться и использоваться лишь в пределах, заявленных онлайн-сервисом; 3) личные данные должны храниться в форме, которая позволяет идентифицировать субъекты данных на срок не более, чем это необходимо для целей обработки; 4) процесс обработки данных пользователей компании должен быть обеспечен защитой персональных данных от несанкционированного уничтожения и повреждения.

Лычковский Д. Н.

ПЕРИОДЫ ЭВОЛЮЦИИ НЕПРИКОСНОВЕННОСТИ ЛИЧНОСТИ И ЭТАПЫ ИХ ФОРМИРОВАНИЯ

Лычковский Денис Николаевич, исследователь, Академия Министерства внутренних дел Республики Беларусь, г. Минск, Беларусь, denisly@tut.by

Правовой институт неприкосновенности личности в своем развитии прошел ряд периодов и этапов, позволивших ему в настоящее время получить правовое закрепление на конституционно-правовом уровне и в качестве международного стандарта. Однако неприкосновенность личности как правовое явление в своей эволюции не всегда имело закрепление в качестве права человека. По нашему мнению, развитие неприкосновенности личности прошло несколько периодов, отрезков времени, в которых происходили те или иные изменения – этапы, формирующие, выделяющие данные периоды, являясь их организующим стержнем и определяющим качеством, в подтверждение чему далее приведена авторская классификация периодов эволюции неприкосновенности личности и этапов, сформировавших их.

I. Период Античности и раннего Средневековья. В правовых актах этого периода предприняты только первые попытки закрепления оснований, условий и пределов воздействия на телесную неприкосновенность человека, т. е. сделан шаг от обычного и религиозного закрепления к юридическому (шаг от «не права» к праву). Закладывались основы недопустимости произвольного лишения жизни; регулировались имущественные отношения и возможности привлечения должника к ответственности; устанавливалась ответственность за причинение телесного вреда человеку (хотя и в зависимости от социального статуса потерпевшего) и т. д.

II. Период Средневековья. Одним из ведущих оснований для ограничения неприкосновенности личности в средневековой Европе являлось отсутствие возможности у человека доказать свой «благонамеренный», честный статус.