Журнал правовых и экономических исследований.
Journal of Legal and Economic Studies, 2019, 3: 157–161

DOI 10.26163/GIEF.83.94.027
УДК 004.056.53

A.V. Pushinin, A.S. Pushinina

EVOLUTION OF MECHANISM OF PERSONAL DATA PROTECTION: DOMESTIC AND EUROPEAN EXPERIENCE

Andrey Pushinin – Head of the Department of Accounting and Statistics, State Institute of Economics, Finance, Law and Technology, PhD in Economics, Associate Professor, Gatchina; **e-mail: pushinin@mail.ru**.
Anastasia Pushinina – leading specialist, the Department of Personalized Registration and Work with Insurers, Administration of Pension Fund in Gatchina District, Gatchina; **e-mail: a.s.pushinina@gmail.com**.

We pay attention to the problem of establishing and improving the system of personal data protection. A comparison of domestic and international experience in the sphere in question is made. The divergence is revealed. We develop an approach to improving the domestic system of personal data protection.

Keywords: *personal data; domestic approach; international practice; evolution; data protection; responsibility; sanctions.*

А.В. Пушинин, А.С. Пушинина

ЭВОЛЮЦИЯ МЕХАНИЗМА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ: ОТЕЧЕСТВЕННЫЙ И ЕВРОПЕЙСКИЙ ОПЫТ

Андрей Вячеславович Пушинин - зав. кафедрой бухгалтерского учета и статистики, Государственный институт экономики, финансов, права и технологий, кандидат экономических наук, доцент, г. Гатчина; **e-mail: pushinin@mail.ru**.
Анастасия Сергеевна Пушинина – главный специалист-эксперт отдела персонифицированного учета и взаимодействия со страхователями УПФР в Гатчинском районе (межрайонное), г. Гатчина; **e-mail: a.s.pushinina@gmail.com**.

В статье рассматриваются вопросы становления и совершенствования системы защиты персональной информации. Сопоставлен отечественный и зарубежный опыт в данной области. Выявлены существующие отклонения. Разработан подход по совершенствованию отечественной системы защиты персональных данных.

Ключевые слова: *персональные данные; отечественный подход; зарубежная практика; эволюция; защита информации; ответственность; санкции.*

В современных условиях одним из главных факторов успешного хозяйствования и получения экономических выгод становится доступ к объективной и полной информации. Поэтому экономику следует считать информационной.

В процессе становления цифровой экономики персональная информация и ее защита являются в достаточной степени актуальными вопросами. С одной стороны, процесс цифровизации предполагает открытость и доступность информации для ее пользователей, но и права человека на определенную конфиденциальность должны быть соблюдены.

В условиях информационной экономики острой становится проблема сохранности конфиденциальной информации, предотвращения несанкционированного доступа к ней сторонних лиц. Все это относится и к персональным сведениям граждан, их использованию в коммерческой деятельности хозяйствующими субъектами.

Проблема защиты персональных данных актуальна как в зарубежной, так и

отечественной практике. Следует отметить, что защите персональных сведений за рубежом уделялось и уделяется значительное внимание. Данный процесс особенно активизировался в последние двадцать лет. В различных странах сформировались определенные подходы, способы и методы сбора, обработки, хранения персональных сведений.

Впервые проблема обработки вышеуказанной информации и незаконного ее использования была озвучена Генеральной Ассамблеей ООН 10 декабря 1948 г. при утверждении «Всеобщей декларации прав человека». Определенной завершенности и целостности в вопросах правового регулирования данной сферы удалось добиться в европейских странах. В Европе защита персональных сведений государством базируется на праве частной жизни гражданина. При этом государство возлагает значительную часть ответственности на хозяйствующие субъекты, которые обязаны обеспечить сохранность персональных сведений.

Анализируя вопрос формирования законодательства в исследуемой области, упомянем, что впервые в мировой практике законодательство о персональной информации и ее защите было принято в Германии. В земле Гессен в 1970 г. было установлено право на информационное самоопределение при изучении законности автоматизированной системы идентификации подозреваемых, видеофиксации сведений о памятнике искусства, отслеживании автомобильных номеров автоматизированным способом и пр. [3].

Совет Европы первый шаг в данной сфере осуществил 28.01.1981 г., утвердив «Конвенцию о защите физических лиц при автоматизированной обработке персональных данных». В дальнейшем законодательство в области защиты персональных сведений совершенствовалось. Логичным развитием событий стало принятие 27 апреля 2016 года Регламента 2016/679 Европейского парламента и Союза «О защите физических лиц относительно обработки персональных данных и о свободном перемещении таких данных…» (далее – GDPR), который вступил в силу с 2018 г.

В течение двух лет (до 2020 г.) процесс обработки персональной информации должен быть приведен в соответствие с новыми, более жесткими требованиями. GDPR обязателен к применению странами-участницами ЕС.

Регламент к персональным сведениям относит любую информацию, которая касается физического лица [5] (рис. 1).

Согласно требованиям нового закона потребители получают более широкий контроль над своими данными: право доступа; право на исправление; право на забвение; право на ограниченную обработку; право на перенос данных; право на возражение. При этом субъект должен дать однозначное согласие на использование его персональных сведений для определенных нужд. Согласие должно быть четким,

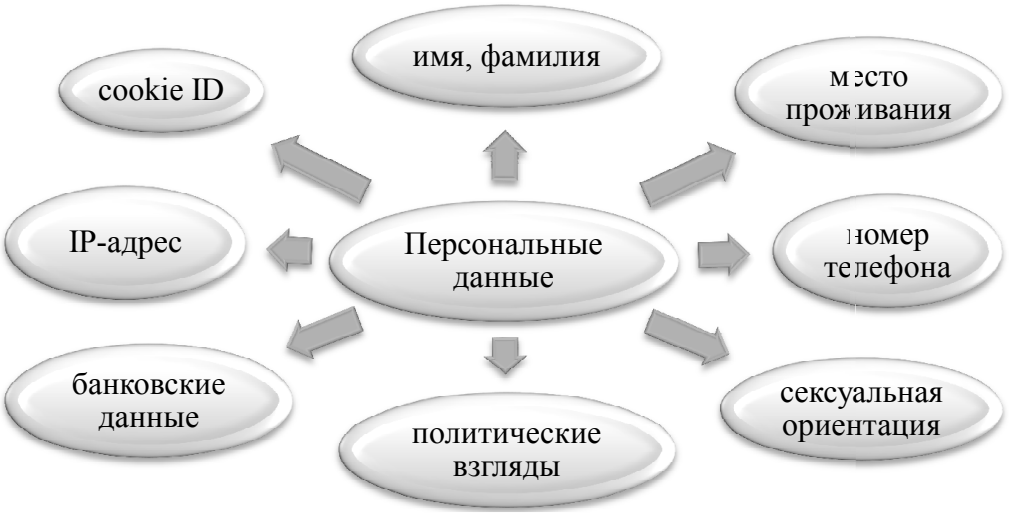

Рис. 1. Состав персональной информации в Европейском Союзе

предполагающим право выбора и отзыва согласия. Так же в Регламенте отражены шесть принципов работы с персональными сведениями: правомерность; целевое ограничение обработки персональных данных; минимизация данных; точность персональных данных; ограничение хранения персональных данных; целостность и конфиденциальность персональных данных.

Рассматриваемый Регламент урегулирует операции, которые связаны с обработкой персональной информации. Для целей GDPR не существенен тот факт, что указанный обработчик оперирует информацией на территории ЕС или нет. Так же законодательно не осуществляется привязка к гражданству лица, данные которого обрабатываются. Таким образом, под действие Регламента попадают данные абсолютно всех лиц, которые находятся на территории ЕС. Это относится, в том числе, и к гражданам Российской Федерации [5].

GDPR гармонизирует и унифицирует действия лиц, которые осуществляют обработку и защиту персональной информации. Надзорные и судебные органы, Суд ЕС, иные учреждения и органы в рамках Регламента должны действовать единообразно.

Российские компании подпадают по действие GDPR, если продают товары и услуги в ЕС, используют язык или валюту стран-участниц ЕС, имеют сайт в зоне национальных доменов или в зоне домена верхнего уровня. К таким хозяйствующим субъектам можно отнести социальные сети, интернет-магазины, финансовые корпорации и т.д.

В России Конвенция 1981 г. была принята, и на ее базе был разработан и утвержден Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных». Целью указанного нормативного акта является реализация защиты прав граждан в процессе получения, обработки и обеспечения сохранности персональной информации [1]. В 2013 году был Гражданский кодекс был дополнен статьей 152.2, которая посвящена вопросам защиты частной жизни физического лица.

Отметим, что при наличии действующих нормативных актов в анализируемой области, в России так и не сформировалось однозначной трактовки персональной информации. Согласно распространенной точке зрения, персональные данные – это информация, которая в определенной степени относится к ее субъекту (рис. 2).

Сейчас требуются более жесткие критерии отнесения данных к персональным. Так, в России выделено три категории персональных данных:

- любая информация, относящаяся к физическому лицу (например, фамилия, дата рождения, адрес, доходы и пр.);

- специальные категории персональных данных (например, раса, религиозная принадлежность, имеющиеся болезни и т.п.);

Рис. 2. Состав персональной информации в России

- биометрическая информация.

Цифровизация экономики предопределила потребность в обеспечении должной защиты персональной информации. Согласно поправкам, вносимым в законодательство, операторы стали вынуждены локализовать базы данных российских граждан. И именно в России впервые был урегулирован вопрос права на забвение [3].

Проанализировав содержание основополагающих нормативных актов, резюмируем, что отечественное и европейское законодательство в данной сфере тождественны. Но в Европе все чаще озвучивается потребность в дальнейшем совершенствовании законодательства, так как обеспечить сохранность персональной информации, попавшей в сеть «Интернет», в настоящее время практически невозможно.

В Европейском сообществе орган, который самостоятельно определяет цели и средства обработки персональных сведений и выступает как физическое или юридическое лицо, орган государственной власти или иной орган считается контролером. Данный субъект обязан сформировать нормативную базу и предпринимать действия, полностью отвечающие принципам обеспечения сохранности персональных сведений [3]. Оператором же выступает субъект, обрабатывающий информацию.

На оператора и контролера возложена обязанность по назначению инспектора по обеспечению сохранности персональной информации. Это влечет введение в штат компаний еще одной должности и дополнительные расходы. Граждане, данные которых используются, имеют право по всем вопросам обратиться непосредственно к инспектору.

Оператор или контролер обязаны сведения об инспекторе сделать публичными и довести их до надзорного органа. В качестве надзорного органа выступает независимый государственный орган, который несет ответственность за отслеживание применения положений Регламента (например, в Германии это Уполномоченное лицо Федеральной комиссии по защите данных). Главы надзорных органов входят в учреждаемый Регламентом Европейский совет по защите данных, основной обязанностью которого является консультирование Европейской Комиссии по вопросам защиты персональных данных, а также издание соответствующих указаний и разъяснений.

В отечественной практике присутствует понятие оператора и надзорного органа. Обрабатывая персональную информацию, оператор (субъект хозяйствования) должен уведомить надзорный орган – Роскомнадзор [1].

Заметим, что с 2017 г. должностные лица Роскомнадзора получили возможность протоколировать административные правонарушения в области обработки персональной информации. Ранее такой возможностью обладала прокуратура. На сайте Роскомнадзора по Северо-Западному федеральному округу представлена статистика в области проверок и правонарушений по рассматриваемому вопросу в Северо-Западном Федеральном округе за период с 01.01.2019 г. по 31.06.2019 г. За 6 месяцев 2019 г. было проведено 31 мероприятие по контролю. При этом выявлено 48 нарушений норм. Выписано 19 предписаний по нейтрализации обнаруженных злоупотреблений и недостатков. Также запротоколировано 1677 административных правонарушений (МВД и прокуратурой – 7). Судами вынесено 500 и оставлено в силе 422 решения/постановления по протоколам об административных правонарушениях. Наложено административных штрафов – 4236800 руб. [4].

За нарушения в области защиты персональных сведений в России предусмотрено несколько видов ответственности [2]:

1. административная – штраф до 75 тыс. рублей;

2. уголовная – штраф до 300 тыс. рублей, дисквалификация до 5 лет, лишение свободы до 4 лет;

3. дисциплинарная – выговор, замечание или увольнение работодателем;

4. материальная – в пределах среднемесячного заработка.

Таким образом, для выполнения положения Закона о защите персональных данных необходимо уведомить Роскомнадзор о намерении обрабатывать личную информацию. При осуществлении работы с персо-

нальной информацией организация обязана, прежде всего, соблюдать законодательство в данной сфере. Информация должна применяться по целевому назначению, поэтому для каждой цели формируется своя информационная база. Информация не должна быть избыточной, ее следует оперативно обновлять и исключать из базы по мере необходимости.

С физического лица должны взять разрешение (согласие) на обработку персональных данных. В нем оговариваются цели, способы обработки, состав сведений и срок использования. Оператор при этом обязан разместить в открытом доступе свой актуальный локальный нормативный акт, определяющий его действия в области обработки и защиты информации. Субъекты должны быть обеспечены возможностью доступа к информации, быть способными ее уточнить, блокировать или сделать запрос на удаление [2].

В Европе надзорные органы также имеют право налагать взыскания на обработчиков данных или контролеров. За нарушение основных принципов обработки данных, включая условия для согласия, прав субъектов данных, трансграничной передачи может быть наложен штраф в размере до 20 млн евро или до 4% выручки. За отсутствие согласия на использование данных детей, нарушения по реализации технических и организационных мер защиты информации, нарушения ведения учета операций по обработке персональных данных возможен штраф до 10 млн евро или до 2% выручки. В то же время при несущественных нарушениях может быть вынесен выговор.

Глобализационные процессы создают достаточное количество проблем, связанных с обеспечением прав граждан по защите их персональной информации. Это свойственно как России, так и Европейскому сообществу. Благодаря цифровизации экономики информация перемещается свободнее, становится более востребованной и доступной. Поэтому необходим действенный механизм постоянного совершенствования нормативной базы в рассматриваемой области.

Отечественная нормативная база в достаточной степени соответствует европейским стандартам. Но внедрение информационных технологий в общественные отношения способствует росту правонарушений в области использования и защиты персональной информации.

Одним из логических действий по совершенствованию отечественной практики стало бы введение новой профессии инспектора по обеспечению сохранности персональных сведений. Указанное должностное лицо (в целях минимизации затрат) должно иметь возможность осуществлять свои профессиональные функции в нескольких организациях. Также следует на сайте Роскомнадзора обеспечить ведение реестра действующих инспекторов. Указанный комплекс действий будет следующим шагом по интеграции России в мировую экономику.

ЛИТЕРАТУРА

1. *Пушинина А.С., Пушинин А.В.* Персональные данные: проблемы сбора и обработки в условиях изменения действующего законодательства // Новеллы права и политики 2017: сб. науч. трудов по материалам Международ. науч.-практич. конф. Гатчина: Изд-во ГИЭФПТ, 2018. С. 50–54.

2. *Пушинин А.В., Пушинина А.С.* О соблюдении законодательства о защите персональных данных при декларировании доходов сотрудниками Пенсионного фонда Российской Федерации // Актуальные проблемы юридической науки и практики: материалы Международ. науч.-практич. конф. Гатчина: Изд-во ГИЭФПТ, 2018. С. 82–86.

3. *Талапина Э.В.* Защита персональных данных в цифровую эпоху: российское право в Европейском контексте // Труды Института государства и права РАН. 2018. № 5. С. 117–150.

4. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций: [сайт]. URL: https://78.rkn.gov.ru/p4657/p14119/p28340/ (дата обращения: 20.08.2019).

5. GDPR (General Data Protection Regulation) Регламент Евросоюза о персональных данных. URL: http://www.tadviser.ru/a/406949 (дата обращения: 20.08.2019).