УДК 349.2
https://doi.org/10.36906/NVSU-2022/30

Якубова Л.А., канд. ист. наук, ORCID: 0000-0002-4721-7317,
Слюсарчук О.И.
Нижневартовский государственный университет
г. Нижневартовск, Россия

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В ОРГАНАХ ГОСУДАРСТВЕННОЙ И МУНИЦИПАЛЬНОЙ ВЛАСТИ: НОВЫЕ ВЫЗОВЫ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Аннотация. Статья посвящена организации сбора, обработки, хранения персональных данных граждан в силу глобального незаконного распространения личных данных граждан в целях мошеннических операций. Особое значение эта проблема имеет для органов государственной и муниципальной власти в условиях цифровой трансформации.
Ключевые слова: персональные данные; органы государственной власти; органы муниципальной власти; правовое регулирование; личная информация.

В последние годы все большее внимания уделяется вопросам обеспечения сохранности персональных данных граждан. Введённый в силу Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» в 2011–2014 годах был в значительной мере детализирован сразу несколькими подзаконными документами всех основных регуляторов в данной области: Федеральной службы по контролю в сфере связи, информационных технологий и массовых коммуникаций, Федеральной службы по промышленному и экспортному контролю и Федеральной службы безопасности Российской Федерации[1].

Регулирование сбора, обработки, а также использования персональных данных является ключевой задачей по обеспечению безопасности личной жизни граждан. С развитием цифровизации и влияния интернета на жизнь людей, увеличилось повсеместное распространение персональных данных о гражданах. В поисковых системах Google или Яндекс, при малом количестве информации о человеке, например, фамилия, имя, примерное место проживание, на некоторых ресурсах можно обнаружить большой список персональных данных, которые добровольно не предоставлялись этим ресурсам. Это часто свидетельствует о том, что гражданин стал жертвой со стороны недобросовестного оператора по обработке персональных данных. Данные действия со стороны недобросовестного оператора по обработке персональных данных, приводят к возможным *манипулятивным* воздействиям на владельцев персональных данных. Таким образом, большое количество людей сталкивается с мошенническими действиями, при которых используется личная информация в различных целях, в том числе для искажения существующей информации, тем самым очерняя личность

[1] Федеральный закон от 27 мая 2003г. № 58-ФЗ «О системе государственной службы Российской Федерации» (ред. от 23.05.2016) // Собрание законодательства РФ. 2018. № 22. Ст. 2063. С. 3.

человека. Кража и намеренное распространение персональных данных, становится наиболее острой проблемой не только в России, но и за рубежом. Мошенники, используя скоростное развитие цифровизации, находят все больше новых способов для получения и продажи личной информации.

Такое нарушение закона имеет место в медицинских учреждениях, банковских сферах, в сфере развлекательных услуг, а так же в государственных и муниципальных органах. В рамках определения группы персональных данных действующим законодательством выделяются отдельные информационные группы, для которых устанавливаются специальные режимы обработки: отдельные категории персональных данных, отражающие национальность, политические взгляды, религиозные или философские убеждения, состояние здоровья и интимную жизнь заинтересованного лица; биометрические собственные данные, отражающие физиологические и биологические возможности человека, на основании которых может быть установлена его личность; публичные персональные данные, изображающие сведения о субъекте персональных данных из общественных источников. Согласно статье 7 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» общедоступной считается информация, доступ к которой не ограничен. К таким общедоступным источникам персональной информации относятся различные руководства, адресные книги, энциклопедии, изданные в печатном или электронном виде, опубликованные в сети Интернет или собранные в библиотеках, архивах, государственных учреждениях и органах местного самоуправления[2].

– иные категории персональных данных – персональные сведения, не относящиеся к группе специальных, биометрических и общедоступных персональных данных.

Оценка массива существующего законодательства в сфере информационного права, персональных данных, а также доступных материалов специальной литературы и сети Интернет показал, что материалы, относимые к категории персональных данных, могут быть условно разделены на основные группы и определены следующим образом:

персональные данные: ФИО и сведения об их изменении, место, день, месяц и год рождения; фотографическое изображение человека, семейное положение, сведения о близких родственниках (фамилия, имя, отчество, степень родства, год рождения, место работы, должность, сведения о доходах, контактный телефон);

государственные удостоверения личности: паспортные данные; регистрация и фактический адрес проживания; гражданство; индивидуальный налоговый номер; страховой номер индивидуального лицевого счета застрахованного лица; номер запасного свидетельства пенсионного страхования; данные полиса медицинского страхования; информация о государственных наградах и поощрениях; сведения о воинском учете (специальности воинского учета);

данные трудовых взаимоотношений: сведения о месте работы (должность, структурное подразделение, категория квалификации, сведения об испытательном сроке работника, период работы, стаж, сведения об аттестации, табельный номер); информация о поощрениях и

[2] Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 02.07.2021) «О персональных данных». С. 1-4.

взысканиях; сведения о прошлых местах работы и особенностях рабочей деятельности; основание прекращения трудового договора (увольнения); сведения об отпуске и командировках; сведения о временной нетрудоспособности;

профессиональные данные: образование (название учебного заведения, место и год окончания, наделенная квалификация); сведения о повышении квалификации и профессиональной переподготовке; сведения о профессиональной пригодности; сведения о наличии специальных знаний в определенных сферах; сведения о знании иностранных языков; сведения о существовании ученой категории и ученого звания [1, с. 84].

Государственные и муниципальные органы создают государственные или муниципальные информационные системы персональных данных в пределах своих полномочий, но при всем этом они должны руководствоваться требованиями в соотношении с федеральным законодательством.

Учитывая, что персональные данные являются одним из видов конфиденциальной информации, совершенствование правовых механизмов, регулирующих и осуществляющих контроль за оборотом персональных данных, совершенствование средств и механизмов защиты такой информации является актуальной задачей всего государственного аппарата Российской Федерации [3, с. 85].

Для защиты персональных данных используются различные варианты:

- Технические средства. Они являются частью программы мероприятий по защите программного обеспечения от несанкционированного доступа. Для защиты программного обеспечения необходимо привлекать ИТ-специалистов, моделировать угрозы, определять степень защиты персональных данных, обеспечивать надежность.
- Физические средства. Это сокращение доступа к персональным данным для посторонних лиц в виде разрешения работы с информацией только для определенных сотрудников; введение контроля доступа; организация мест хранения данных и др.
- Организационные и юридические меры. Они включает в себя разработку и внедрение руководства по обработке персональных данных компанией, положений о защите данных, издание указов о назначении ответственного лица и осуществление мер контроля.

В случае правонарушений предусмотрен полный спектр ответственности: дисциплинарная – за неправомерную обработку данных сотрудником компании; гражданско-правовая – в виде возмещения убытков, возмещения морального вреда; административная – если это предусмотрено законом об административных правонарушениях; уголовная – за причинение вреда наиболее охраняемым общественным интересам. Наиболее распространенным наказанием является наложение штрафа [2, с. 54].

Статья 13.11 Закона об административных преступлениях Российской Федерации устанавливает девять составов правонарушений, в том числе ответственность за обработку данных, если это не предусмотрено законом, в случае отклонений от целей, поставленных компанией и иных неправомерных действий[3].

[3] Гражданский кодекс Российской Федерации (часть первая) 30 ноября 1994г. № 51-ФЗ (ред. от 03.08.2018) // Собрание законодательства РФ. 1994. № 32. Ст. 3301. С. 4.

У каждого сотрудника есть ряд прав по защите его личных данных. Персональные данные сотрудника обрабатываются в соответствии со статьей 86 ТК РФ. Под подготовкой персональных данных понимается поиск, систематизация, накопление, хранение, уничтожение, использование, распространение, обезличивание, блокирование, уничтожение персональных данных в интересах сотрудника[4].

Сбор, обработка, хранение персональных данных со стороны работодателя требуют письменного согласия со стороны сотрудника государственного или муниципального органа.

Передача персональных данных третьим лицам, если таковое условие не указано в письменном согласии по обработке персональных данных, – запрещена. Исключениями из правил, могут считаться мотивированные запросы на передачу данных из органов исполнительной власти, органов судебной власти и других. Они вправе запрашивать и обрабатывать персональные данные работников в рамках своей компетенции, без согласия субъектов персональных данных.

В силу развития цифровизации органам государственной и муниципальной власти требуется размещать информацию о своей деятельности в сети интернет, таким образом, возникают новые аспекты в защите персональных данных работников.

Например, принимая во внимание новые изменения в Федеральном Законе «О персональных данных» от 01.03.2021г., работодатель при размещении персональных данных сотрудника на сайте муниципального или государственного органа, должен заключить с работником новое согласие на распространение персональных данных. В ином случае размещение фотографий и имен сотрудников без дополнительного согласия работника может считаться нарушением закона.

Литература

1. Борисова С.А. Общие требования при обработке персональных данных работника и гарантии их защиты // Трудовое право. 2016. № 5. С. 35-39.

2. Бундин М.В. Персональные данные как информация ограниченного доступа // Информационное право. № 1. 2019. С. 10-14.

3. Салимова Т.А., Атнабаева Ю.В. Особенности обеспечения безопасности персональных данных в Российской Федерации // Юридические науки. 2021. № 11-1 (62). С. 119-122.

© Якубова Л.А., Слюсарчук О.И., 2022

[4] Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 02.07.2021) «О персональных данных». С. 4.