УДК 34.096

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

Каменнова Валерия Владимировна, студентка юридического факультета ФГБОУ ВО Саратовской государственной юридической академии;
Научный руководитель: Анисимова Алина Сергеевна, старший преподаватель кафедры информационного права и информационных технологий СГЮА, к.ю.н.

Практически каждый день мы сталкиваемся с тем, что нам необходимо предоставлять свои персональные данные (регистрация на веб-сайте, покупки в онлайн-магазинах и т.д.). Кто отвечает за сохранность личных данных и в каких случаях информацией лучше не делиться?

Ключевые слова: персональные данные, ответственность, защита, правонарушение, информация, правовое регулирование.

PERSONAL DATA PROTECTION

Kamennova Valeria Vladimirovna, a student of the Law Faculty of the Saratov State Law Academy;
Supervisor: Alina S. Anisimova, Senior Lecturer of the Department of Information Law and Information Technologies of the SSLA, Candidate of Law.

Almost every day we are faced with the fact that we need to provide our personal data (registration on the website, purchases in online stores, etc.). Who is responsible for the security of personal data and in which cases it is better not to share information?

Key words: personal data, liability, protection, offense, information, legal regulation.

Важной современной тенденцией развития информационного общества является возрастание интереса к персональным данным. В Федеральном

законе «О персональных данных»[1] так называют информацию, которая позволяет определить личность пользователя. **Персональные данные** - это любая информация о физическом лице, в частности, фамилия, имя, отчество, место и дата рождения, место проживания и регистрации, социальное, имущественное и семейное положение, профессия, образование, доходы и другое. При этом пароли к аккаунтам не являются персональными данными, т. к. не сообщают ничего о человеке.

Сбором такой информации занимаются государственные или муниципальные органы, практически любые юридические лица, а также физические лица (п. 2 ст. 3 ФЗ «О персональных данных»). Все они выступают в качестве операторов персональных данных и несут ответственность за их сохранность. На практике оператором является любая организация, в которой есть наёмный труд, будь то школа, больница или банк. Например, желая трудоустроиться и придя на собеседование, потенциальные работники получают для заполнения анкету с подробным перечнем вопросов о себе. По сути, даже записываясь на любые курсы или приобретая абонемент в фитнес-клуб, мы делимся своими персональными данными. А сколько информации о себе мы оставляем в сети? По справедливому замечанию руководителя отдела аналитики Positive Technologies Евгения Гнедина: «Всем нужно понять: все, что мы оставляем в интернете, там и останется, а возможно, будет использовано с недобросовестными целями»[2]. На «черном рынке» персональные данные стоят кратно больше, чем даже полные сведения банковской карты, хотя, казалось бы, все должно быть наоборот.

Любое юридическое лицо в силу требований Федерального закона «О персональных данных» обязано принимать меры по защите персональных

[1] Федеральный закон "О персональных данных" от 27.07.2006 № 152-ФЗ [Электронный ресурс] // КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 25.03.2021).

[2] Граждане дорого стоят [Электронный ресурс] // Российская газета. URL: https://rg.ru/2020/02/06/rastet-interes-zloumyshlennikov-k-personalnym-dannym.html (дата обращения: 06.04.2021).

данных, при этом перечень таких мер оно вправе определять самостоятельно. Мероприятия по защите персональных данных можно разделить на две большие подгруппы: по внутренней и внешней защите персональных данных.

К мерам по внутренней защите персональных данных относятся следующие действия:

- ограничение числа работников (с регламентацией их должностей), которым открыт доступ к персональным данным;

- назначение ответственного лица, обеспечивающего исполнение организацией законодательства в рассматриваемой сфере;

- издание внутренних документов по защите персональных данных, осуществление контроля за их соблюдением;

- ознакомление работников с действующими нормативами в области защиты персональных данных и локальными актами и т.д.

Среди мер по внешней защите персональных данных следует выделить такие:

- введение пропускного режима, порядка приема и учета посетителей;

- внедрение технических средств охраны, программных средств защиты информации на электронных носителях и др.

Главным требованием, предъявляемым к обладателю персональных данных, полученных от работников или клиентов, является обеспечение их сохранности. И ладно, если утечка заканчивается телефонным спамом, но не редки случаи, когда люди неожиданно для себя узнают, что они являются директорами обанкротившихся фирм или обладателями кредитов. В такой ситуации может оказаться кто угодно.

Высокий уровень сохранности персональных данных обеспечивают в большинстве случаев только крупные компании, потому что у них предусмотрены специальные отделы безопасности. Надо понимать, что суммарно большая часть утечек происходит не от них. Данные организации полностью исполняют ФЗ «О персональных данных» и осознают

ответственность за персональные данные, которые они могут использовать только в рамках договора для оказания услуг или исполнения иного обязательства, а не для того, чтобы передать их мошенникам. Лица, виновные в нарушении требований закона «О персональных данных», наряду с административной, дисциплинарной, материальной и уголовной ответственностью, несут и гражданско-правовую ответственность.

Однако даже крупные компании не всегда могут обеспечить сохранность данных, а новости об утечке персональных данных стали для нас привычной реальностью, которая возмущает с каждым днём всё меньше. В феврале 2021 года информационный сайт РИА Новости опубликовали список «громких» утечек 2020-2021 года[1]. Среди источников утечек оказались такие крупнейшие организации, как «Яндекс», Сбербанк, Россельхозбанк, Тинькофф банк, Райффайзенбанк, Авито, Юла и многие другие. Количество опубликованных и продаваемых данных, т.е. количество пострадавших, колеблется от нескольких до сотен тысяч. По данным РБК, в начале апреля 2021 года стало известно, что хакеры, воспользовавшись уязвимостью в дистанционной подаче первичных заявок на получение кредита наличными, выставили на продажу данные граждан, которые обращались в банк «Дом.РФ» для оформления потребительского кредита[2]. Записи могут содержать полный набор персональных данных, которые требуются для оформления кредита: Ф.И.О., дата рождения, сумма и вид кредита, номер телефона, почтовый ящик, паспортные данные, ИНН, СНИЛС, домашний адрес, адрес места работы, должность, размер дохода и другие сведения. Согласно объявлению, полная база стоит 100 тыс. руб.

[1] Громкие утечки персональных данных в России в 2020-2021 году [Электронный ресурс] // РИА Новости. URL: https://ria.ru/20210212/utechki-1597206122.html (дата обращения: 27.03.2021).

[2] Данные желающих взять кредит в банке «Дом.РФ» выставили на продажу [Электронный ресурс] // РБК Новости. URL: https://www.rbc.ru/finances/05/04/2021/606884099a7947c826949628?from=article_link (дата обращения: 17.04.2021).

Отдельные строки с данными за 2021 год продаются за 15 руб., за вторую половину 2020 года — 10 руб., за первую половину 2020 года — 7 руб.

Всё это говорит о том, что даже сегодня при современном уровне развития технологий ни одна организация, включая органы государственной власти, не может гарантировать абсолютную защиту личных данных от мошенников и нелегальных учреждений.

Целесообразным представляется упоминание последних изменений в ФЗ «О персональных данных», вступивших в силу с 1 марта 2021 года. Введено новое понятие «персональные данные, разрешенные для распространения». Речь идет о распространении персональных данных неограниченному кругу лиц. Этот новый термин, по сути, пришел на смену прежнему – «общедоступные персональные данные». Судя по пояснительной записке к законопроекту, главная цель поправок – ограничить неконтролируемое использование персональных данных, размещенных на сайтах и в других открытых источниках. Получив персональные данные, оператор не вправе распространять их, как это было раньше. В связи с этим для обработки персональных данных, разрешенных для распространения, нужно получать отдельное согласие лица, предоставившего такие данные. То, каким образом данные изменения отразятся на качестве сохранности персональных данных, покажет время.

Таким образом, технологии по систематизированному сбору, хранению и обработке персональных данных используются как в положительных целях, так и для осуществления противозаконной деятельности, о чем свидетельствуют данные выше. Значимость и ценность персональных данных будут усиливаться, поэтому в будущем у пользователей увеличится желание и возможности для принятия решений о том, что для них важно и кому они передают свои данные.

ЛИТЕРАТУРА

1. Федеральный закон "О персональных данных" от 27.07.2006 № 152-ФЗ [Электронный ресурс] // КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 25.03.2021).

2. Граждане дорого стоят [Электронный ресурс] // Российская газета. URL: https://rg.ru/2020/02/06/rastet-interes-zloumyshlennikov-k-personalnym-dannym.html (дата обращения: 06.04.2021).

3. Громкие утечки персональных данных в России в 2020-2021 году [Электронный ресурс] // РИА Новости. URL: https://ria.ru/20210212/utechki-1597206122.html (дата обращения: 27.03.2021).

4. Данные желающих взять кредит в банке «Дом.РФ» выставили на продажу [Электронный ресурс] // РБК Новости. URL: https://www.rbc.ru/finances/05/04/2021/606884099a7947c826949628?from=article_link (дата обращения: 17.04.2021).