МЕРЫ ЗАЩИТЫ И ОГРАНИЧЕНИЯ ПРИ ПОЛУЧЕНИИ ДОСТУПА К ИНФОРМАЦИИ И К ПЕРСОНАЛЬНЫМ ДАННЫМ В РОССИЙСКОЙ ФЕДЕРАЦИИ

С.Г. Янбаев, *магистрант*
И.И. Ларинбаева, *доцент*
Уфимский университет науки и технологий
(Россия, г. Уфа)

DOI:10.24412/2500-1000-2024-2-3-181-185

Аннотация. *В данной статье рассматривается актуальная проблема незаконной передачи персональных данных и клиентских баз третьим лицам, особенно в условиях интернет-развития и социальных сетей. Автор подчеркивает необходимость эффективной защиты персональных данных граждан, выделяя противоречия между удобством использования интернет-ресурсов и необходимостью обеспечения безопасности информации. Автор также призывает к совершенствованию систем обезличивания персональных данных, особенно в медицинской сфере, и устанавливает важность минимизации запроса данных при трудоустройстве, с предложением ввести юридическую ответственность за незаконный запрос личной информации.*

Ключевые слова: *персональные данные, интернет и социальные сети, обезличивание, трудоустройство, защита данных.*

В условиях ужесточения рыночной конкуренции между производителями разнообразных товаров и услуг, с одной стороны, и расширения их возможностей по использованию прогресса в сфере информационно-коммуникационных технологий, – с другой, появляются новые формы воздействия, в том числе незаконного, на потенциальных потребителей с использованием баз их персональных данных [1, с. 14].

Практически каждый человек имеет компьютер, ноутбук или планшет, смартфон, а они в большинстве случаев подключаются к сети интернет. Одни люди держат различные фото и видео на электронных устройствах, другие выкладывают их в различные социальные сети, третьи используют привязку банковской карты к различным приложениям. Практически каждое приложение просит заполнить те или иные персональные данные. Информационные технологии развиваются, с каждым днем появляются новые базы обработки или хранения персональных данных. Но не всегда такие базы являются надежными.

Таким образом, персональные данные весьма успешно могут использоваться для рекламы в рамках телефонного обзвона, для других личных корыстных целей. Поэтому спрос на персональные данные есть всегда, а в задачу государства входит создание необходимых мер для защиты персональных данных граждан.

В современном российском законодательстве определение персональных данных содержится в статье 3 Федерального закона «О персональных данных». Согласно этому закону, персональными данными считается любая информация, которая может быть прямо или косвенно связана с определенным физическим лицом, то есть субъектом персональных данных. Примерами персональных данных могут быть фамилия, имя, отчество, дата рождения, место рождения, адрес проживания, паспортные данные, номер телефона, семейное положение, религиозные убеждения, информация о доходах, политические убеждения и другая аналогичная информация.

Важно отметить, что персональные данные делятся на два типа: номинативные и иные. Номинативные данные представляют собой информацию, которая позволяет однозначно идентифицировать конкретное лицо. К этой категории отно-

сятся биометрические данные, такие как отпечатки пальцев или скан сетчатки глаза, которые уникальны для каждого человека и могут использоваться для точной идентификации.

К иной информации относятся данные о доходах, месте работы, политических убеждениях, медицинских записях, наличии судимости и подобные сведения. Эти данные, хотя и могут содержать информацию о личности, не всегда позволяют однозначно идентифицировать субъекта персональных данных.

Современное российское законодательство постоянно расширяет перечень сведений, которые могут быть признаны персональными данными. Важным критерием здесь является возможность идентификации лица по предоставленной информации. Это дает гибкость в судебных процессах, учитывая разнообразие информации, которая может быть связана с личностью субъекта персональных данных.

Авторы также отмечают, что институт персональных данных продолжает развиваться в России, и современное законодательство подвергается реформам, особенно в связи с развитием информационных технологий. Эти реформы включают в себя добавление сетевых идентификаторов, таких как пароли, пользовательские имена и другие, в понятие персональных данных. Таким образом, законодательство широко подходит к определению персональных данных, учитывая разнообразие информации, которая может быть связана с личностью человека [2, с. 25].

Рекламные и назойливые телефонные звонки нарушают спокойствие граждан, их право на неприкосновенность частной жизни, наносят моральный вред. Многие звонки способны причинить значительный финансовый вред, ведь часто граждане перезванивают на дозвоны и с их счетов снимаются немалые деньги за исходящие звонки. Между тем, таких обзвонов со сбросом телефона много и большая часть из них производится автоматизировано, без участия человека. То есть масштаб такого мошенничества растет. В первую очередь страдают самые доверчивые и уязвимые категории граждан: пенсионеры, инвалиды, матери-одиночки, многодетные матери.

Также при приеме на работу часто работодатель требует предоставить персональные данные в большем объеме, чем это необходимо для осуществления трудовых обязанностей. Так, работодатели часто пытаются узнать, если ли маленькие дети у будущего работника, есть ли бабушки и дедушки на случай того, если ребенок заболеет и его необходимо будет с кем-то оставить. Работодатели не хотят, чтобы новый сотрудник уходил на больничные. Также есть случаи, когда работодатели интересуются такими личными данными работника, как наличие ипотеки, кредитов с той целью, чтоб иметь возможность понять, можно ли установить работнику зарплату чуть поменьше планируемой, а также для того, что понять, будет ли такой работник «держаться» за работу.

Работодатели при приеме на работу на должности без вредных условий работы часто незаконно запрашивают у сотрудника медицинские справки с более полным перечнем информации о здоровье. Так, работодатели не хотят брать на работу сотрудника, который будет слабым и утомляемым.

Стоит отметить, что работодатель обязан ознакомить работника с уровнем защиты его персональных данных и условиями обеспечения информационной безопасности его персональных данных, но это на практике не делается. Между тем, часто анкеты просят заполнить заранее на сайте организации. На сайте просят загрузить даже фото, хотя работник должен иметь право отказаться от этого. При этом часто стоит условие заполнения всех полей анкеты.

Не заполнение хотя бы одного поля приведет к невозможности ее отправки. Стоит заметить, что любой сбой в системе безопасности и все заполненные и отправленные данные по сети интернет будут в открытом доступе [3, с. 135].

Недостаточная регламентация в законодательстве перечня информации, необходимой для трудоустройства и недостаточная регламентация юридической ответ-

ственности позволяют уходить от ответственности многим работодателям.

Государственная защита персональных данных строится исходя из регламентированных конституционных положений, которые провозглашают неприкосновенность частной жизни, право на личную и семейную тайны, а также права человека, принятые на основе международных обязательств Российской Федерации, в том числе вытекающих из Европейской конвенции о защите физических лиц при автоматизированной обработке персональных данных, а также из Договора о Евразийском экономическом союзе.

Государство в лице уполномоченных органов контролирует соблюдение установленных законодательством мер. Уполномоченный орган по защите прав субъектов персональных данных обеспечивает, организует и осуществляет государственный контроль и надзор за соответствием обработки персональных данных требованиям закона.

Право на защиту персональных данных является относительным, а не абсолютным. Поэтому при установлении требований к защите персональных данных важным моментом является обеспечение баланса интересов личности, общества, государства и бизнес-структур. Все это подразумевает соразмерность, обоснованность и реальную выполнимость требований, включая требование обеспечить «адекватную» защиту персональных данных. Юридические и технические меры защиты персональных данных должны быть сбалансированы и адекватны, чтобы не создавать помех развитию рынка, а также не нарушать интересы субъектов персональных данных.

Стоит также отметить, что есть и такие персональные данные, которые в соответствие с законом, должны быть обнародованы. К таким персональным данным, например, относятся некоторые персональные данные кандидатов в депутаты

На сегодняшний день разработаны различные меры для защиты персональных данных при их обработке в информационных системах, утверждены антивирусные программы. Федеральной службой по техническому и экспортному контролю также совершенствуются меры для повышения безопасности хранения персональных данных. Конечно, пока защита несовершенна, существуют утечки информации через сеть интернет.

Происходили крупные утечки персональных данных из Пенсионного фонда России, Сбербанка России. Среди персональных данных были фамилии и имена клиентов, их телефонные номера, номера налогоплательщиков, данные пенсионных свидетельств, данные страховых и накопительных частей пенсии и др.

Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

На сегодняшний день, к сожалению, часты случаи незаконной передачи персональной информации, клиентской базы третьим лицам. Пожалуй, почти каждому человеку хоть раз звонили компании, ранее о которых человек не слышал и не предоставлял разрешения на допуск к персональным данным, однако такие компании обращаются по имени и отчеству и знают другую идентифицирующую человека информацию, например, о наличии у него кредиторской задолженности, либо о рождении в семье ребенка, смерти близкого родственника, покупке квартиры.

Такие организации используют полученную незаконным путем информацию о персональных данных человека в своих коммерческих целях, предлагая выдачу кредита на более выгодных условиях, юридическую помощь, другие товары и услуги в соответствии с последними событиями в жизни человека, о которых компаниям известно. А с развитием интернет и социальных сетей, получить доступ к персональным данным человека и воспользоваться этими данными становится все проще.

Для эффективной защиты персональных данных государству следует совершенствовать электронную защиту. Ведь при реализации прав граждан на доступ к информации о деятельности органов государственной власти и органов местного самоуправления, получения различных государственных и муниципальных услуг, участии в федеральных государственных программах нужно неоднократно размещать в сети Интернет свои персональные данные, например, при регистрации на портале государственных услуг.

В последнее время распространяется и регистрация и использование электронной подписи граждан на портале государственных услуг, с помощью которого гражданин без личного посещения учреждений по оказания государственных и муниципальных услуг может реализовать свои права. Взлом такой информации, ее утечка позволит злоумышленникам от имени гражданина совершать операции, последствия которых будет очень сложно устранить. Это неизбежно налагает на субъекты правоотношений дополнительную ответственность по гарантированию безопасности регистрируемой информации и ее хранения от третьих лиц.

Наряду с возможными отрицательными последствиями в случае утечки информации при использовании сети интернет, нельзя не отметить большие плюсы и возможности, которые дает сеть интернет. С помощью сети интернет люди сокращают время на получение необходимой информации, имеют возможность сдавать декларации и подписывать их, записываться к врачу, к органам государственной власти, заказывать документы, предоставлять свои данные на регистрацию без личного присутствия и многое другое. Государству лишь следует уделить больше внимания защите персональных данных при реализации гражданами своих прав и обязанностей с помощью сети Интернет.

Государство должно обеспечить контроль соблюдения законодательства о персональных данных лицами, которые получили доступ к таким данным. Оператор, осуществляющий обработку персональных данных, обязан получить согласие субъекта персональных данных на обработку его персональных данных.

Обработка персональных данных допускается также без разрешения гражданина в случаях, когда она нужна для исполнения полномочий федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг. Например, в случае регистрации лица на едином портале государственных и муниципальных услуг и (или) региональных порталах государственных и муниципальных услуг [4].

Свободная обработка персональных данных допускается и в случаях, когда она необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект персональных данных, а также в случаях, когда согласие получить невозможно, но данные необходимы для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных. Обработка персональных данных объектов государственной охраны и членов их семей осуществляется с учетом особенностей, предусмотренных законом [5].

Из вышеизложенного следует, что нормативно-правовое регулирование исследуемой темы следует совершенствовать. Доказательством этому утверждению выступают многочисленные утечки баз данных. Стоит разработать и законодательно закрепить процедуру обезличивания персональных данных как способ обеспечения безопасности персональных данных, когда без дополнительных источников информации станет невозможно определить, к кому относятся те или иные личные данные.

Особенно это актуально в области медицины. Это позволит в случае утечки информации исключить возможность определения ее принадлежности к конкретному лицу.

С этой целью рекомендуется разработать специальные информационные про-

граммы с различными алгоритмами обезличивания. Необходимо также установить необходимый минимум персональных данных, требующийся при приеме на работу. При этом дополнительные сведения могут быть затребованы в случаях, если это напрямую связано с занимаемой должностью. Необходимо установить юридическую ответственность за злоупотребление правом сбора информации при приеме на работу, когда у кандидата требуют предоставить дополнительные личные данные, а в этом необходимости нет.

Библиографический список

1. Лаптева Е.В. Механизмы защиты прав граждан при использовании ими телефонных средств связи // Beneficium. – 2019. – № 2 (31). – С. 71.

2. Батлынова А.Н. Персональные данные // Административное право. – 2020. – № 4. – С. 25.

3. Трошина С.М., Павловская А.В Проблемы совершенствования мер защиты персональных данных // Вестник Томского государственного университета. – 2018. – № 23. – С. 135.

4. Федеральный закон от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» (с посл. изм. и доп. от 31 июля 2023 года № 397-ФЗ) // Официальный интернет-портал правовой информации. – [Электронный ресурс]. – Режим доступа: http://www.pravo.gov.ru/ (дата обращения: 05.12.2023).

5. Федеральный закон от 27 мая 1996 года № 57-ФЗ «О государственной охране» (с посл. изм. и доп. от 4 августа 2023 года № 440-ФЗ) // Официальный интернет-портал правовой информации. – [Электронный ресурс]. – Режим доступа: http://www.pravo.gov.ru/ (дата обращения: 05.12.2023).

MEASURES OF PROTECTION AND RESTRICTIONS IN OBTAINING ACCESS TO INFORMATION AND PERSONAL DATA IN THE RUSSIAN FEDERATION

S.G. Yanbaev, *Graduate Student*
I.I. Larinbayeva, *Associate Professor*
Ufa University of Science and Technology
(Russia, Ufa)

Abstract. *This article discusses the actual problem of illegal transfer of personal data and customer databases to third parties, especially in the context of Internet development and social networks. The author emphasizes the need for effective protection of personal data of citizens, highlighting the contradictions between the convenience of using Internet resources and the need to ensure information security. The author also calls for the improvement of systems for depersonalizing personal data, especially in the medical field, and establishes the importance of minimizing data requests during employment, with a proposal to introduce legal liability for illegal requests for personal information.*

Keywords: *personal data, Internet and social networks, depersonalization, employment, data protection.*