

*Михалева Т.А.,
студент магистратуры
2 курс, Институт права
Уфимский университет науки и технологии
Россия, г. Уфа*

ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ПРАВИЛ РАБОТЫ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

***Аннотация:** в данной статье автор анализирует ответственность за нарушение правил работы с персональными данными в Российской Федерации. В работе делается вывод, что на сегодняшний день соответствующие нормы, регламентирующие ответственность за незаконное использование персональных данных, можно найти в ТК Российской Федерации, КоАП Российской Федерации, УК Российской Федерации. Общие положения отражены и в ГК Российской Федерации. Следует улучшить взаимодействие государства и граждан, повысить уровень правовой грамотности населения, а также ответственность граждан при подписании согласия и иных форм предоставления персональных данных. Все это позволит качественно решить имеющиеся проблемы.*

***Ключевые слова:** обеспечение конфиденциальности, персональные данные, интернет, уполномоченный орган, приватность.*

***Annotation:** in this article, the author analyzes the responsibility for violating the rules for working with personal data in the Russian Federation. The paper concludes that today the relevant rules governing liability for the illegal use of personal data can be found in the Labor Code of the Russian Federation, the Code of Administrative Offenses of the Russian Federation, the Criminal Code of the Russian Federation. General provisions are reflected in the Civil Code of the*

Russian Federation. It is necessary to improve the interaction between the state and citizens, increase the level of legal literacy of the population, as well as the responsibility of citizens when signing consent and other forms of providing personal data. All this will qualitatively solve the existing problems.

Key words: *privacy, personal data, Internet, authorized body, privacy.*

Персональные данные человека в настоящее время являются той критически уязвимой информацией о личности, без должной защиты способной создать благоприятные условия для различного рода правонарушений с ее незаконным использованием, к тому же стремительно развивающиеся доступные информационные технологии облегчают этот процесс¹. Существует ряд проблем, связанных с обеспечением конфиденциальности персональных данных в интернете. Одна из них заключается в том, что информация, размещенная онлайн, может оставаться доступной для всех на неопределенный срок, что может привести к нарушению частной жизни и безопасности людей.

Законодательство, регулирующее обработку и защиту персональных данных, часто не успевает за стремительным развитием технологий и общественных потребностей. В результате этого законы и положения могут быть устаревшими или недостаточно эффективными в борьбе с современными угрозами конфиденциальности.

В Российской Федерации есть законодательство, которое регулирует обработку персональных данных. Оно предусматривает права и средства защиты персональных данных субъектов. Например, субъекты могут обратиться в суд или к уполномоченному органу по защите персональных данных в случае нарушения их прав. Однако, несмотря на это, некоторые

¹ Прохорова Т.Ю. К вопросу о нормативно-правовом регулировании защиты персональных данных // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2016. № 1 (33). С. 318.

аспекты защиты персональных данных могут быть недостаточно прописаны или подробно регламентированы.

Важно постоянно обновлять законодательство в области персональных данных, чтобы соответствовать современным вызовам и технологиям. Это также требует повышения осведомленности граждан о их правах и обязанностях в отношении защиты персональных данных. Только так можно обеспечить эффективную защиту личной информации и приватности в сети»².

На сегодняшний день статья 24 Закона № 152-ФЗ «О персональных данных» прямо указывает виды ответственности за нарушение предписаний федерального закона. Лица, нарушившие предписания закона «О персональных данных», несут ответственность:

- дисциплинарную (например, выговор);
- гражданскую (гражданско-правовые санкции: компенсации имущественных потерь и морального вреда)³;
- административную (штраф);
- уголовную (обязательные работы, ограничение свободы, лишение свободы);
- иную, предусмотренную законодательством Российской Федерации.

Также стоит учесть, что согласно статье 5.39 КоАП Российской Федерации, неправомерный отказ в предоставлении гражданину и (или) организации информации, предоставление которой предусмотрено законом, несвоевременное ее предоставление либо предоставление заведомо недостоверной информации ведет к административному штрафу на должностных лиц в размере от 5 тыс. до 10 тыс. руб.

Согласно статье 19.7 КоАП Российской Федерации, непредставление или несвоевременное представление в государственный или иной уполномоченный орган сведений, представление которых предусмотрено

² Крюкова Д.Ю., Мокрецов Ю.В. Актуальные проблемы правового регулирования оборота и защиты персональных данных в России // Пенитенциарная наука. 2019. № 2 (38). С. 35.

³ Трофимова И.А., Питько Е.В. Особенности гражданско-правовой ответственности за нарушение норм, регулирующих защиту персональных данных работников // Пробелы в российском законодательстве. 2016. № 3. С. 138.

законом либо предоставление таких сведений в неполном объеме или в искаженном виде наказывается административным штрафом в размере: на граждан – от 100 до 300 руб., на должностных лиц – от 300 до 500 руб., на юридических лиц – от 3 тыс. до 5 тыс. руб.

Статья 86 ТК Российской Федерации регламентирует правила, которые должны соблюдать работодатели при обработке и хранении персональных данных работника и потенциальных работников. Отмечено, что объем состава персональных данных и цели их обработки может устанавливать лишь федеральное законодательство.

Таким образом, требовать какую-либо еще информацию о частной жизни работника работодатель не вправе. Также отмечено, что сведения о персональных данных работника работодатель вправе получать от него самого, а у третьих лишь после уведомления и письменного согласия потенциального работника.

Работодатель должен под подпись ознакомить работника о целях обработки персональных данных и способе их хранения. Известны случаи, когда при приеме на работу работодатели уже были в курсе истории болезней новых работников⁴. Передача персональных данных медицинского характера может свободно осуществляться через сетевые ресурсы, что упрощает незаконное распространение индивидуальной информации. Нельзя допускать, чтобы данные медицинских осмотров попадали в руки третьих лиц.

Необходимо ужесточить контроль за персональной информацией медицинского характера. Необходимо четко регламентировать, что в каждой организации должны быть ответственные лица за доступ к персональным данным, их обработке. Следует создать способы отслеживания передачи информации персонального характера через сеть интернет и блокировать незаконную передачу.

⁴ Макаревич М.Л., Бутырская К.Е., Наумова С. И. Проблема правовой защиты персональных данных работника торгового предприятия // Инновационная экономика: перспективы развития и совершенствования. 2019. № 3 (21). С. 64.

Между тем, стоит отметить, что часто работодатели при приеме на работу потенциального работника часто звонят на предыдущее место его работы и требуют дополнительную информацию о личности, привычках, семье, о характере. В большинстве случаев предыдущий работодатель предоставляет такую информацию сразу же по телефону, иногда в письменной форме в виде характеристики.

Между тем, нельзя признать законной распространение и получение такой информации, тем более, если работник согласия на такое распространение не давал. Будет законным, если работодатель обратится непосредственно к потенциальному работнику с просьбой предоставить информацию о частной жизни работника, его персональные данные. И если работник согласен, он ее может предоставить или запросить характеристику с предыдущего места работы.

Если же работник не согласен предоставить информацию о персональных данных, которая не является необходимой согласно федеральному законодательству и образует специальную категорию персональных данных, то работодатель не имеет права отказать в трудоустройстве лишь по этой причине. При решении вопроса о приеме на работу работодатель не вправе руководствоваться лишь автоматизированной обработкой персональных данных.

Работодатель не вправе требовать огласить работника информацию, составляющую тайну его семьи, а также не вправе требовать информацию о политических взглядах. Вся полученная информация о персональных данных потенциальных сотрудников должна быть защищена от утечки и незаконного использования за счет средств работодателя.

Стоит отметить, что согласно статье 85 ТК Российской Федерации, информация, относящаяся к персональным данным нужна работодателю для оформления и поддержания трудовых отношений. Но часто работодатели

требуют у трудоустраивающегося документы, которые не нужны по Федеральному закону.

Так, в обязательном порядке некоторые работодатели незаконно требуют рекомендательные письма и характеристики с предыдущих мест работы, документы о дополнительном образовании, справки о состоянии здоровья с подробным заключением без соответствующих на это оснований, справки об отсутствии судимости на вакансии, где материальная ответственность практически отсутствует.

Ответственность за нарушения правил работы с персональными данными граждан особенно необходима для защиты работников от работодателей. Ведь работодатель является основным звеном, откуда может произойти утечка информации. В отделе кадров организаций в личных карточках работников содержатся сведения о составе семьи, уровне образования, трудовые книжки содержат информацию, где и когда работал гражданин, его стаж, трудовые договоры говорят о величине окладной части заработной платы, об объемах и условиях выплаты премий.

В бухгалтерии организации имеются такие сведения, как доходы гражданина, наличие у него удержаний из зарплат в виде алиментов, отчислений по решению суда, данные о больничных листах работника. Нарушения в использовании персональных данных должны наказываться, ведь информация, попав в руки злоумышленников, способна нанести большой вред жизни гражданина.

Перечень должностей, которые не могут занимать лица, имевшие судимость, закреплен законом. На работу, в которой нет материальной ответственности, могут быть приняты лица, имевшие или имеющие судимость.

Но, как показывает практика, работодатели отказывают в приеме на работу таким лицам, ссылаясь на другие причины. В таких ситуациях сложно привлечь к ответственности работодателя за отказ в приеме на работу.

Большинство организаций имеют службу безопасности, которая имеет доступ к информации о судимости граждан. При этом такой доступ к информации не всегда законный, часто с использованием коррупционных связей. Бывшие сотрудники МВД устраиваются в различные частные фирмы и используют свои связи. Но, как показывает практика, под угрозой отказа в приеме на работу, потенциальные работники все же предоставляют больший объем информации о персональных данных работодателю, чем это необходимо.

Работники предоставляют справки об отсутствии тех или иных заболеваний, об отсутствии беременности при приеме на работу, в которой такие справки не являются необходимостью. Просто работодатель боится себя от рисков принятия на работу сотрудника, который часто будет уходить на больничный, либо уйдет в скором времени в декрет. Такие нарушения законодательства остаются и распространяются, ведь сами работники не заявляют об этом и не требуют соблюдения их прав.

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее - Роскомнадзор) ежегодно выявляет различные нарушения, которые допускает работодатель. Очень часто работодатели не создают приказов и не назначают лиц, которые осуществляют сбор персональных данных и должны быть ответственны за конфиденциальность и безопасность при обработке такой информации. Нет приказов, которые утверждают места хранения материальных носителей персональных данных. Есть организации, в которых отсутствует письменное согласие работника на обработку информации, содержащей его персональные данные. Также часто отсутствуют документы, которые могут подтвердить уничтожение персональных данных работников после достижения цели обработки. В соответствии с Федеральным законом «Об основах охраны

здоровья граждан в Российской Федерации»⁵, информация о факте обращения за медицинской помощью, о состоянии здоровья гражданина, диагнозе его заболевания и иные сведения, полученные при его обследовании и лечении врачами, являются конфиденциальными персональными данными и составляют врачебную тайну.

Никто не вправе разглашать данные сведения, если они стали известны лицу при исполнении им его профессиональных, служебных и иных обязанностей. Передача информации, составляющей врачебную тайну гражданина возможна лишь с его согласия или с согласия его представителя, либо без согласия гражданина, но по запросу органов дознания и следствия, прокурора и суда в связи с проведением расследования или судебным разбирательством.

Стоит заметить, что сайты, которые содержат списки недобросовестных работников с указанием их фамилии, имени и отчества, времени и стажа работы в конкретном месте также не вправе обнародовать такую информацию, ведь она не доказана и является субъективной. Кроме того, указание на сайте личных данных является нарушением конфиденциальности персональных данных гражданина, ведь гражданин не давал согласие на обнародование такой информации. Стоит отметить, что, когда у граждан берут согласие на обработку персональных данных, они ставят подпись в основном, не читая.

В результате граждане подписываются на более широкий перечень использования информации. На официальном сайте Роскомнадзора 2 августа 2021 года было разъяснено совместное информационное письмо от 29 июля 2021 года Банка России и Роскомнадзора «О согласии заемщиков на обработку их персональных данных»⁶. Было указано, что «договор между финансовой организацией и заемщиком является сам по себе основанием для обработки

⁵ Федеральный закон от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» // Официальный интернет-портал правовой информации [Электронный ресурс]. URL:<http://www.pravo.gov.ru/> (дата обращения: 25.04.2023).

⁶ Информационное письмо Банка России № ИН-06-59/57, Роскомнадзора № 08ЛА-48666 от 29 июля 2021 г. «О согласии заемщиков на обработку их персональных данных» [Электронный ресурс]. Документ официально не был опубликован. Доступ из справ. -правовой системы «КонсультантПлюс»

персональных данных. Предлагать заемщику предоставить согласие нужно только в случае, если финансовая организация планирует обрабатывать персональные данные в целях, никак не связанных с исполнением договора, а также, если она планирует поручить обработку персональных данных своего клиента третьим лицам.

Между тем, практически все медицинские, страховые и прочие организации просят подписать разрешения на обработку персональных данных бессрочно. То есть, затем гражданину придется каждому писать письменный отказ на использование персональных данных, чтобы обеспечить прекращение использования информации, прекратить уведомления о различных акциях, не допустить бесконечной рассылки рекламы и др. За несоблюдение защиты персональных данных ответственны не только работодатели, но и работники.

Таким образом, на сегодняшний день соответствующие нормы, регламентирующие ответственность за незаконное использование персональных данных, можно найти в ТК Российской Федерации, КоАП Российской Федерации, УК Российской Федерации. Общие положения отражены в ГК Российской Федерации. Следует улучшать взаимодействие государства и граждан, повысить уровень правовой грамотности населения, а также ответственность граждан при подписании согласия и иных форм предоставления персональных данных. Все это позволит качественно решить имеющиеся проблемы.

Использованные источники:

1. Информационное письмо Банка России № ИН-06-59/57, Роскомнадзора № 08ЛА-48666 от 29 июля 2021 г. «О согласии заемщиков на обработку их персональных данных» [Электронный ресурс]. Документ

официально не был опубликован. Доступ из справ. -правовой системы «КонсультантПлюс»

2. Крюкова Д.Ю., Мокрецов Ю.В. Актуальные проблемы правового регулирования оборота и защиты персональных данных в России // Пенитенциарная наука. 2019. № 2 (38). С. 35.

3. Макаревич М.Л., Бутырская К.Е., Наумова С.И. Проблема правовой защиты персональных данных работника торгового предприятия // Инновационная экономика: перспективы развития и совершенствования. 2019. № 3 (21). С. 64.

4. Прохорова Т.Ю. К вопросу о нормативно-правовом регулировании защиты персональных данных // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2016. № 1 (33). С. 318.

5. Трофимова И.А., Питько Е.В. Особенности гражданско-правовой ответственности за нарушение норм, регулирующих защиту персональных данных работников // Пробелы в российском законодательстве. 2016. № 3. С. 138.

6. Федеральный закон от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» // Официальный интернет-портал правовой информации [Электронный ресурс]. URL:<http://www.pravo.gov.ru/>.