

ПРОБЛЕМЫ В ОБЛАСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКА

PROBLEMS IN THE FIELD
OF EMPLOYEE'S PERSONAL DATA

I. Ospichev

Summary: The article considers the importance of compliance with personal data processing requirements both on the part of the employee and on the part of the employer. The role of personal data processing to ensure information security of the company is analyzed, the place of legal regulation in the mechanism of its formation is identified.

On the example of individual problems, legal gaps in the regulation of issues of personal data processing of employees were considered. For each of them, promising directions for the development of law are determined.

The problem of personal data processing after the introduction of experimental legal regimes in Russia after January 2021 was highlighted.

Keywords: personal data, protection, security, experimental legal regime, risk, employee, employer.

Оспичев Игорь Михайлович

К.ю.н., доцент, ФГБОУ ВО «Югорский государственный университет», г. Ханты-Мансийск
iospichev@yandex.ru

Аннотация: В статье рассматривается значение соблюдения требований к обработке персональных данных, как со стороны работника, так и со стороны работодателя. Анализируется роль обработки персональных данных для обеспечения информационной безопасности компании, выявляется место правового регулирования в механизме ее формирования.

На примере отдельных проблем рассмотрены правовые пробелы регулирования вопросов обработки персональных данных работников. По каждой из них определены перспективные направления развития норм права.

Выделена проблема обработки персональных данных после введения в России экспериментальных правовых режимов после января 2021 года.

Ключевые слова: персональные данные, защита, безопасность, экспериментальный правовой режим, риск, работник, работодатель.

Работодатели собирают персональные данные о работниках по целому ряду причин. Такие сведения необходимы для соблюдения прав и интересов всех участников трудовых отношений, с их помощью реализуется отбор среди потенциальных кандидатов на вакантную должность, обеспечивается обучение и продвижение сотрудников по карьерной лестнице. Соблюдение требований к обработке персональных данных со стороны работодателя обеспечивает для работников их личную безопасность, защищает достоинство работников, их частную жизнь и гарантирует их фундаментальные права, а для работодателей – контроль качества и защиту собственности.

Новые способы сбора и обработки данных влекут за собой некоторые новые риски для работников. В то время как различные национальные законы и международные стандарты имеют установленные обязательные процедуры обработки персональных данных, существует необходимость в разработке положений о защите данных, которые конкретно касаются использования персональных данных работников.

Одним из основных препятствий на пути развития организаций является вопрос обеспечения конфиденциальности и сохранности персональных данных работников. Любая компания, имеющая доступ к данным своих сотрудников, должна гарантировать сохранность и конфиденциальность этой информации.

Информационная безопасность персональных данных анализируется на трех уровнях: организационном, процедурном и техническом. Соответственно, она включает в себя ту цель, которая поставлена организацией и ее политику безопасности для достижения этой цели, разработку и реализацию мер физической защиты и руководящих принципов информационной безопасности персонала, реализацию проверенных и сертифицированных решений, в том числе резервное копирование, парольная и антивирусная защита, брандмауэры, шифрование данных и так далее.

В состав организационного уровня защиты персональных данных включено правовое регулирование их обработки и защиты.

Так, персональные данные граждан относятся к особо охраняемой правовой категории. Ряд ученых рассматривают проблему персональных данных через призму информационного права. Далее рассмотрим некоторые проблемы персональных данных работника с учетом указанного критерия.

Ни Трудовым кодексом Российской Федерации [1], ни законодательством о персональных данных [2] не предусмотрена обязанность работника своевременно извещать своего работодателя о каких-либо изменениях в своих персональных данных.

Вместе с тем, очевидно, что в случае отсутствия у ра-

ботодателя актуальной информации о работнике в части некоторых персональных данных, может привести к неисполнению или неполному исполнению работодателем определенных обязательств перед работником, например, по выплате заработной платы.

Соответственно, целесообразно закрепить в трудовом законодательстве, а в последующем привести в локальные правовые акты организаций, в том числе в положения о персональных данных, личные карточки и трудовые книжки, требование в части сроков и обязанностей работников сообщать работодателю обо всех изменениях в своих персональных данных. Это позволит предупредить наступление ситуации, при которой права работника будут нарушены.

Еще одним вариантом решения указанной проблемы является возможность установить требование в части обязательств работника сообщать об изменениях его персональных данных в трудовом договоре. Важно отметить, что установление такого рода требований в соглашениях между работниками и работодателями не противоречит законодательству и положение работника не ухудшает.

Еще одной проблемой в области защиты персональных данных работника является ее неправомерная передача третьим лицам. В данной ситуации следует учитывать, что такого рода передача может осуществляться исключительно при наличии предварительного письменного согласия владельца персональных данных (работника).

По данному требованию законодательства судебная практика имеет однозначную позицию: суды поддерживают участника судебного разбирательства, который либо обеспечивает защиту своих прав ввиду неправомерной передачи его персональных данных третьей стороны без согласия на такую передачу или встает на сторону участника разбирательства (работодателя), который не передал персональные данные работника без его согласия.

К примеру, суд поддержал работодателя, который несмотря на запрос собрания акционеров общества, не предоставил копию трудового договора с директором этого общества ввиду наличия в трудовом договоре персональных данных руководителя [7].

Вместе с тем, раскрытие персональных данных заявителю в некоторых случаях допускается без согласия его владельца, например, в целях защиты общественных интересов. Судебная практика признает законными такого рода передачи персональных данных, например, в рамках запросов ФКУ ГИАЦ МВД России и ИЦ обо всех

судимостях заявителя, включая погашенные [6].

Законной является передача персональных данных работника профессиональным союзом необходимым для осуществления возложенных на него в силу закона функций запрашивать у работодателя информацию по вопросам исполнения коллективного договора [5].

Потребители банковских услуг подтверждают наличие проблемы незаконного распространения персональных данных сотрудниками кредитных организаций. К примеру, в ситуации, когда сотрудники банков оставляют письма (обращения) без конвертов в дверях граждан или при передаче соседям, а также когда банковская информация клиента, находящаяся исключительно в кредитной организации, попадает в открытый доступ в сеть Интернет. В такой ситуации помимо нарушения требований законодательства о персональных данных, кредитная организация нарушает и законодательство о банковской тайне, согласно которому кредитной организацией гарантируется тайна о счетах и вкладах, а также об операциях корреспондентов и клиентов [3].

Для устранения такого рода нарушений в части обработки персональных данных необходимо обращаться в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) с требованием о прекращении незаконного использования персональных данных. Кроме того, важно обеспечить установление повышенной ответственности кредитных организаций за незаконную обработку персональных данных клиентов [8].

Проблема сохранности персональных данных (паспорт, СНИЛС, ИНН, номера телефонов и т.д.) является причиной роста числа мошенничества в сфере микрокредитования. Одним из самых распространенных способов такого рода незаконных действий является оформление микрозайма на гражданина, персональных данные которого получены преступником незаконным путем. В такой ситуации финансовые ресурсы (займ) практически мгновенно переходит на банковские счета подставных лиц.

Для устранения этой проблемы необходимо на законодательном уровне установить необходимость проведения микрофинансовыми организациями всех переводов денежных средств с применением единой системы идентификации и аутентификации и единой биометрической системы.

Стремительное развитие компьютерных технологий, а также расширение и рост обработки персональных данных с помощью компьютерных систем привели к возникновению проблем, связанных с информационно-тех-

нической безопасностью и защитой. Обеспечение безопасности персональных данных сотрудников и защита их от нежелательного доступа должны основываться на новых инновационных подходах.

Обеспечение конфиденциальности и неприкосновенности частной жизни сотрудников требует усиления организационных, технологических и правовых мер в соответствии с принятыми стандартами информационной безопасности, а также с учетом специфики каждой организации.

Особую актуальность получили вопросы защиты персональных данных в последнее время – в период пандемии коронавируса. К примеру, остро стоит вопрос защиты специальной категории персональных данных – данных о температуре тела работников, получаемой в результате применения тепловизоров.

Многие работники негативно воспринимают данную меру борьбы с распространением вируса COVID-19, тогда как Роскомнадзор однозначно определил, что термометрия является прямой мерой по выявлению заболевания и связана с определением возможности выполнения

трудовых функций, соответственно, согласия работника на измерение температуры не требуется [9].

В дополнение к вышеуказанному следует отметить, что в рамках экспериментальных правовых режимов, применяемых с 28 января 2021 года [4], предложено не применять отдельные требования законодательства о персональных данных. Такая инициатива в случае обработки больших массивов персональных данных, например, в медицинских целях при использовании технологий искусственного интеллекта, предполагающих анализ информации о тысячах пациентов, или обработке персональных данных работников транснациональных корпораций ставит под угрозу права владельцев персональных данных в случае их незаконного использования.

Рассмотренные выше проблемы в области персональных данных работников показывают несовершенство правового регулирования данного объекта правовой защиты. Только анализ проблем правоприменения позволит качественно поменять и обеспечить развитие правовых средств охраны такого рода сведений от их незаконного использования.

ЛИТЕРАТУРА

1. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ (ред. от 31.07.2020) / Собрание законодательства РФ, 20.07.2020, № 29, ст. 4520.
2. О персональных данных: федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 24.04.2020) / Российская газета, № 92, 28.04.2020.
3. О банках и банковской деятельности: Федеральный закон от 02.12.1990 № 395-1 (ред. от 27.12.2019) / Собрание законодательства РФ, 23.12.2019, № 51 (часть I), ст. 7486.
4. Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации: Федеральный закон от 31 июля 2020 г. № 258-ФЗ (документ не вступил в силу) / Российская газета от 6 августа 2020 г. № 173.
5. Определение Верховного Суда РФ от 20.07.2012 № 56-КГ12-3 / [Электронный ресурс] Режим доступа: <https://lawpravo.ru/pract/Opredelenie-VS-RF-N-56-KG12-3-ot-20-iyulya-2012-g/>.
6. Решение Заводского районного суда г. Грозного Чеченской Республики от 4 июля 2017 г. по делу № 2А-271/2017 / [Электронный ресурс] Режим доступа: <https://sudact.ru/regular/doc/G4toJoErouQ5/>.
7. Постановление ФАС Московского округа от 14.01.2010 № КА-А40/14463-09 по делу № А40-38438/09-17-269 / [Электронный ресурс] Режим доступа: <https://www.garant.ru/products/ipo/prime/doc/5732081/>.
8. Письмо ЦБ РФ от 29 сентября 2014 г. № 41-2-2-8/1757 / [Электронный ресурс] Режим доступа: <https://base.garant.ru/71073540/>.
9. Роскомнадзор разъясняет особенности использования тепловизоров работодателями / [Электронный ресурс] Режим доступа: <https://rkn.gov.ru/news/rsoc/news72206.htm>.

© Осипчев Игорь Михайлович (iospichev@yandex.ru).

Журнал «Современная наука: актуальные проблемы теории и практики»