DOI: http://dx.doi.org/10.21686/2411-118X-2025-1-141-146

Передача персональных данных третьим лицам работниками компаний: проблемы правового регулирования и перспективы развития законодательства

М. А. Ширяева
аспирант Пятигорского государственного университета.
Адрес: ФГБОУ ВО «Пятигорский государственный университет»,
357532, г. Пятигорск, Калинина пр., д. 9.
E-mail: mash.sumerova@yandex.ru

Transfer of Personal Data to Third Parties by Company Employees: Problems of Legal Regulation and Prospects for the Development of Legislation

M. A. Shiryaeva
Postgraduate Student of Pyatigorsk State University.
Address: Federal State Budgetary Educational Institution of Higher Education
“Pyatigorsk State University”,
1A Pushkin Str., Pyatigorsk, 357532, Russian Federation.
E-mail: mash.sumerova@yandex.ru

Поступила 19.01.2025 Принята к печати 30.01.2025

Аннотация

В статье рассмотрены ключевые аспекты передачи персональных данных третьим лицам работниками компаний в условиях цифровизации и расширения применения электронного документооборота. В статье поднимаются проблемы правого регулирования работы с персональными данными третьих лиц работниками компании, фиксирования факта нарушений при неправомерной передаче персональных данных третьих лиц работниками компании, введения санкций работодателем в отношении работников за нарушение передачи персональных данных третьих лиц, будет проведет анализ действующего законодательства о персональных данных Российской Федерации и предложены варианты его развития. Автором статьи приводится актуальная статистика судебных дел, возникающих на основании поднятой в данной статье проблемы утечек персональных данных, были сделаны соответствующие выводы и предложены пути устранения нарушений прав субъектов персональных данных и усовершенствования законодательства. В статье рассматриваются решения судебных органов по вопросу незаконной передачи и обработки персональных данных субъектов, а также, приведены примеры правовых коллизий в отношении данного вопроса. Автор также приходит к выводу о сложности и многогранности проблем, поднятых в данной статье, и указывает на то, что со стороны законодателя требуется более внимательное правовое регулирование в части обработки и передачи персональных данных.

Ключевые слова: информация, обработка, утечки, автоматизация, оптимизация, база данных, человеческий фактор, злоумышленники.

Abstract

The article considers the key aspects of the transfer of personal data to third parties by company employees in the context of digitalization and the expansion of the use of electronic document management. The article raises the problems of legal regulation of work with personal data of third parties by company employees, recording the fact of violations in the unlawful transfer of personal data of third parties by company employees, the introduction of sanctions by the employer against employees for violating the transfer of personal data of third parties, will analyze the current legislation on personal data of the Russian Federation and propose options for its development. The author of the article provides current statistics of court cases arising on the basis of the problem of personal data leaks raised in this article, appropriate conclusions were made and ways to eliminate violations of the rights of personal data subjects and improve legislation were proposed. The article considers the decisions of judicial bodies on the issue of illegal transfer and processing of personal data of subjects, and also provides examples of legal conflicts in relation to this issue. The author also comes to the conclusion about the complexity and multifaceted nature of the problems raised in this article, and points out that more careful legal regulation in terms of processing and transfer of personal data is required from the legislator.

Keywords: information, processing, leaks, automation, optimization, database, human factor, intruders.

Введение в проблематику правового регулирования персональных данных. В современном мире передача персональных данных третьим лицам становится все более актуальной темой. С развитием технологий и увеличением объемов обрабатываемых данных компании сталкиваются с необходимостью делиться информацией как внутри, так и вне организации. Однако это порождает множество правовых и этических вопросов, касающихся защиты личной информации. Недобросовестные сотрудники государственных органов, банковского сектора продают персональные данные своих клиентов третьим лицам; хакерские атаки приводят к регулярным утечкам информации из баз данных – в результате в социальных сетях формируются сообщества, где за небольшие деньги можно просмотреть любую информацию о субъекте, начиная с наименования банка, в котором у субъекта открыт счет, заканчивая адресами для доставки продуктов[1]. С правовой точки зрения такое отношение к персональным данным третьих лиц является недопустимым. Возникают следующие вопросы:

1. Как остановить распространение своих персональных данных?
2. Что делать с данными, которые уже стали публичными?
3. Как обезопасить себя в будущем?
4. Как реагирует российский законодатель на все более масштабные утечки в самых передовых компаниях Российской Федерации?

Причины возникновения утечек персональных данных. «Кто владеет информацией – тот владеет миром»: эти слова принадлежат британскому банкиру Натану Ротшильду. Уже в XIX веке люди понимали, что информация – ресурс, который можно продать, купить, обменять, которым можно шантажировать и угрожать [3. – С. 177]. В наше же время четыре цифры от банковского приложения могут привести к разорению всей семьи, а никнейм в электронной почте может подсказать нам год рождения пользователя.

В современном мире каждый день происходит обработка и передача персональных данных – при трудоустройстве на работу, при входе в электронную почту, даже при предъявлении пропуска на контрольно-пропускном пункте. В своем стремлении упростить выполнение ежедневных задач и улучшить результаты своей деятельности человек перестал замечать, какое большое количество информации он регулярно обрабатывает и передает третьим лицам[2].

В похищении и злоупотреблении персональными данными заинтересованы мошенники. Торговля и спекуляция информацией, полученной незаконным путем, являются их основным заработком [2. – С. 67]. За такие правонарушения предусмотрена уголовная ответственность.

Персональные данные не всегда попадают в руки к злоумышленникам путем их целенаправленного похищения. Самая частая причина утечки персональных данных – человеческий фактор: незаблокированный компьютер, ошибочно отправленное письмо, использование для рабочих процессов сервисов, чьи бэк-офисы (бэк-офис – операционно-учетное подразделение, в задачи которого входит документарное и электронное оформление сделок между подразделениями организации) находятся за пределами Российской Федерации. Компании хранят персональные данные уволенных сотрудников, которые, соответственно, уже являются третьими лицами по отношению к компании, в виде копий паспортных данных, ИНН, СНИЛС, без определения цели хранения копий таких документов. Если какие-либо цели отсутствуют или хранение является избыточным с точки зрения достижения целей, хранение копий таких документов противоречит требованиям Закона о персональных данных № 152-ФЗ. Хранение таких документов неправомерно даже при наличии согласия на обработку персональных данных.

Для того, чтобы обезопасить своих сотрудников, клиентов и репутацию от негативных последствий утечек персональных данных, российские компании предпринимают соответствующие меры:

1) обеспечивают безопасность при работе с облачными сервисами для работы с информацией. Облачные технологии – это инструмент, который позволяет хранить данные пользователей на серверах, находящихся в удаленном data-центре. Их используют небольшие организации или круп-

[1] URL: https://rt-solar.ru/products/solar_dozor/blog/4275/

[2] URL: https://www.rbc.ru/finances/10/10/2019/5d9e05ce9a79474c70839c73

ные предприятия для хранения корпоративной информации, а также частные лица для хранения личных данных и файлов. Все облачные сервисы работают через сеть Интернет, а значит, существует риск несанкционированного доступа к данным клиентов. Владельцам таких сервисов важно доверие пользователей, поэтому их главная задача – обеспечить безопасность данных, которые находятся на серверах. Проблема заключается в том, что клиент не может самостоятельно узнать, где находятся сервера или data-центр. Владелец облачного хранилища может иметь как собственные сервера для хранения данных, так и арендовать их. Поэтому пользователи должны учитывать риски, связанные с передачей данных владельцам облачных хранилищ на удаленные серверы;

2) используют механизмы шифрования данных;

3) контролируют трафик, доступ к информации и ее использование;

4) учитывают необходимые параметры идентификации пользователей (логины, пароли, коды подтверждения);

5) используют средства защиты от вирусов других вредоносных программ, которые могут угрожать безопасности данных клиентов;

6) обеспечивают резервное копирование на другие сервера в случае отказа основного сервера;

7) соблюдают правовые требования законодательства Российской Федерации;

8) регулярно обновляют пароли;

9) ограничивают доступ сотрудников к конфиденциальной информации в облаке.

Проблемы и перспективы развития правового регулирования обработки и передачи персональных данных. Одной из основных проблем правового регулирования обработки и передачи персональных данных является отсутствие четких и однозначных норм, регулирующих передачу персональных данных. В разных юрисдикциях могут существовать различные требования к передаче данных, что создает правовую неопределенность для компаний. Компании стремятся защитить доступ к персональным данным клиентов, создавая многоуровневые системы защиты, ограничивая возможности ознакомления и копирования данной информации, обеспечивая безопасность хранения и конфиденциальности информации. При этом, как показывает статистика, ежегодно количество утечек персональных данных многократно увеличивается. В 2024 г. в России выросло количество судебных дел, связанных с передачей персональных данных. По данным издания «Коммерсантъ», количество споров о незаконном использовании персональных данных выросло на 17% относительно начала 2023 г.[1] Чаще всего административные и уголовные дела касались незаконного получения данных о конкретном человеке. По мнению экспертов, на статистику повлиял общий рост утечек данных россиян, а также массовый сбор согласий клиентов компаний на обработку их данных. Количество судебных дел в первом квартале 2024 г. выросло до 4,4 тысяч. Положительный опыт практики взыскания возмещения морального вреда с оператора данных, допустившего их неправомерную передачу, подталкивает граждан чаще обращаться в суд. Сумма компенсаций на данный момент составляет 5 тысяч рублей.

В связи с возросшим количеством судебных дел бизнес несет репутационные риски и чаще сталкивается с претензиями граждан о надежности хранения их информации. И если сумма компенсации гражданам может показаться бизнесу небольшой, то штрафы после проверок Роскомнадзора по заявлениям об утечке персональных данных исчисляются уже сотнями тысяч рублей.

Также возникает вопрос о правомерности передачи персональных данных по адвокатскому запросу. Вопрос неоднозначный, и суды принимают различные решения. Это зависит от того, кому принадлежат персональные данные и есть ли согласие владельца на их раскрытие. Например, когда клиент поручает адвокату задачу, то предполагает, что он будет использовать полученные для ее решения данные. При этом передавать данные третьим лицам без разрешения клиента адвокат не может. Адвокатская тайна защищает интересы клиента. В этом случае суд признает отказ в предоставлении информации по адвокатскому запросу незаконным, потому что у адвоката есть согласие на получение информации о персональных данных клиента (Кассационное определение Судебной коллегии по административным делам Верховного суда Российской Федерации от 11.08.2021 № 67-КАД21-3-К8). Кроме того, суды считают, что адвокат не имеет права запрашивать информацию о персональных данных других лиц, если это не предусмотрено федеральным законодательством. Адвокат мо-

[1] URL: https://www.kommersant.ru/doc/6665239

жет собирать информацию, необходимую для юридической помощи, но конфиденциальные данные (например, служебная тайна или данные сотрудников правоохранительных органов) к ней не относятся (Кассационное определение Девятого кассационного суда общей юрисдикции от 14.12.2022 № 88а-10995/2022 по делу №2а-350/2022; Кассационное определение Шестого кассационного суда общей юрисдикции от 12.11.2019 № 88а-260/2019). Если нужно получить такую информацию, адвокат может обратиться в суд с просьбой истребовать доказательства, включая конфиденциальные данные. Однако есть другие ситуации [4. – С. 183]. Например, суд признал законным отказ адвокату в предоставлении копии договора на обучение, который содержал персональные данные обучающегося.

В отношении правового статуса никнейма тоже нет законодательной определенности. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» не дает однозначного ответа на вопрос о том, можно ли отнести никнейм к персональным данным. У государственных органов и судов также нет официальной позиции по такой проблеме. По смыслу пункта статьи 3 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» никнейм можно отнести к персональным данным, если он позволяет установить сведения о владельце. Например, никнейм в соцсети, который позволит найти аккаунт с изображением человека, его имени и другими сведениями, относится к персональным данным, а никнейм urist15 на форуме без указания инициалов, телефона и фото нельзя назвать персональными данными. В то же время Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи» относит псевдоним гражданина к сведениям ограниченного доступа. Согласно статье 53 указанного закона Оператор[1] имеет право распространять такие данные только с согласия абонентов. Во избежание конфликтов с владельцами персональных данных рекомендуется получить согласие на обработку данных пользователя сайта (он же – владелец никнейма), даже если он не указал никакую другую информацию о себе.

Согласие на обработку персональных данных может быть представлено:

1) в письменном виде;

2) в электронной форме;

3) путем конклюдентных (поведенческих) действий;

4) в устной форме (например, при телефонном разговоре).

В письменном виде согласие на обработку персональных данных требуется при:

– включении персональных данных в общедоступные источники (ст. 8 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»);

– обработке специальных категорий персональных данных (п. 1 ч. 2 ст. 10 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»);

– обработке биометрических персональных данных (ч. 1 ст. 11 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»);

– передаче персональных данных работников третьим лицам (ст. 88 Трудового кодекса Российской Федерации от 30 декабря 2001 г. № 197-ФЗ);

– распространении персональных данных неограниченному кругу лиц (ст. 10.1 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»);

– принятии решения, которое приведет к юридическим последствиям в отношении субъекта персональных данных или иным образом затронет его права и законные интересы, на основании исключительно автоматизированной обработки персональных данных (ч. 2 ст. 16 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»).

Согласие в форме электронного документа, которое подписано электронной подписью в соответствии с федеральным законом, признается равнозначным согласию в письменной форме на бумажном носителе, содержащему собственноручную подпись субъекта персональных данных.

При конклюдентной форме предоставления персональных данных субъект может передать материальные носители с персональными данными (например, при подаче заявления или резюме). Также конклюдентной формой предостав-

[1] Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных (в соответствии с п. 2 ст. 3 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»).

ления данных можно считать продолжение телефонного разговора.

Устная форма предоставления персональных данных предполагает выражение согласия Субъекта на обработку персональных данных напрямую или по телефону. Однако Оператору в любом случае необходимо обеспечить возможность подтвердить факт получения такого согласия, поскольку на него возлагается обязанность доказывать факт обработки персональных данных с согласия субъекта (ч. 3 ст. 9 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»).

Перспективы развития законодательства. Развитие IT-технологий и массовое использование искусственного интеллекта подтолкнуло Правительство к разработке единого нормативного правового акта в этой сфере. Члены Совета Федерации готовят документ – Цифровой кодекс, который станет основой правового регулирования взаимоотношений в области информации и цифровых технологий. В кодексе будут в первую очередь определены понятийные основы: термины, принципы, субъекты и объекты права, на которые он будет распространяться, а также конкретные виды государственных и социальных институтов, виды правоотношений и способы их взаимодействия. Единый нормативный документ будет регулировать вопросы информации и связи, включая ее традиционные виды (например, Почта России). Значительную часть документа планируют посвятить защите персональных и биометрических данных. Важно отметить, что персональные данные – это основа для создания больших баз данных, обучения и использования искусственного интеллекта, а также развития цифровых технологий, но персональная безопасность – в приоритете. По словам члена Совета Федерации Ирины Рукавишниковой, главная задача Цифрового кодекса – это определить правила, которые защищали бы каждого гражданина от несанкционированного использования его персональных данных и от любого воздействия технологий, связанных с искусственным интеллектом.

Для того, чтобы единый нормативный документ получился полноценным, в Цифровом кодексе должны быть учтены интересы всех субъектов права: граждан, государственных органов, коммерческих структур, разработчиков цифровых технологий. Важно, чтобы помимо норм, направленных на защиту прав субъектов, действовали понятные правила и требования в отношении операторов персональных данных.

В целях обеспечения благоприятных правовых условий для передачи данных с использованием новых технологий в части установления порядка обезличивания персональных данных, порядка получения согласия на передачу персональных данных, а также регулирования оборота больших объемов данных с учетом необходимости защиты прав и свобод третьих лиц предлагается введение обязательного корпоративного регулирования работы с персональными данными на законодательном уровне. Предполагается обязать юридические лица учреждать профильные подразделения по работе с персональными данными в составе департаментов информационной безопасности с привлечением юридической службы, а также утверждать локальные нормативные акты с указанием процедур по выявлению незаконной передачи персональных данных третьих лиц работниками компаний, фиксированию таких передач и введению дальнейших санкций в отношении работников компании, которые допустили незаконную передачу персональных данных [1. – С. 52].

Так, в Государственную Думу был внесен законопроект (Законопроект «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» (в части усиления ответственности за нарушение порядка обработки персональных данных) от 4 декабря 2023 г. № 502104-8) об увеличении административной ответственности компаний, допустивших утечки персональных данных. Авторы инициативы предлагают внести поправки в Кодекс Российской Федерации об административных правонарушениях. Ключевые положения такого законопроекта касаются увеличения суммы штрафов за незаконную передачу персональных данных третьих лиц, а также введения новых оснований для административной ответственности:

– уведомление Роскомнадзора о начале обработки персональных данных;

– неуведомление об утечках персональных данных;

– неправомерная передача, распространение, предоставление доступа к персональным данным;

– неправомерное распространение биометрических персональных данных.

Также в Государственную Думу был внесен законопроект (Законопроект «О внесении изме-

нений в статью 9 Федерального закона “О персональных данных” и статью 10 Закона Российской Федерации “О защите прав потребителей”» от 27 февраля 2024 г. № 679980-8) об отдельном оформлении согласия на обработку персональных данных. Авторы инициативы призывают отказаться от формального включения согласия на обработку персональных данных в состав договоров и других документов и предлагают следующую формулировку в статью 9 Закона №152-ФЗ «О персональных данных»: «Согласие на обработку персональных данных должно быть оформлено отдельно от иных информации и (или) документов, которые подтверждает и (или) подписывает субъект персональных данных». Внесение такого законопроекта логично, понятно и совпадает с мнением уполномоченного органа. Роскомнадзор неоднократно давал разъяснения о том, что согласие субъекта на обработку персональных данных должно быть отдельным документом. Его нельзя, например, включить в текст договора, это неправомерно [5. – С. 73]. Такой ситуацией часто пользуются недобросовестные компании. Они включают текст согласия на обработку персональных данных в пользовательские соглашения, договоры и другие юридические документы, где среди большого объема информации также могут быть добавлены условия о передаче данных неопределенному кругу лиц, что не позволяет соблюдать требования части 1 статьи 9 Закона № 152-ФЗ «О персональных данных» к согласию на обработку персональных данных. Принятие поправки поможет избежать неопределенности и введения субъектов в заблуждение при предоставлении согласия на обработку персональных данных. У субъекта всегда должен быть выбор – давать или не давать свое согласие.

Заключение. Передача персональных данных третьим лицам является сложной и многогранной проблемой, требующей внимательного правового регулирования. С учетом текущих тенденций и вызовов можно ожидать дальнейшего развития законодательства в этой области, направленного на защиту прав субъектов данных и повышение ответственности компаний.

Список литературы

1. *Гордеева Е. Н., Киселёва Т. С.* Беспроигрышная последовательность действий для обработки персональных данных // Инженерно-технологические решения проблем развития АПК и общества : сборник трудов LVVII международной научно-практической конференции студентов, аспирантов и молодых ученых. – Тюмень, 2024. – С. 49–54.

2. *Грибачев К. К., Седаков К. А., Ермаков Д. О.* Международный опыт регулирования обработки персональных данных и его применимость в Российской Федерации // Информационная безопасность и защита персональных данных. Проблемы и пути их решения : сборник материалов и докладов XVI межрегиональной научно-практической конференции. – Брянск, 2024. – С. 66–69.

3. *Мамыкина Е. В*. Правовой статус субъектов, участвующих в персональных данных: субъект персональных данных; оператор персональных данных // Моя профессиональная карьера. – 2020. – № 11. – С. 117–122.

4. *Полякова Т. А., Бойченко И. С.* Цифровой оборот данных – проблемы взаимодействия субъектов и оператора обработки персональных данных // Право и государство: теория и практика. – 2021. – № 11 (203). – С. 181–184.

5. *Семенов Е. Ю., Лысенко Е. С., Графуткин Е. И.* Регулирование обработки персональных данных в России: юридические и технические аспекты // Научный вестник Орловского юридического института МВД России имени В. В. Лукьянова. – 2023. – №3 (96). – С. 69–77.