Обеспечение права работодателя на защиту информации: проблемы правового регулирования

Н. В. Пугачёва

Российский государственный университет правосудия,
Российская Федерация, 197046, Санкт-Петербург, Александровский парк, 5

Для цитирования: Пугачёва, Наталья В. 2024. «Обеспечение права работодателя на защиту информации: проблемы правового регулирования.» *Ежегодник трудового права* 14: 219–230. https://doi.org/10.21638/spbu32.2024.113

В условиях бурного развития информационно-коммуникационных технологий и провозглашения конституционного права каждого на свободный поиск, получение и распространение информации все сложнее обеспечить ограничение доступа к информации различного рода. Между тем находящаяся в распоряжении работодателя конфиденциальная информация, доступ к которой он ограничивает либо в своих интересах (коммерческая тайна), либо в публичных интересах или в интересах третьих лиц (сведения, имеющие режим тайны, персональные данные физических лиц), нуждается в защите. Предметом исследования выступают положения законодательства, в том числе трудового, позволяющие работодателю как обладателю конфиденциальной информации выстроить систему ограниченного доступа к ней и принимать меры к работникам, нарушившим установленные правила защиты информации. Анализ соответствующих норм приводит к выводу о том, что в бурно развивающемся информационном обществе, предоставляющем широкие возможности для мгновенной передачи (распространения) значительного объема информации, действующее правовое регулирование не в полной мере отвечает требованиям обеспечения баланса прав и законных интересов работника и работодателя, поскольку оно позволяет работодателю прекратить доступ работника к охраняемой информации только путем его увольнения по дисциплинарному основанию, что вынуждает работодателя принимать такие решения и в тех случаях, когда для этого отсутствуют закрепленные законодательством основания (разглашение), нарушая тем самым права работника. В связи с этим предлагается введение правового механизма лишения работника доступа к конфиденциальной информации при совершении им действий, создающих угрозу ее распространения, что, с одной стороны, исключит его работу с такой информацией, а с другой стороны, позволит ему (при определенных условиях) продолжить работу у данного работодателя. Такой механизм, будучи нацеленным на оптимальное согласование интересов работодателей и работников, обеспечит право работодателя на защиту информации и в то же время не допустит чрезмерного ограничения прав работника.

Ключевые слова: конфиденциальная информация, коммерческая тайна, информационно-коммуникационные технологии, персональные данные, разглашение тайны, дисциплинарная ответственность.

1. Введение

В течение последних десятилетий одним из основных процессов в обществе является повышение значимости информационных потоков, а также развитие соответствующих технологий и инструментов, предназначенных для получения, обработки, использования и передачи информации, чему, естественно, способствовал технический прогресс — бурное развитие информационно-коммуникационных технологий (далее — ИКТ), которые прочно вошли во все сферы общественной жизни. Сфера применения труда не является исключением. В условиях цифровизации появились и прогнозируются новые формы занятости, привлекающие внимание специалистов в области трудового права: дистанционный труд (Чесалина 2021), разные виды платформенной занятости (Лушников и Лушникова 2020; Гребенщиков, Дивеева и Кузьменко 2020), работа в метавселенных (Филипова 2023), которые построены на передаче информации посредством общедоступных средств связи; повышаются технические возможности работодателей наблюдать за работниками и тем самым собирать о них информацию (Офман 2021).

В связи с интенсификацией процессов оборота информации в условиях цифровизации экономики, легкости ее добывания и передачи обостряется вопрос о необходимости защиты информации, представляющей ценность для ее обладателя либо охраняемой в публичных интересах или интересах третьих лиц (различного рода тайны, персональные данные физических лиц). Он, конечно, возник не сегодня, но возможность компьютерной обработки информации, ее получения и передачи посредством современных средств связи, увеличение скорости ее передачи, создание возможности обмена большими объемами информации, расширение диапазона способов ее распространения вызывает к жизни новые риски. Как отмечают исследователи проблем, связанных с использованием ИКТ в предпринимательской деятельности, «информация всегда была необходима для эффективного управления, но революция, произошедшая в коммуникационных системах, увеличила объем доступной информации и сделала процесс управления информацией более сложным и важным для фирмы» (Информационные технологии в бизнесе 2002, 16).

Таким образом, применение труда все больше и больше связано с автоматизацией, компьютеризацией, использованием инновационных достижений, повышением значимости информации в экономической деятельности и появлением в этой сфере конфиденциальной информации, под которой Э. Н. Бондаренко и Д. В. Иванов понимают легально полученную информацию, которая в силу действующего правового регулирования доступна строго определенному кругу лиц и в отношении которой установлен соответствующий режим секретности (Бондаренко и Иванов 2012, 11). Такая ситуация обусловливает актуальность вопроса об обеспечении эффективной защиты конфиденциальности информации в условиях цифрового общества, в том числе и трудоправовыми средствами, и даже позволяет ученым, занимающимся проблемами трудового права, высказывать предложение об обособлении в рамках общей части трудового права отдельного института «информационное трудовое право» (Лушников и Лушникова 2015, 127).

Соответственно, мы можем говорить о необходимости в рамках трудовых отношений обеспечения информационной безопасности, понимаемой в целом как

«состояние и условия жизнедеятельности личности, при которых реализуются ее информационные права и свободы» (Ковалева 2012, 268). При этом информационную безопасность работодателя, на наш взгляд, можно определить как состояние его защищенности от несанкционированных умышленных или неосторожных действий (доступ, уничтожение, искажение, модифицирование, блокирование, копирование, распространение и др.) работников и третьих лиц в отношении информации, обладателем которой является работодатель и в отношении которой установлен соответствующий режим защиты.

2. Основное исследование

В трудоправовой сфере остро стоит вопрос о защите конфиденциальной информации различных видов: защите подлежит информация, имеющая режим тайны (государственной, служебной[1], коммерческой, профессиональной), а также персональные данные работников (бывших работников, кандидатов на трудоустройство).

Вопросы защиты государственной тайны урегулированы Законом РФ «О государственной тайне»[2]; вопросы защиты профессиональной тайны — рядом федеральных законов (например, ст. 26 ФЗ «О банках и банковской деятельности»[3] посвящена защите банковской тайны, ст. 13 ФЗ «Об основах охраны здоровья граждан в Российской Федерации»[4] обязывает лиц, получивших доступ к врачебной тайне, в том числе в связи с исполнением трудовых, должностных обязанностей, хранить ее); защита персональных данных работника обеспечивается как гл. 14 Трудового кодекса РФ (далее — ТК РФ), так и ФЗ «О персональных данных»[5], который также нацелен на защиту персональных данных иных физических лиц. Таким образом, на работодателе лежит обязанность обеспечить конфиденциальность всех указанных видов информации в публичных интересах либо в интересах третьих лиц.

Вместе с тем работодатель является обладателем информации, непосредственно связанной с его экономической (предпринимательской) деятельностью и представляющей для него ценность как для субъекта экономики, сохранность которой он обеспечивает в собственных интересах, реализуя при этом не обязанность, возложенную на него федеральными законами, а права, законодательством предоставленные. Речь, конечно, идет об информации, составляющей коммерческую тайну, которая сегодня стала «новым капиталом» и представляет собой сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной

---

[1] Следует отметить, что в законодательстве отсутствует определение служебной тайны, вопрос является предметом научной дискуссии, однако его рассмотрение выходит за рамки темы настоящей статьи.

[2] Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне». — Здесь и далее все ссылки на российские и международные нормативные правовые акты и судебную практику приводятся по СПС «КонсультантПлюс». URL: http://www.consultant.ru (дата обращения: 19.10.2023).

[3] Федеральный закон от 02.12.1990 № 395-I «О банках и банковской деятельности».

[4] Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации».

[5] Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен соответствующий режим (п. 2 ст. 3 ФЗ «О коммерческой тайне»[6]).

2.1. Обеспечение работодателем защиты информации ограниченного доступа

Вся информация, обладателем которой является работодатель, находится в руках работников, трудовые функции которых связаны с ее хранением, обработкой, использованием и пр. И во многом работники, допущенные к работе с информацией, и являются (умышленно или неосторожно) субъектами нарушения режима конфиденциальности. О важности обеспечения защиты конфиденциальной информации работодателя от действий работников говорит следующая статистика. По аналитическим данным компании InfoWatch, занимающейся ежегодным анализом утечек конфиденциальной информации, в 2021 г. 75 % утечек информации из организаций, работающих в России, произошло в результате действий внутренних нарушителей, при этом доля таких умышленных утечек в 2020–2021 гг. по сравнению с предыдущими годами возросла почти до 80 %. Основной массив несанкционированно распространяемой информации образуют персональные данные (в 2021 г. — 89,8 %), однако и доля информации, составляющей тайну, значительна — 9,8 % (из которых 5,1 — коммерческая тайна, 4,7 — государственная)[7]. В 2022 г. произошел резкий скачок количества утечек (более чем в 2,1 раза) и почти вдвое выросло количество утечек информации, составляющей коммерческую тайну (до 9,1 %)[8].

Соответственно, работодатель в целях обеспечения своей информационной безопасности должен принять меры для установления контроля за сохранностью информации и ее обращением. Кроме мер организационного (установление режимных, временных, пространственных ограничений на доступ к информации) и технического (применение технических и программных мер защиты информации) характера необходимы и правовые меры, направленные на урегулирование отношений субъектов трудового договора по защите конфиденциальной информации. В противном случае у работников, допущенных к такой информации, не возникнет обязанность воздерживаться от совершения действий, ведущих к ее уничтожению, повреждению либо нарушению режима конфиденциальности, а работодатель будет лишен возможности привлечь работника к ответственности.

Обязанность за свой счет осуществлять защиту персональных данных работников от неправомерного их использования или утраты возложена на работодателя п. 6 ст. 86 ТК РФ и ФЗ «О персональных данных». Для введения режима коммерческой тайны работодателю необходимо определить информацию, составляющую объект защиты; урегулировать порядок доступа и обращения с ней; определить

---

[6] Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне».

[7] Россия. Утечки информации ограниченного доступа в 2021 году // Экспертно-аналитический центр InfoWatch. 2022. URL: https://www.infowatch.ru/analytics/analitika (дата обращения: 28.04.2023).

[8] Там же.

работников, имеющих право на доступ к информации, оформить им допуск, ознакомить с перечнями сведений, составляющих объект защиты, и порядком работы с ними, закрепить в трудовых договорах с такими работниками обязанность не разглашать охраняемую законом тайну; промаркировать носители конфиденциальной информации соответствующей надписью с указанием обладателя информации (ст. 10 ФЗ «О коммерческой тайне»).

Кроме того, Трудовой кодекс РФ указывает, что в трудовом договоре с работником в качестве его дополнительного условия может быть закреплено условие о неразглашении охраняемой законом тайны. Некоторые исследователи считают, что введение у работодателя режима тайны обязывают его включить работника в отношения по правовой защите такой информации. Так, например, М. С. Сагандыков полагает, что условие трудового договора о неразглашении охраняемой законом тайны (государственной, служебной, профессиональной или коммерческой) должно относиться к числу обязательных, если работник допускается к соответствующей информации (Сагандыков 2019, 38). Е. В. Ракитина и М. С. Кошелев предлагают закрепить в ТК РФ «промежуточную» природу такого условия трудового договора, предусмотрев, что «указанное условие является обязательным в случае, если трудовая функция работника подразумевает работу с информацией, составляющей тайну» (Ракитина и Кошелев 2022, 38).

Однако следует принимать во внимание тот факт, что условие о неразглашении конфиденциальной информации, имеющей режим тайны, потому и является дополнительным, что включается в трудовой договор инициативно, по предложению работодателя, для того чтобы иметь возможность привлечь работника к ответственности за разглашение конфиденциальных сведений: к дисциплинарной вплоть до увольнения за разглашение охраняемой законом тайны или персональных данных другого работника (подп. «в» п. 6 ч. 1 ст. 81 ТК РФ), а также к материальной за разглашение сведений, имеющих режим тайны, в полном размере причиненного ущерба (п. 7 ч. 1 ст. 243 ТК РФ). При этом иные, публично-правовые последствия разглашения работником информации ограниченного доступа не зависят от наличия или отсутствия в трудовом договоре такого условия — в случае если действия работника содержат состав административного правонарушения или уголовно наказуемого деяния, он будет привлечен к ответственности независимо от того, есть ли в трудовом договоре условие о сохранении конфиденциальности информации. Включение же условия о неразглашении тайны в разряд обязательных позволит восполнять в этой части трудовой договор по правилам части третьей ст. 57 ТК РФ, что ухудшит положение работника по сравнению с моментом заключения трудового договора. По этой причине считаем, что условие о неразглашении конфиденциальной информации, к которой работник имеет доступ в связи с выполнением своей трудовой функции, совершенно обоснованно отнесено законодателем к дополнительным условиям, внесение которого в трудовой договор зависит от воли сторон и достижения между ними соглашения, а его наличие (отсутствие) влияет только на возможность (невозможность) привлечения работника к трудоправовой ответственности и не затрагивает права и законные интересы третьих лиц и публичные интересы.

2.2. Привлечение работника к дисциплинарной ответственности за нарушение правил обращения с информацией ограниченного доступа

Трудовое законодательство формулирует только один дисциплинарный проступок, совершенный в связи с нарушением правил обращения с информацией ограниченного доступа, — разглашение охраняемой законом тайны или персональных данных другого работника, но относит его к грубым и позволяет работодателю применить за его совершение к работнику такую меру дисциплинарной ответственности, как увольнение (подп. «в» п. 6 ч. 1 ст. 81 ТК РФ). Как разъяснено в Постановлении Пленума ВС РФ от 17.03.2004 № 2 «О применении судами Российской Федерации Трудового кодекса Российской Федерации», для признания увольнения по данному основанию законным работодателю следует доказать два обстоятельства: сведения, которые работник разгласил, относятся к охраняемой законом тайне или персональным данным; работник имел доступ к такой информации в связи с выполнением трудовых обязанностей и принял на себя обязательство не разглашать ее.

При этом понятие «разглашение» ни в ТК РФ, ни в указанном Постановлении не раскрывается, но его нормативное определение содержится, например, в п. 9 ст. 3 ФЗ «О коммерческой тайне»: под разглашением следует понимать действие или бездействие, в результате которых конфиденциальная информация в любой возможной форме становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому договору. Данное определение, несмотря на его закрепление в специальном законе, применимо, по нашему мнению, и к другим случаям распространения конфиденциальной информации. Аналогичное по сути определение содержится в национальном стандарте Российской Федерации «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения» (ГОСТ Р 53114-2008)[9], согласно которому разглашением информации является «несанкционированное доведение защищаемой информации до лиц, не имеющих права доступа к этой информации». Понятие распространения персональных данных содержит п. 5 ст. 3 ФЗ «О персональных данных» — действия, направленные на раскрытие данных сведений неопределенному кругу лиц.

Таким образом, разглашение конфиденциальной информации имеет место только в том случае, если в результате действий работника она стала известна лицам, к ней не допущенным. Кроме указанного проступка, работник может нарушить установленные работодателем правила обращения с информацией и совершить действия, не связанные с ее распространением, но создающие такую угрозу, влекущие или могущие повлечь иные негативные последствия для работодателя (искажение, уничтожение и пр.). Соответственно, следует различать дисциплинарный проступок, представляющий собой разглашение сведений, составляющих информацию ограниченного доступа, за совершение которого законодатель позволяет работодателю уволить работника, и дисциплинарный проступок в виде иного

[9] ГОСТ Р 53114-2008. «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения» (утв. и введен в действие Приказом Ростехрегулирования от 18.12.2008 № 532-ст).

несоблюдения режима защиты информации, однократное совершение которого по действующему законодательству не может являться основанием для увольнения работника.

Несмотря на такое, на наш взгляд, достаточно явно следующее из правового регулирования разграничение дисциплинарных проступков, в правоприменительной практике не наблюдается единообразия в вопросе о том, что считать распространением конфиденциальной информации, влекущем возможность увольнения работника по дисциплинарному основанию.

Одни суды признают незаконным увольнение работника в тех случаях, когда нарушение им правил защиты информации не повлекло ее разглашения, т. е. доступа к ней третьих лиц. Так, например, суд признал незаконным увольнение работника по основанию, предусмотренному подп. «в» п. 6 ч. 1 ст. 81 ТК РФ, за копирование конфиденциальной информации на флеш-носитель, указав, что такие действия без разглашения информации не образуют состава вмененного работнику дисциплинарного проступка[10]. В другом деле суд кассационной инстанции, отменяя решение суда апелляционной инстанции, признавшего законным увольнение работника, скопировавшего на внешний носитель информацию, являющуюся коммерческой тайной работодателя, указал, что имевшаяся у уволенного работника возможность по распоряжению скопированной информацией еще не означает совершения им конкретных действий, в результате которых информация стала известна третьим лицам[11].

Другие суды высказывают противоположную позицию, считая, что действия работника по копированию информации или ее пересылке через незащищенные каналы связи без цели передачи ее третьим лицам можно оценивать как разглашение конфиденциальной информации и признавать в такой ситуации увольнение работника законным.

Подобное правоприменение имело место и в деле гражданина, обратившегося с жалобой в Конституционный Суд РФ (далее — КС РФ). Суд, куда гражданин, уволенный по предусмотренному подп. «в» п. 6 ч. 1 ст. 81 ТК РФ основанию за пересылку конфиденциальной информации с электронного адреса корпоративной почты на свой личный адрес, обратился с иском о восстановлении на работе, посчитал правообладателя интернет-сервиса, посредством которого осуществлялась передача информации, обладателем конфиденциальной информации, отправленной истцом, и отказал в иске, посчитав его действия разглашением конфиденциальной информации. КС РФ по жалобе данного гражданина рассматривал вопрос о конституционности п. 5 ст. 2 ФЗ «Об информации, информационных технологиях и о защите информации»[12], закрепляющего понятие «обладатель информации». В Постановлении от 26.10.2017 № 25-П (далее — Постановление № 25-П)[13] данная норма была признана не противоречащей Конституции РФ, поскольку она не наде-

[10] Определение Первого кассационного суда общей юрисдикции от 24.10.2022 № 88-27205/2022. Аналогичная позиция выражена в Определении этого же суда от 19.07.2022 № 88-18870/2022.

[11] Определение Первого кассационного суда общей юрисдикции от 17.01.2022 № 88-175/2022.

[12] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 31.07.2006. № 31 (ч. 1). Ст. 3448.

[13] Постановление КС РФ от 26.10.2017 № 25-П по делу о проверке конституционности п. 5 ст. 2 Федерального закона «Об информации, информационных технологиях и о защите информации» в связи с жалобой гражданина А. И. Сушкова.

ляет правообладателя интернет-сервиса статусом обладателя информации, содержащейся в передаваемых сообщениях пользователей, и не позволяет правообладателю интернет-сервиса разрешать или ограничивать доступ к этой информации; напротив, он обязан обеспечить тайну связи. Вместе с тем КС РФ указал, что такие действия работника все же могут рассматриваться как нарушение прав и законных интересов работодателя — обладателя информации, поскольку в результате их совершения гражданин получает возможность распоряжаться такими сведениями без согласия работодателя, т. е. создается угроза неконтролируемого распространения информации. При этом действия работника вопреки предпринятым работодателем разумным мерам по защите информации могут рассматриваться в качестве нарушения прав и законных интересов работодателя как обладателя информации.

Несмотря на то что данная правовая позиция сформулирована не в отношении каких-либо норм ТК РФ, а применительно к оценке положения, регулирующего отношения в информационной сфере, некоторые правоприменители ее восприняли как подтверждение ранее имевшейся практики признания законным увольнения работника за разглашение конфиденциальной информации в ситуации, когда он нарушил внутренние правила обращения с информацией, но эти нарушения не повлекли за собой такого последствия, как передача (известность) информации третьим лицам. В этих случаях, по мнению судов, распространение подтверждается самим фактом выхода информации из-под контроля ее обладателя. Так, в одном из постановлений суд указал, что действия работника по отправке через почтовый сервис конфиденциальной информации являются разглашением коммерческой тайны работодателя, сославшись при этом на Постановление № 25-П[14]. В другом деле суд посчитал доказанным совершение работником дисциплинарного проступка, выражающегося в разглашении охраняемой законом тайны, при отправке файлов, содержащих конфиденциальную информацию, на стороннее принадлежащее истцу устройство (флеш-носитель), не предусмотренное для хранения таких данных согласно локальным нормативным актам работодателя, поскольку эти действия создали условия для дальнейшего неконтролируемого распространения скопированной информации[15]. Судебные решения об отказе в удовлетворении требований уволенных работников с аналогичной мотивировкой принимаются в ситуации отправки работником конфиденциальной информации с адреса корпоративной почты на свой личный адрес электронной почты[16], а также в случае загрузки работником охраняемой информации во внешнее облачное хранилище[17]. Такой подход поддерживается и в научно-практической литературе (Коршунова, 2019). В тех же случаях, когда увольнение в подобных обстоятельствах признается незаконным, суды могут ссылаться не на отсутствие состава дисциплинарного проступка, заключающегося в разглашении защищаемой информации, а на несо-

[14] Апелляционное определение Санкт-Петербургского городского суда от 05.05.2021 № 33-1290/2021 по делу № 2-253/2020.

[15] Определение Третьего кассационного суда общей юрисдикции от 10.03.2021 по делу № 88-2992/2021.

[16] См., например, Апелляционное определение Московского городского суда от 18.06.2020 по делу № 33-17559/2020. Аналогичные обстоятельства и выводы изложены в Определении Четвертого кассационного суда общей юрисдикции от 16.08.2022 № 88-19420/2022 по делу № 2-1364/2021.

[17] См., например, Апелляционное определение Санкт-Петербургского городского суда от 05.05.2021 № 33-1290/2021 по делу № 2-253/2020.

размерность примененной работодателем меры дисциплинарного воздействия совершенному деянию[18].

Между тем в рассматриваемом Постановлении КС РФ специально подчеркнул, что юридическая, в том числе дисциплинарная, ответственность работника за действия в нарушение имеющихся у работодателя правил обращения с информацией устанавливается актами трудового законодательства, и наступать она может только за те деяния, которые признаются правонарушениями действующим на момент их совершения законом. Соответственно, КС РФ обратил внимание правоприменителей на то обстоятельство, что основания для привлечения работника к ответственности следует искать в ТК РФ и действовать сообразно буквальному содержанию его положений. При этом он призвал федерального законодателя своевременно и адекватно реагировать на меняющиеся отношения в информационной сфере и принимать меры к совершенствованию правового регулирования юридической ответственности.

Рассмотренная судебная практика, в том числе содержащийся в Постановлении № 25-П посыл законодателю о совершенствовании правового регулирования, наглядно демонстрирует, что действующее законодательство не всегда своевременно реагирует на потребности развития информационного общества с его все ускоряющимися информационными потоками и не обеспечивает защиту прав и законных интересов как работодателя, так и работника.

3. Выводы

Сегодня в правовом регулировании, обеспечивающем право работодателя на защиту информации, сложилась парадоксальная ситуация. Положения трудового законодательства, предоставляющие работодателю возможность реагировать на действия нарушающего режим защиты информации работника, допускают привлечение такого работника к дисциплинарной ответственности вплоть до увольнения. Однако к самой строгой мере дисциплинарного воздействия — увольнению по основанию, предусмотренному подп. «в» п. 6 ч. 1 ст. 81 ТК РФ, — работодатель вправе прибегнуть только тогда, когда работник разгласил вверенные ему конфиденциальные сведения, т. е. сделал их доступными третьим лицам или неопределенному кругу лиц. Все же остальные нарушения, в чем бы они ни выражались и сколь бы существенными они ни были, позволяют только объявить работнику замечание или выговор и надеяться, что работник, продолжающий работать с защищаемой работодателем информацией, больше не допустит нарушения режима конфиденциальности либо совершит еще один дисциплинарный проступок, что позволит его уволить за неоднократность нарушения (п. 6 ч. 1 ст. 81 ТК РФ). Такое положение в условиях бурного развития информационно-коммуникационных технологий, позволяющих мгновенно делиться большим объемом информации или распространять ее среди неопределенного круга лиц, заставляет работодателя, стремящегося защитить свою информационную сферу, пойти на единственно допускаемый законодателем способ прекращения доступа работника к конфиден-

[18] См., например, Определение Второго кассационного суда общей юрисдикции от 26.07.2022 по делу № 88-16912/2022.

циальной информации — увольнение даже при отсутствии состава вменяемого работнику дисциплинарного проступка (разглашение). Суды же, рассматривающие иски работников о признании увольнения незаконным, видимо, признавая высокую степень угрозы для прав и законных интересов работодателя и третьих лиц при совершении работником действий по выведению информации из-под сферы контроля ее обладателя, предпочитают защитить информационную безопасность работодателя, несмотря на отсутствие к тому формально-юридических оснований и нарушая при этом права работников.

В целях обеспечения права работодателя на действенное сохранение конфиденциальной информации, а также защиты прав и законных интересов работников, допущенных к такой информации, следует:

1) дать четкое разъяснение понятия «разглашение» применительно к положению, содержащемуся в п. 6 ч. 1 ст. 81 ТК РФ, с целью придания ему определенности, что позволит увольнять работников только за совершение тех проступков, которые повлекли передачу информации третьим лицам или ее распространение среди неопределенного круга лиц; при этом данный факт должен входить в предмет доказывания по делам об увольнении работников за такие деяния;

2) предусмотреть в трудовом законодательстве механизм лишения работника допуска к любой защищаемой работодателем конфиденциальной информации, а не только к государственной тайне, закрепив в качестве основания прекращения такого допуска нарушение работником установленных работодателем правил обращения с информацией ограниченного доступа, создавшее угрозу ее распространения. При этом последствия прекращения такого допуска должны быть аналогичны последствиям прекращения допуска к государственной тайне: если работник может выполнять свою трудовую функцию и без работы с конфиденциальной информацией, он продолжает трудиться; если же прекращение допуска к защищаемым сведениям препятствует выполнению трудовых обязанностей, то работодатель обязан предложить работнику иную работу, которую работник способен выполнять исходя из имеющейся у него квалификации и состояния здоровья, и только при отсутствии такой работы (должности) или при отказе работника от перевода работодатель вправе уволить работника.

Такое правовое регулирование, на наш взгляд, будет отвечать требованию об обеспечении баланса прав и законных интересов сторон трудового договора: работодатель исключит доступ к информации работника, создавшего угрозу ее распространения, а работник получит возможность продолжить работу.

Библиография

Бондаренко, Эльвира Н., и Дмитрий В. Иванов. 2012. *Конфиденциальная информация в трудовых отношениях*. Санкт-Петербург: Юридический центр «Пресс».

Гребенщиков, Анатолий В., Нелли И. Дивеева и Александр В. Кузьменко. 2020. «Трудовые отношения с интернет-агрегатором: завтрашняя реальность?» *Ежегодник трудового права* 10: 53–66.

Информационные технологии в бизнесе. 2002. Под ред. М. Желены. Санкт-Петербург: Питер.

Ковалева, Наталия Н. 2012. *Информационное право России: Учебное пособие*. Москва: Дашков и К.

Коршунова, Татьяна Ю. 2019. «Некоторые проблемы расторжения трудового договора за разглашение охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей, в том числе разгла-

шение персональных данных другого работника.» *Комментарий судебной практики*. Отв. ред. К. Б. Ярошенко. Москва: Институт законодательства и сравнительного правоведения при Правительстве РФ, КОНТРАКТ, 107–118.
Лушников, Андрей М. и Марина В. Лушникова. 2020. «Трудовое право и цифровая экономика: российский опыт в контексте мировых тенденций.» *Ежегодник трудового права* 10: 19–29.
Лушников, Андрей М. и Марина В. Лушникова. 2015. *Трудовые права в XXI веке: современное состояние и тенденции развития.* Москва: Проспект.
Офман, Елена М. 2021. «Наблюдение и контроль в трудовых отношениях: баланс прав и интересов работников и работодателей.» *Журнал российского права* 25 (11): 73–87.
Ракитина, Екатерина В., и Михаил С. Кошелев. 2022. «Некоторые вопросы государственной и коммерческой тайны в трудовых отношениях.» *Государственная власть и местное самоуправление* 8: 35–40.
Сагандыков, Михаил С. 2019. «Реализация конституционного права на защиту информации в трудовых отношениях.» *Вестник Южно-Уральского государственного университета. Серия: Право* 26: 36–41.
Филипова, Ирина А. 2023. «Метавселенные: как их развитие повлияет на работников и работодателей.» *Ежегодник трудового права* 13: 45–64.
Чесалина, Ольга В. 2021. «Новеллы законодательства о дистанционной (удаленной) работе: сравнительно-правовой анализ.» *Актуальные проблемы российского права* 9: 99–113.

Статья поступила в редакцию 25 мая 2023 г.;
рекомендована к печати 24 июля 2023 г.

Контактная информация:

Пугачёва Наталья Владимировна — канд. юрид. наук, доц.; n.v.pugachiova@gmail.com

Ensuring the employer's right to information protection: Problems of legal regulation

N. V. Pugacheva

Russian State University of Justice,
5, Aleksandrovskiy park, St. Petersburg, 197046, Russian Federation

For citation: Pugacheva, Natalia V. 2024. "Ensuring the employer's right to information protection: Problems of legal regulation." *Russian Journal of Labour & Law* 14: 219–230.
https://doi.org/10.21638/spbu32.2024.113 (In Russian)

In the context of the rapid development of information and communication technologies and the proclamation of the constitutional right of everyone to freely search, receive and disseminate information, it is becoming increasingly difficult to restrict access to information of various kinds. Meanwhile, the confidential information at the disposal of the employer, access to which he restricts either in his own interests (commercial secret), or in the public interest or in the interests of third parties (information that has a secret regime, personal data of individuals) needs protection. The subject of the study is the provisions of the legislation, including labor legislation, which allow the employer, as the owner of confidential information, to build a system of limited access to it and take measures against employees who violate the established rules for protecting information. An analysis of the relevant norms leads to the conclusion that in the rapidly developing information society, which provides ample opportunities for the instant transmission (distribution) of a significant amount of information, the current legal regulation does not fully meet the requirements for balancing the rights and legitimate interests of the employee and the employer, since it allows the employer to stop the employee's

access to protected information only by dismissing him on a disciplinary basis, which forces the employer to make such decisions even in cases where there are no grounds for this fixed by law (disclosure), thereby violating the rights of the employee. In this regard, it is proposed to introduce a legal mechanism for depriving an employee of access to confidential information when he commits actions that create a threat of its dissemination, which, on the one hand, will exclude him from working with such information, and on the other hand, will allow him (under certain conditions) to continue work for this employer. Such a mechanism, being aimed at optimal reconciliation of the interests of employers and employees, will ensure the right of the employer to the protection of information and at the same time will not allow excessive restriction of the rights of the employee.

Keywords: confidential information, trade secret, information and communication technologies, personal information, disclosure of secrets, disciplinary liability.

References

Bondarenko, El'vira N., and Dmitrii V. Ivanov. 2012. *Confidential Information in an Employment Relationship*. St. Petersburg: Iuridicheskii tsentr Press. (In Russian)

Grebenshchikov, Anatolii V., Nelli I. Diveeva and Aleksandr V. Kuz'menko. 2020. "Labor relations with an Internet aggregator: Tomorrow's reality?" *Russian Journal of Labour & Law* 10: 53–66. (In Russian)

Information technology in business. 2002. Ed. by M. Zheleny. St. Petersburg: Piter Publ.

Kovaleva, Nataliia N. 2012. *Russian Information Law: textbook*. Moscow: Dashkov i K Publ. (In Russian)

Korshunova Tat'iana Iu. 2019. "Some problems of termination of an employment contract for disclosing a secret protected by law (state, commercial, official and other), which became known to the employee in connection with the performance of his labor duties, including the disclosure of personal data of another employee." *Kommentarii sudebnoi praktiki*. Ed. by K. B. Iaroshenko. Moscow: Institut zakonodatel'stva i sravnitel'nogo pravovedeniia pri Pravitel'stve RF Publ., KONTRAKT Publ., 24, 107–118. (In Russian)

Lushnikov, Andrei M., and Marina V. Lushnikova. 2020. "Labor law and the digital economy: Russian experience in the context of global trends." *Russian Journal of Labour & Law* 10: 19–29. (In Russian)

Lushnikov, Andrei M., and Marina V. Lushnikova. 2015. *Labor rights in the 21st century: Current state and development trends.* Moscow: Prospekt Publ. (In Russian)

Ofman, Elena M. 2021. "Supervision and control in labor relations: Balance of rights and interests of employees and employers." *Zhurnal rossiiskogo prava* 25 (11): 73–87. (In Russian)

Rakitina, Ekaterina V., and Mikhail S. Koshelev. 2022. "Some issues of state and commercial secrets in labor relations." *Gosudarstvennaia vlast' i mestnoe samoupravlenie* 8: 35–40. (In Russian)

Sagandykov, Mikhail S. 2019. "Implementation of the constitutional right to protection of information in labor relations." *Vestnik Iuzhno-Ural'skogo gosudarstvennogo universiteta. Seriia: Pravo* 2: 36–41. (In Russian)

Filipova, Irina A. 2023. "Metaverses: How their development will affect workers and employers." *Russian Journal of Labour & Law* 13: 45–64. (In Russian)

Chesalina, Ol'ga V. 2021. "Legislative novelties on remote (remote) work: A comparative legal analysis." *Aktual'nye problemy rossiiskogo prava* 9: 99–113. (In Russian)

Received: May 25, 2023
Accepted: July 24, 2023

Author's information:

Natalia V. Pugacheva — PhD in Law, Associate Professor; n.v.pugachiova@gmail.com