

Место персональных данных в системе информации ограниченного доступа



Е.К. Волчинская

главный специалист по информационному праву Фонда «Центр инноваций и информационных технологий» Федеральной нотариальной палаты, доцент Национального Исследовательского университета Высшей школы экономики, кандидат экономических наук. Адрес: 127006, Российская Федерация, Москва, Долгоруковская ул., д. 20. E-mail: info@fciit.ru



Аннотация

Предлагается подход к формированию в российском законодательстве «закрытой» системы ограничения доступа к информации, то есть системы, содержащей ограниченное количество видов тайн. Согласно авторской концепции тайны классифицируются по способу их образования:

«первичные» тайны непосредственно связаны с деятельностью субъекта и обеспечивают реализацию его права на ограничение доступа к касающейся его информации (такие тайны составляет информация, вырабатываемая субъектом в процессе его деятельности или жизнедеятельности);

«производные» тайны связаны с обязанностью субъекта по защите информации другого субъекта, получаемой в режиме тайны (режиме конфиденциальности).

Определяются элементы правового режима для каждой из категорий тайн, в том числе субъектный состав, состав правовых регуляторов. Предложены принципы трансформации режимов тайн при передаче информации. Исследуются режимы конфиденциальности, приемлемые для защиты персональных данных (коммерческая тайна, профессиональная тайна, государственная и служебная тайны) и делается вывод о целесообразности использования этих режимов, а не самостоятельного режима защиты персональных данных. Рассматриваются отдельные проблемы защиты персональных данных в режиме коммерческой тайны, связанные с соотношением положений Трудового кодекса Российской Федерации, Федерального закона «О коммерческой тайне» и Федерального закона «О персональных данных». Формулируются условия достижения баланса интересов субъекта персональных данных (работника) и оператора (работодателя).

Исследуется вопрос о сбалансированности норм ответственности за разглашение различных видов тайн. Отмечается, что соотношение санкций не представляется логичным. Например, уравниены максимальные санкции за разглашение коммерческой и государственной тайн, не продумано соотношение уголовной ответственности за нарушение неприкосновенности частной жизни и другие преступления, которые, по сути, «обеспечивают» ответственность за нарушение неприкосновенности частной жизни (нарушение тайны переписки, разглашение тайны усыновления). присутствует разброс в санкциях за разглашение различных профессиональных тайн. Все это требует совершенствования мер ответственности в рамках формируемой и законодательно закрепленной системы тайн.



Ключевые слова

информация ограниченного доступа, виды тайн, режим конфиденциальности, персональные данные, государственная тайна, коммерческая тайна, профессиональная тайна, уголовная и административная ответственность

Ограничение доступа к информации — это **важный элемент демократического общества**, который призван защищать как конституционные права граждан на доступ к информации, так и конституционные права различных субъектов на ограничение этого доступа. Указанные ограничения должны быть законными (установленными федеральным законом) и соразмерными, обеспечивающими баланс интересов субъектов по доступу к информации и ограничению доступа.

Почему нужна именно система ограничения доступа к информации? Ответим от противного:

- отсутствие системы создает условия для нарушения прав граждан на доступ к информации и прав на ограничение доступа;
- отсутствие системы создает условия для злоупотреблений правами граждан на доступ к информации и правами на ограничение доступа;
- отсутствие системы не позволяет эффективно защищать информацию, а значит, и права субъектов.

В целом отсутствие системы ограничения доступа к информации тормозит развитие демократических институтов информационного общества¹.

Какой должна быть или может быть такая система?

«Открытой» (содержащей неограниченное количество видов информации ограниченного доступа) или «закрытой» (содержащей ограниченное число видов информации ограниченного доступа)? Выбор зависит от возможности свести все существующие виды информации ограниченного доступа к ограниченному количеству.

Существующие обозначения информации ограниченного доступа при всем терминологическом разнообразии российского законодательства в сфере информационной безопасности включают четыре:

- 1) информация ограниченного доступа (или ограниченного распространения);
- 2) информация, в отношении которой следует обеспечить конфиденциальность (эта конструкция применяется после принятия Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и внесения изменений в иные федеральные законы в целях унификации терминологии);
- 3) тайны;
- 4) конфиденциальная информация (в нескольких федеральных законах, в которые не внесли изменения после принятия Федерального закона от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации»).

¹ Неверно рассматривать как системообразующий Перечень сведений конфиденциального характера, утвержденный Указом Президента Российской Федерации от 6 марта 1997 г. № 188. Данный перечень изначально был спорным по составу сведений, а сейчас он прямо противоречит законодательству Российской Федерации как минимум в части пункта 3 (служебная тайна), поскольку определение понятия «служебная тайна» опирается на положения статьи 139 Гражданского кодекса Российской Федерации, которая утратила силу еще в 2006 году. Кроме этого, Законом об информации исключено разделение информации ограниченного доступа на информацию, составляющую государственную тайну, и конфиденциальную информацию. Не употребляется и сам термин «конфиденциальная информация». Более того, по смыслу закона, ограничивая доступ к информации, необходимо обеспечить ее конфиденциальность, что относится как к государственной тайне, так и к другим видам тайн. Следовательно, термин «конфиденциальная информация», производный от термина «конфиденциальность», будет включать информацию, составляющую государственную тайну, что также не учитывается в Перечне сведений конфиденциального характера. Кроме того, сфера применения Перечня сведений конфиденциального характера ограничена целями «дальнейшего совершенствования порядка опубликования и вступления в силу актов Президента Российской Федерации, Правительства Российской Федерации и нормативных правовых актов федеральных органов исполнительной власти».

Содержательно первая и вторая группы равноценны и включают две последующие.

Можно ли создать «закрытую» систему тайн? Такая система предпочтительна, поскольку она более надежно защищает информационные права субъектов. В юридической литературе присутствуют различные подходы к классификации тайн². Концепция «закрытой» системы тайн была предложена автором³, и составляют ее две категории тайн: тайны «первичные» и тайны «производные»⁴.

Согласно концепции тайны классифицируются по способу их образования:

- «первичные» тайны непосредственно связаны с деятельностью субъекта и обеспечивают реализацию его права на ограничение доступа к касающейся его информации (такие тайны составляет информация, вырабатываемая субъектом в процессе его деятельности или жизнедеятельности);

- «производные» тайны связаны с обязанностью субъекта по защите информации другого субъекта, получаемой в режиме тайны (режиме конфиденциальности).

В состав «первичных» тайн входят: личная и семейная тайны (тайна физического лица); коммерческая тайна (тайна юридического лица, осуществляющего предпринимательскую деятельность); государственная тайна и служебная тайна в части внутрисистемной информации (тайна государства, в том числе в лице органа государственной власти).

Здесь и далее я говорю о служебной тайне в концепции законопроекта, который долгое время находился на рассмотрении Государственной Думы, но так и не был принят. В соответствии с этой концепцией информация, составляющая служебную тайну, включает:

- информацию, создаваемую (генерируемую) в органе государственной власти, доступ к которой временно ограничен в интересах государственного управления по решению руководителя;

- информацию, представляемую в орган государственной власти в режиме конфиденциальности.

В состав «производных» тайн входят:

- профессиональные тайны, когда информация передается субъекту профессиональной деятельности от физических лиц в режиме личной или семейной тайны (врачебная тайна, тайна исповеди, тайна банковских вкладов, тайна усыновления, налоговая тайна, нотариальная тайна и др.) либо от юридических лиц в режиме коммерческой тайны (налоговая, банковская, нотариальная тайны и др.);

- служебная тайна в части переданной в органы власти от физических и юридических лиц информации ограниченного доступа (по типу профессиональной тайны государственных и муниципальных служащих).

Принципиальное различие этих категорий тайн состоит в том, что для «первичных» тайн у субъектов (обладателей соответствующей информации) есть право на установ-

² См., напр., Пилипенко Ю.С. К вопросу о классификации правовых тайн // Журнал российского права. 2009. no 9. С. 48–56.

³ См.: Волчинская Е.К. Роль государства в обеспечении информационной безопасности // Информационное право. 2008. no 4. 9–16; Волчинская Е.К. Коммерческая тайна в системе конфиденциальной информации // Информационное право. 2005. no 3. С. 17–21; Волчинская Е.К. О проблемах формирования правовой системы ограничения доступа к информации // Информационное право. 2013. no 4. С. 3–8.

⁴ Терминология может быть изменена. Можно вообще не называть категории тайн, но важно определить их характерные признаки.

ление режима конфиденциальности, а для «производных» тайн у лица, которому доверена информация ограниченного доступа, возникает обязанность устанавливать соответствующий режим конфиденциальности.

Максимальный объем регулирования «первичных» тайн со стороны государства приходится на государственную и служебную тайны.

В отношении других видов «первичных» тайн государство должно уступить право основного регулятора тем субъектам, которые образуют (устанавливают) эти режимы. Задача государства — обеспечить защиту их прав и интересов с учетом интересов других субъектов.

В отношении «производных» тайн государство в целях защиты прав и интересов физических и юридических лиц, предоставляющих информацию в каком-либо режиме конфиденциальности, обязывает субъектов (при исполнении ими профессиональных обязанностей или при осуществлении ими определенных видов деятельности) защищать такую информацию.

Автором был проведен эксперимент, в результате которого почти все виды информации ограниченного доступа, содержащиеся в «Перечне нормативных актов, относящихся сведения к категории ограниченного доступа» (их там 54), подготовленном специалистами фирмы «КонсультантПлюс»⁵ и размещенном в соответствующей информационно-поисковой системе, попали в одну из указанных категорий тайн⁶. Исходя из этого, можно утверждать, что создание «закрытой» системы в принципе возможно и, соответственно, создание «открытой» системы не целесообразно.

Ни в одну из указанных категорий тайн первоначально не попали два вида информации:

- информация, содержащаяся в паспортах безопасности объектов топливно-энергетического комплекса (Федеральный закон от 21 июля 2011 г. N 256-ФЗ «О безопасности объектов топливно-энергетического комплекса»);
- инсайдерская информация (Федеральный закон от 27 июля 2010 г. N 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации»).

Эти виды информации не вполне укладываются в предложенную выше систему тайн, поскольку указанные федеральные законы предусматривают обязательное установление режима конфиденциальности для «первичных» тайн (государственной, коммерческой и служебной), что ограничивает права соответствующих субъектов на установление режима конфиденциальности и распоряжение сведениями, составляющими одну из таких тайн.

В первом случае паспорт безопасности содержит информацию об обеспечении антитеррористической защищенности объекта топливно-энергетического комплекса и план мероприятий по обеспечению антитеррористической защищенности объекта, поэтому установление режима конфиденциальности такой информации, а именно режима коммерческой тайны, не находится в прямом противоречии с правами обладателя информации. А дополнительные обязанности по согласованию паспортов безопасности с органами исполнительной власти, и (или) органами местного самоуправления, по нашему

⁵ При подготовке данной статьи использовалась СПС «КонсультантПлюс».

⁶ Волчинская Е.К. О проблемах формирования правовой системы ограничения доступа к информации // Информационное право. 2013. no 4. С. 3–8.

мнению, укладываются в конституционный принцип ограничения прав субъектов (ч. 3 ст. 55 Конституции Российской Федерации).

Во втором случае дело обстоит сложнее, поскольку в соответствии с законом инсайдерская информация включает, в том числе, сведения, составляющие коммерческую, служебную, банковскую тайну, тайну связи и иную охраняемую законом тайну. Следовательно, исходя из определения к такой информации, могут быть отнесены и сведения, составляющие государственную тайну. При этом законом накладываются определенные ограничения на использование инсайдерской информации, а с другой стороны, закон предусматривает обязательное раскрытие или предоставление инсайдерской информации. Очевидно, что это положение противоречит, по меньшей мере, Закону Российской Федерации от 21 июля 1993 г. по 5485-1 «О государственной тайне» и Федеральному закону от 29 июля 2004 г. по 98-ФЗ «О коммерческой тайне», которыми установлены права и обязанности обладателя соответствующей информации. Для устранения этих противоречий необходимо, по нашему мнению, уточнить определение и концепцию защиты инсайдерской информации.

После уточнения соответствующих режимов конфиденциальности указанные особенности могут быть нивелированы, и тогда система тайн будет сведена к «закрытой» системе.

Для законодательного оформления системы информации ограниченного доступа необходимо, прежде всего, определить субъектов правоотношений и соотнести их с видами тайн:

- личность (физическое лицо) безотносительно к ее служебному положению образует и обеспечивает конфиденциальность сведений, составляющих личную тайну;
- социальная общность (семья, общественное объединение, хозяйствующий субъект) образует и обеспечивает конфиденциальность соответственно семейной тайны, коммерческой тайны либо обеспечивает конфиденциальность профессиональной тайны;
- государство (в лице органов государственной власти) образует и обеспечивает конфиденциальность государственной и служебной тайны.

Следующим элементом системы информации ограниченного доступа является состав правовых регуляторов применительно к каждой категории тайн, которые необходимо реализовать в федеральном законе.

Для «первичных» тайн необходимо законодательно установить:

- ограничения на введение режима тайны (режима конфиденциальности) для информации, к которой есть общественный интерес;
- обязанность и условия предоставления информации, составляющей тайну, другим лицам, в том числе в органы государственной власти, для осуществления государственного управления и отправления правосудия;
 - в отдельных случаях — требования к используемым средствам защиты информации, составляющей тайну, или ограничения на использование таких средств;
 - в отдельных случаях — требования к субъектам, обеспечивающим защиту информации, составляющей тайну;
 - меры ответственности за нарушение конфиденциальности информации.

Для «производных» тайн необходимо законодательно установить:

- обязанность лиц, которым доверена информация, составляющая «первичные» тайны, обеспечивать ее конфиденциальность;
- меры ответственности за нарушение конфиденциальности доверенной информации;

- условия предоставления доверенной информации третьим лицам;
- в отдельных случаях требования к используемым средствам защиты конфиденциальности информации или ограничения на использование таких средств.

Для завершения концепции формирования системы тайн необходимо решить три актуальные проблемы:

1) формирование режима служебной тайны (конструкция, содержание информации и права и обязанности обладателя информацией, ответственность за нарушение режима конфиденциальности);

2) согласование правил изменения (трансформации) режимов тайн при передаче информации между субъектами, особенно из органов государственной власти;

3) установление принципов иерархии в системе тайн и уточнение норм ответственности за разглашение сведений, составляющих тайну, с учетом соотношения видов тайн.

Первую проблему можно решить в рамках разработки проекта Федерального закона «О служебной тайне». Новый проект подготовлен и проходит обсуждение в Правительстве Российской Федерации.

Принципы (правила) трансформации режимов тайн предлагается сформулировать следующим образом:

1) «первичные» тайны могут переходить как в один из режимов «первичных» тайн, так и в один из режимов тайн «производных», за исключением, о котором ниже;

2) «производные» тайны могут переходить только в режим государственной тайны или служебной тайны (комплексный по своей структуре).

Рассмотрим подробнее, как реализуются эти принципы.

В отношении «первичных» тайн:

- сведения, составляющие государственную тайну, и информация, составляющая служебную тайну, при передаче в любую организацию, охраняются в том же режиме;

- сведения, составляющие государственную тайну, при рассекречивании могут охраняться в режиме коммерческой, служебной тайны, личной или семейной тайны;

- информация, составляющая коммерческую, служебную, личную или семейную тайну, может быть засекречена в режиме государственной тайны;

- информация, составляющая коммерческую тайну, может при передаче в орган государственной власти охраняться в режиме служебной тайны;

- информация, составляющая личную или семейную тайну, может в случае использования ее в рамках предпринимательской деятельности охраняться в режиме коммерческой тайны;

- информация, составляющая личную, семейную, коммерческую тайну, при передаче в органы и организации может перейти в режим профессиональной тайны, если таковой установлен законом.

Особенность трансформации режимов «первичных» тайн состоит, по мнению автора, в том, что сведения, составляющие государственную тайну, не могут охраняться в других режимах, если они не рассекречены, поскольку этот режим все же имеет (или должен иметь) определенный приоритет. Вероятно, эта особенность распространяется и на режим служебной тайны. В любом случае новая концепция федерального закона о служебной тайне должна ответить и на данный вопрос.

В отношении «производных» тайн, исходя из рассмотренного выше механизма их формирования, возможности трансформации режимов ограничены. Поскольку эта категория тайн обеспечивает охрану сведений, составляющих коммерческую, личную или семейную тайну, то возврат в эти режимы не нужен (они сохраняют свое действие

наряду с профессиональной тайной). Следовательно, трансформация режимов «производных» (профессиональных) тайн фактически возможна только в сторону режима государственной или служебной тайны.

Особенности трансформации режимов «первичных» тайн вновь возвращают нас к вопросу об иерархии в системе тайн. Представляется, что государственная тайна должна сохранить приоритет перед другими «первичными» тайнами. В свою очередь, последние не могут иметь приоритет перед тайнами «производными», поскольку, в силу условий формирования, «производные» тайны» включают «первичные».

Для законодательного закрепления системы тайн возможно использовать два варианта: либо в Федеральном законе от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее — Закон об информации), либо в новом самостоятельном законе. Предпочтительнее это сделать в рамках дополнения действующего Закона об информации и не плодить новые нормативные правовые акты.

Принятие практически одновременно Закона об информации и Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее — Закон о персональных данных) не обеспечило, к сожалению, их согласование в части правового режима персональных данных.

Нужно ли особым образом защищать персональные данные, если и без этого существуют режимы личной, семейной, профессиональной, государственной, коммерческой, служебной тайн? Вопрос не простой, и российское законодательство отвечает на него противоречиво⁷.

Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» определил предмет правоотношений как любую информацию, относящуюся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). Следовательно, персональные данные не определены как информация ограниченного доступа.

Закон об информации ограничился в отношении персональных данных отсылочной нормой к специальному законодательству, правда, в статье 9 «Ограничение доступа к информации». Тем не менее, и этот закон не отнес персональные данные в явной форме к категории информации ограниченного доступа.

Объяснить это можно следующим.

Во-первых, далеко не все персональные данные охраняются режимом конфиденциальности (некоторые персональные данные должны быть обнародованы в соответствии с федеральными законами, например, персональные данные кандидатов в депутаты, другие могут быть обнародованы по решению субъекта персональных данных, например, содержащиеся в профессиональных энциклопедиях).

Во-вторых, персональные данные могут охраняться и охраняются в настоящее время различными режимами ограниченного доступа. Так, в режиме государственной тайны охраняются персональные данные ряда лиц, имеющих доступ к государственным секретам. В режиме коммерческой тайны могут охраняться персональные данные авторов ноу-хау, используемых в производстве. В режиме коммерческой или профессиональной тайны охраняется информация персонального характера, характеризующая пользователей предоставляемых услуг. В режиме личной тайны — сведения об особенностях личности, ее пристрастиях, привычках, интересах

⁷ Волчинская Е.К. Нотариальная тайна и режимы конфиденциальности // Нотариальный вестник. 2013. № 4. С. 27–39.

Исходя из этого, можно утверждать, что персональные данные — это вид сведений, непосредственно связанных с личностью и/или позволяющих ее идентифицировать, но не режим тайны. Законодательное регулирование сбора и использования персональных данных обусловлено защитой неприкосновенности частной жизни как базового конституционного принципа⁸.

Тем не менее Закон о персональных данных определяет (статья 19) меры по обеспечению безопасности персональных данных при их обработке вне зависимости от установленного оператором режима конфиденциальности, а скорее исходя из самостоятельного режима конфиденциальности персональных данных.⁹

В рамках уточнения в 2009–2010 гг. концепции обеспечения конфиденциальности и безопасности персональных данных правоприменителями предлагалось операторов негосударственных информационных систем обязать защищать свои системы либо в рамках режимов конфиденциальности, распространяемых на информационную систему в целом (в частности, режимы защиты банковской тайны, налоговой тайны и иных видов тайн, установленных федеральными законами), либо исходя из общих стандартов защиты информации, самостоятельно определяя адекватные методы и средства защиты персональных данных с учетом их природы, объема обрабатываемых данных, стоимости применения мер защиты, характеристик информационных систем оператора и учитывая отраслевые рекомендации.

Однако данная концепция встретила сопротивление регуляторов и не была реализована. Несмотря на смягчение в 2011 году под влиянием протестов правоприменителей требований по безопасности персональных данных, вопрос их соотношения с мерами, принимаемыми для защиты сведений в установленных их обладателем режимах конфиденциальности, остается открытым.

Рассмотрим особенности охраны персональных данных в рамках отдельных режимов конфиденциальности.

Проблемы охраны персональных данных в режиме коммерческой тайны определяются тем, что требования по защите персональных данных обязательны, а режим коммерческой тайны обладатель информации (работодатель) устанавливает по своему усмотрению с учетом законодательных ограничений. Следовательно, он вынужден либо охранять все персональные данные в режиме коммерческой тайны (это сейчас практикуется), либо устанавливать для них (или для части их) какой-то особый режим конфиденциальности.

⁸ См. Малейна М.Н. Право на тайну и неприкосновенность персональных данных // Журнал российского права. 2010. no 11. С. 18–28; Смирнова И.Г. К вопросу о роли правовых позиций Конституционного Суда РФ для защиты уголовно-процессуального института тайны // Адвокат. 2010. no 3. С. 5–12.

⁹ Постановление Правительства РФ от 1 ноября 2012 г. no 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных»; Приказ ФСБ России от 10 июля 2014 г. no 378 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» (Зарегистрировано в Минюсте России 18 августа 2014 г. no 33620); Приказ ФСТЭК России от 18 февраля 2013 г. no 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (Зарегистрировано в Минюсте России 14 мая 2013 г. no 28375).

Первый вариант удобен работодателю, поскольку он может унифицировать механизмы защиты информации, составляющей коммерческую тайну, и механизмы защиты персональных данных. Однако ряд уважаемых исследователей считают, что «сведения о персонале не могут являться коммерческой тайной, а составляют персональные данные и должны защищаться в соответствии с гл. 14 Трудового кодекса РФ и Законом о персональных данных»¹⁰.

В частности, ссылаясь на ТК РФ, Л.К.Терещенко указывает (там же) «Спорным является отнесение к коммерческой тайне сведений о должностных окладах, системе премирования и иного поощрения». В числе сведений, которые не могут составлять коммерческую тайну, названы сведения о системе оплаты труда (п. 5 ст. 5 Федерального закона от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне») и об оплате труда работников некоммерческих организаций (п. 9 ст. 5 этого Закона). Следовательно, данное ограничение не относится к сведениям о размере оплаты труда конкретного работника.

Возникает вопрос о возможных правовых последствиях разглашения информации о своей заработной плате самим работником. Если признать, что эти сведения составляют коммерческую тайну, то в соответствии с подп. «в» п. 6 ст. 81 Трудового кодекса РФ (далее — ТК РФ) работнику грозит увольнение. Необходимо обратить внимание на формулировку этого положения в ТК РФ: «Трудовой договор может быть расторгнут работодателем в случаях: ...в) разглашения охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей, в том числе разглашения персональных данных другого работника»¹¹.

Отсюда следуют два вывода:

1) персональные данные рассматриваются как составная часть охраняемой законом тайны;

2) разглашение работником чужих персональных данных может повлечь увольнение. Следовательно, такие персональные данные не должны быть известны другим работникам, в том числе и от самого работника. Фактически ТК РФ дает работодателю право запрещать разглашение своих персональных данных работником. Это элемент кадровой политики, который характерен для постсоветского бизнеса. Вместе с тем, не исключая, что некоторые работники будут благодарны работодателю за полученное от него законное право не сообщать членам семьи размер своего дохода.

Если же данные о заработной плате работника охраняются в режиме персональных данных, то работник вправе самостоятельно определять порядок их распространения. Но вступая в трудовые отношения, работник принимает на себя определенные обязанности, установленные работодателем, в том числе обязанности, касающиеся режимов охраны сведений, ставших известными работнику в связи с исполнением трудовых обязанностей.

У.М. Станскова (там же) сомневается, что при отнесении информации о заработной плате к коммерческой тайне работодателем может быть получена коммерческая выгода, хотя последнее является признаком коммерческой тайны. Действительно, федеральным

¹⁰ Терещенко Л.К. Правовой режим персональных данных и безопасность личности // Закон. 2013. № 6. С. 37-43; Станскова У.М. Правовой анализ локальных нормативных актов работодателя по защите информации ограниченного доступа // Трудовое право в России и за рубежом. 2011. № 2. С. 30–32.

¹¹ К сожалению, авторы часто игнорируют соотношение в указанном положении ТК РФ персональных данных и тайн как частного и общего. См., напр.: Топоркова С.А. Разглашение охраняемой законом тайны как трудовое правонарушение // Трудовое право в России и за рубежом. 2012. № 3. С. 26–30.

законом коммерческая тайна определяется как «режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду» (п. 1 ст. 3). Полагаю, что в данном случае коммерческая выгода работодателя может складываться, как минимум, из трех составляющих:

- 1) возможность избежать неоправданных расходов при обеспечении одного режима конфиденциальности вместо двух;
- 2) возможность оптимизировать фонд заработной платы за счет индивидуальных условий трудового договора;
- 3) возможность удержать ценных работников от перехода к конкурентам.

Вместе с тем, необходимо признать, что судами общей юрисдикции созданы прецеденты как отмены решений работодателя, основанных на охране персональных данных в режиме коммерческой тайны¹², так и признания такой охраны правомерной¹³.

У.М. Станкова указывает также на то, что введение режима коммерческой тайны в отношении сведений о заработной плате влечет закрепление в локальных нормативных актах ряда запретов для работников, из смысла которых следует, в частности, что «работнику получить справку о доходах для получения кредита в банке или для оформления визы невозможно. Дело в том, что в соответствии с положениями ч. 1 ст. 6 Федерального закона «О коммерческой тайне» обладатель информации, составляющей коммерческую тайну, обязан предоставить информацию, составляющую коммерческую тайну, только по мотивированному требованию органа государственной власти, иного государственного органа, органа местного самоуправления. Однако ст. 62 ТК РФ предусматривает, что по письменному заявлению работника работодатель обязан выдать копии документов, связанных с работой, в том числе справки о размере заработной платы и фактически начисленных и уплаченных налогов».

Представляется, что указанная проблема лежит не столько в плоскости соотношения режимов конфиденциальности, сколько в корректности установления и обеспечения режима коммерческой тайны. Очевидно, что работодатель не может руководствоваться в своей деятельности только ТК РФ, только Федеральным законом «О коммерческой тайне» или только Федеральным законом «О персональных данных». Все законодательное регулирование исполняется им в совокупности. При этом в разных случаях могут устанавливаться разные приоритеты. В частности, когда работнику требуется справка для получения кредита в банке или оформления визы, у работодателя нет оснований отказывать ему в этом, хотя бы потому, что передача этих сведений банку или ФМС не наносит ему коммерческого вреда. То есть в данном случае приоритет имеют права работника. С другой стороны, можно представить ситуацию, когда в целях защиты от недобросовестной конкуренции работодатель жестко запрещает разглашать сведения о заработной плате и иных выплатах работнику, участвующему в проведении выставок, конференций, переговоров и т.п.

Специалисты-правоведы обращают внимание на дисбаланс интересов в российском законодательстве в сторону абсолютизации интересов субъекта персональных

¹² См., напр.: Иванов И. Не растерять коммерческую тайну // ЭЖ-Юрист. 2013. № 35. С. 1, 6.

¹³ Напр.: Нюлланд Е.С., Перевалов В.А. Охрана и защита информации, составляющей коммерческую тайну // Закон. 2013. № 6. С. 48–55.

данных без учета реальных возможностей операторов¹⁴. Этим существенно различаются положения Закона о персональных данных и Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных. В качестве оператора выступает и работодатель. Обеспечение баланса интересов работодателя (оператора) и работника (субъекта персональных данных) особенно необходимо при разработке и применении мер защиты информации, составляющей коммерческую тайну, в том числе персональных данных, таких как результаты видеонаблюдения, прослушивания служебного телефона, просмотра электронной почты и др.

Работодателю при этом необходимо осознавать, что уважение и защита интересов работника как субъекта персональных данных приносит работодателю коммерческую выгоду — повышается производительность труда.

Работнику стоит помнить, что трудовые отношения ставят его неизбежно в зависимое положение от работодателя, но уважение и защита интересов работодателя приносит дивиденды и самому работнику — повышается оплата труда.

Однако в выборе режима конфиденциальности для защиты персональных данных работников работодатель законом не ограничен.

В части соотношения профессиональной тайны и персональных данных необходимо отметить, что профессиональная тайна собственно и включает сведения, составляющие личную или семейную тайну (персональные данные) и (или) информацию, составляющую коммерческую тайну. Примером «однородной» профессиональной тайны является врачебная тайна, а примерами «смешанной» — налоговая¹⁵ и нотариальная.

Например, в соответствии с Основами законодательства Российской Федерации о нотариате нотариус, должностные лица нотариальных палат, лица, осуществляющие обработку вносимых в единую информационную систему нотариата сведений, обязаны хранить в тайне сведения, которые стали ему известны в связи с осуществлением его профессиональной деятельности, не раскрывать третьим лицам и не распространять сведения, содержащиеся в этой информационной системе, за исключением случаев, установленных Основами. За разглашение или незаконное использование указанных сведений (составляющих нотариальную тайну) такие лица несут ответственность, предусмотренную законодательством Российской Федерации. Применительно к конкретной информационной системе уровень защиты сведений, составляющих нотариальную тайну, выше требований по безопасности персональных данных, установленных Законом о персональных данных и принятыми в соответствии с ним нормативными правовыми актами. При этом, конечно, реализуется один режим конфиденциальности, а не два.

Применительно к государственной тайне, полагаю, что баланс интересов субъектов персональных данных, имеющих доступ к сведениям, составляющим государственную тайну, смещается в сторону интересов государства, требования по защите сведений, составляющих государственную тайну, жестче требований по защите персональных данных, но и при этом работодатель должен помнить о правах субъекта персональных данных и защищать их в тех случаях, когда это не противоречит требованиям защиты государственной тайны. К этому его обязывает Конституция Российской Федерации, в ч. 3 ст. 55 которой и установлены принципы баланса интересов:

¹⁴ Терещенко Л.К. О соблюдении баланса интересов при установлении мер защиты персональных данных // Журнал российского права. 2011. № 5. С. 5–12; Назарова Д.Н. Проблемы правовой охраны операторами персональных данных // Информационное право. 2010. № 1. С. 14–19.

¹⁵ Шеховцева Е.В. Налоговая тайна: правовой режим охраны // Ленинградский юридический журнал. 2013. № 1. С. 38–42.

«3. Права и свободы человека и гражданина могут быть ограничены федеральным законом только в той мере, в какой это необходимо в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства».

Вернемся к одному из поставленных в самом начале вопросов. Это вопрос о сбалансированности норм ответственности за разглашение различных видов информации ограниченного доступа.

До недавнего времени диспропорции были вопиющими, в частности, уголовная ответственность за разглашение коммерческой, банковской и налоговой тайны (ст. 183 УК РФ) была выше, чем ответственность за разглашение государственной тайны (ст. 283 УК РФ). Федеральный закон от 7 декабря 2011 г. № 420-ФЗ ее устранил, снизив максимальный срок лишения свободы по статье 183 УК РФ с 10 до 7 лет. Однако существующее соотношение санкций вызывает много вопросов. Например, уравнились максимальные санкции за разглашение коммерческой и государственной тайн. Очень большой разброс в санкциях за разглашение различных профессиональных тайн. Минимальный уровень одинаков — штраф в размере 80 тысяч рублей, а вот максимальный колеблется от исправительных работ на срок до 1 года (ст. 138, ст. 141 УК РФ) до лишения свободы на срок до 7 лет (налоговая, банковская тайны, ст. 183 УК РФ).

Странным выглядит соотношение санкций по ст. 137 («Нарушение неприкосновенности частной жизни») и другим статьям УК РФ, которые, по сути, «обеспечивают» ответственность за нарушение неприкосновенности частной жизни (нарушение тайны переписки, разглашение тайны усыновления). Получается, что за незаконное собирание, например, журналистом сведений о частной жизни лица (в том числе об усыновлении) установлена минимальная ответственность в виде штрафа в размере до 200 тысяч рублей, а за незаконное предоставление этих сведений журналисту работником органа опеки и попечительства последний будет наказан штрафом в размере до 80 тысяч рублей.

А вот уголовное наказание на разглашение врачебной тайны в явной форме не установлено¹⁶. Есть общий состав административного правонарушения — Статья 13.14. «Разглашение информации с ограниченным доступом» Кодекса Российской Федерации об административных правонарушениях, который покрывает все случаи разглашения, за исключением случаев, если разглашение такой информации влечет уголовную ответственность. Установлены санкции по этой статье: административный штраф на граждан в размере от 500 до 1 тысячи рублей; на должностных лиц — от 4 тысяч до 5 тысяч рублей.

Определена также административная ответственность за «Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)» (Статья 13.11.). Минимальная санкция — штраф от 300 до 1 тыс. рублей, максимальный штраф — до 10 тыс. руб.

Получается, что за разглашение врачебной тайны, т.е. распространение персональных данных пациента, виновное лицо может быть оштрафовано либо на 5 тыс. руб. (по ст. 13.14) либо на 10 тыс. руб. (по ст. 13.11). Разница невелика, но все же она есть. Кроме того, сомнительно, чтобы даже максимальный штраф удовлетворил субъекта персональных данных, чьи данные были разглашены.

Трудно сказать, каким должно быть соотношение санкций за разглашение различных видов тайн, но, очевидно, что это соотношение должно быть логичным, причем

¹⁶ Иванов И.С. Врачебная тайна // СПС «КонсультантПлюс». 2012.

такая логика должна вытекать из конструкции системы ограничения доступа к информации. А это еще один аргумент в пользу ее создания и законодательного оформления.



Библиография

- Бриллиантова Н.А., Архипов В.В. Об охраняемой законом тайне в трудовых отношениях // Законодательство и экономика. 2010. № 1. С. 33–40.
- Волчинская Е.К. Коммерческая тайна в системе конфиденциальной информации // Информационное право. 2005. № 3. С. 17–21.
- Волчинская Е.К. Роль государства в обеспечении информационной безопасности // Информационное право. 2008. № 4. С. 9–16.
- Волчинская Е.К. О проблемах формирования правовой системы ограничения доступа к информации // Информационное право. 2013. № 4. С. 3–8.
- Волчинская Е.К. Нотариальная тайна и режимы конфиденциальности // Нотариальный вестник. 2013. № 4. С. 27–39.
- Иванов И. Не растерять коммерческую тайну // ЭЖ-Юрист. 2013. № 35. С. 1, 6.
- Иванов И.С. Врачебная тайна // СПС «КонсультантПлюс». 2012.
- Малеина М.Н. Право на тайну и неприкосновенность персональных данных // Журнал российского права. 2010. № 11. С. 18–28.
- Назарова Д.Н. Проблемы правовой охраны операторами персональных данных // Информационное право. 2010. № 1. С. 14–19.
- Нюлландс Е.С., Перевалов В.А. Охрана и защита информации, составляющей коммерческую тайну // Закон. 2013. № 6. С. 48–55.
- Пилипенко Ю.С. К вопросу о классификации правовых тайн // Журнал российского права. 2009. № 9. С. 48–56.
- Смирнова И.Г. К вопросу о роли правовых позиций Конституционного Суда РФ для защиты уголовно-процессуального института тайны // Адвокат. 2010. № 3. С. 5–12.
- Терещенко Л.К. Правовой режим персональных данных и безопасность личности // Закон. 2013. № 6. С. 37–43.
- Терещенко Л.К. О соблюдении баланса интересов при установлении мер защиты персональных данных // Журнал российского права. 2011. № 5. С. 5–12.
- Топоркова С.А. Разглашение охраняемой законом тайны как трудовое правонарушение // Трудовое право в России и за рубежом. 2012. № 3. С. 26–30.
- Станкова У.М. Правовой анализ локальных нормативных актов работодателя по защите информации ограниченного доступа // Трудовое право в России и за рубежом. 2011. № 2. С. 30–32.
- Шеховцева Е.В. Налоговая тайна: правовой режим охраны // Ленинградский юридический журнал. 2013. № 1. С. 38–42.

Role of Personal Data in the System of Information with Restricted Access



Elena Volchinskaya

Associate Professor, Chief Specialist on Information Law, Centre of Innovation and Information Technology at the Federal Chamber of Notaries, National Research University Higher School of Economics, Candidate of Economical Sciences. Address: 20 Dolgorukovskaya Str., Moscow, 127006, Russian Federation. E-mail: info@fciit.ru



Abstract

The article proposes a personal approach to the formation in Russian legislation a closed system of limiting access to information that is a system with several types of secrets. Under the presented conception, the secrets are classified by the type of their formation. Primary secrets directly related to the activity of a subject and ensure his right to the restricted access to the information. Such secrets deal with the information processed by the subject during his activity. Derived secrets relate to the obligation of a subject as to the protection of information of another subject and communicated on a secret basis (regime of confidentiality). The article specifies the elements of legal regime for each type of secrets including subjective elements and the elements of legal regulators. The article proposes the principles of transforming the regimes for secrets when transmitting information. It studies the regimes of confidentiality acceptable to protect personal data (commercial secret, professional secret, state secret, business secret) and makes a conclusion on the necessity to use these regimes instead of establishing an independent regime of the personal data protection. The author examines certain problems of protecting personal data in the regime of commercial secret, related to the RF Labour Code and the Federal laws *On Commercial Secret* and *On Personal Data*. The paper also formulates the conditions of achieving the balance of interests of the subject of personal data (employee) and the operator (employer). A question is studied as to the balance of responsibility of norms for disclosing different types of secrets. It is noted that the balance of sanctions is inconsistent. In particular, maximum sanctions for disclosing commercial or state secrets are equal, the balance has not been arranged properly as to the criminal liability for breaching privacy (breaching the secret of correspondence, disclosing the secret of adoption), sanctions vary too much in relation to the disclosure of professional secrets. All these aspects require the further development of liability measures within the system of secrets.



Keywords

Information of restricted access, types of secrets, privacy, personal data, state secrets, commercial secret, professional secret, criminal and administrative liability.

Citation: Volchinskaya E.K. Role of Personal Data in the System of Information with Restricted Access. *Pravo. Zhurnal Vysshey shkoly ekonomiki*, no. 4, pp. 193–207 (in Russian)



References

- Brilliantova N.A., Arkhipov V.V. (2010) Ob okhrayaemoy zakonom tayne v trudovih otnosheniyah [On the Protected by Law Secret in Labour Relations]. *Zakonodatelstvo i ekonomika*, no 1, pp. 33–40.
- Ivanov I.S. (2012) *Vrachebnaya tayna* [Medical Secrecy]. Moscow, Yuridicheskaya pressa.
- Ivanov I. (2013) Ne rasterat' kommercheskuyu taynu [Do not Lose Commercial Secret]. *EJ-urist*, no 35. pp. 1, 6.
- Maleina M.N. (2010) Pravo na taynu i neprikosновенnost' personal'nykh dannykh [Right to the Secrecy and Immunity of Personal Information]. *Zhurnal rossiyskogo prava*, no 11, pp. 18–28.
- Nazarova D.N. (2010) Problemy pravovoy okhrany operatorami personal'nykh dannykh [The Problems of Legal Protection of Personal Data by Operators]. *Informatsionnoe pravo*, no 1, pp. 14–19.
- Nyullans E.S., Perevalov V.A. (2013) Okhrana i zashchita informatsii, sostavlyayushchey kommercheskuyu taynu [Protection and security of Information related to Commercial Secrecy]. *Zakon*, no 6, pp. 48–55.
- Pilipenko Yu.S. (2009) K voprosu o klassifikatsii pravovykh tayn [On Classifying Legal Secrets]. *Zhurnal rossiyskogo prava*, no 9, pp. 48–56.
- Smirnova I.G. (2010) K voprosu o roli pravovykh pozitsiy Konstitutsionnogo Suda RF dlya zashchity ugovolno-protsessual'nogo instituta tayny [On the Role of Legal Positions of the RF Constitutional Court to protect the institution of secrecy]. *Advokat*, no 3, pp. 5–12.
- Tereshchenko L.K. (2013) Pravovoy rezhim personal'nykh dannykh i bezopasnost' lichnosti [Legal Regime of Personal Data and Personal Security]. *Zakon*, no 6, pp. 37–43.

Tereshchenko L.K. (2011) O soblyudenii balansa interesov pri ustanovlenii mer zashchity personal'nykh dannykh [On the Balance of Interests to Establish the Measures to Protect Personal Data]. *Zhurnal Rossiyskogo prava*, no 5, pp. 5–12.

Toporkova S.A. (2012) Razglashenie okhranyaemoy zakonom tayny kak trudovoe pravonarushenie [Disclosing Protected by Law Secret as a Breach of Labour Law]. *Trudovoe pravo v Rossii i za rubezhom*, no 3, pp. 26–30.

Stanskova U.M. (2011) Pravovoy analiz lokal'nykh normativnykh aktov rabotodatelya po zashchite informatsii ogranichenogo dostupa [Legal Analysis of Local Norms of Employers to Protect the Information with Limited Access]. *Trudovoe pravo v Rossii i za rubezhom*, no 2, pp. 30–32.

Shekhovtseva E.V. (2013) Nalogovaya tayna: pravovoy rezhim okhrany [Tax Secret]. *Leningradskiy yuridicheskiy zhurnal*, no 1, pp. 38–42.

Volchinskaya E.K. (2005) Kommercheskaya tayna v sisteme konfidentsial'noy informatsii [Commercial Secret in the System of Confidential Information]. *Informatsionnoe pravo*, no 3, pp. 17–21.

Volchinskaya E.K. (2008) Rol' gosudarstva v obespechenii informatsionnoy bezopasnosti [The Role of State in Ensuring Information Security]. *Informatsionnoe pravo*, no 4, pp. 9–16.

Volchinskaya E.K. (2013) O problemakh formirovaniya pravovoy sistemy ogranicheniya dostupa k informatsii [On the Problems of the Legal Basis for Restricting Access to Information]. *Informatsionnoe pravo*, no 4, pp. 3–8.

Volchinskaya E.K. (2013) Notarial'naya tayna i rezhimy konfidentsial'nosti [Notarial Secret and Confidentiality Regimes]. *Notarial'nyy vestnik*, no 4, pp. 27–39.