# Государственный контроль в сфере защиты персональных данных

**Л.К. Терещенко**

Заслуженный юрист Российской Федерации, зам. заведующего отделом административного законодательства и процесса Института законодательства и сравнительного правоведения при Правительстве Российской Федерации, доктор юридических наук. Адрес: 115142, Российская Федерация, Москва, Коломенская ул., 21, кв. 234. E-mail: ltereschenko@hse.ru

**Аннотация**

Статья посвящена наиболее актуальным проблемам, возникающим в процессе применения законодательства о персональных данных при осуществлении государственного контроля за соблюдением установленных требований, а также анализу правоприменительной практики, в том числе защите персональных данных несовершеннолетних. Установленные требования защиты персональных данных рассматриваются с точки зрения обеспечения баланса интересов личности, общества в целом и бизнес-структур, что предполагает соразмерность, обоснованность и выполнимость этих требований, включая требование обеспечить «адекватную» защиту персональных данных. Юридические и технические требования, устанавливаемые в целях обеспечения защиты персональных данных, прав физических лиц и законных интересов юридических лиц, должны быть четко сбалансированы и адекватны, чтобы не создавать помех развитию рынка, с одной стороны, и не нарушать интересов субъектов персональных данных, с другой. Показана практика контроля за соблюдением законодательства о персональных данных. Автором установлено, что контрольные мероприятия, как правило, направлены на обеспечение защиты информации о гражданах как таковой, соблюдение условий ее обработки, а не прав граждан при обработке их персональных данных. Не всегда формальное соблюдение оператором требований законодательства о персональных данных свидетельствует о соблюдении интересов самих субъектов персональных данных. Имеет место направленность государственного контроля на проверку формального соблюдения законодательства, неурегулированность отдельных вопросов, нечеткость норм, позволяющих неоднозначно их трактовать, в том числе при проведении государственного контроля и надзора. В статье проводится анализ общих тенденций развития и совершенствования государственного контроля. Предлагается применение дифференцированного подхода к тем сферам, где обрабатываются персональные данные. Делается вывод о необходимости модернизации организации контрольной деятельности по защите персональных данных, активизации использования новых технологий обработки информации. Особое внимание уделено правоприменительной практике защиты персональных данных несовершеннолетних, в том числе их биометрических персональных данных.

**Ключевые слова**

государственный контроль, персональные данные, право на неприкосновенность частной жизни, ограничения прав, баланс интересов, судебная практика, несовершеннолетние

Библиографическое описание: Терещенко Л. К. Государственный контроль в сфере защиты персональных данных // Право. Журнал Высшей школы экономики. 2018. № 4. С. 142–161.

JEL: K1; УДК: 340 DOI: 10.17323/2072-8166.2018.4.142.161

Государственная политика в сфере защиты персональных данных строится исходя из конституционных положений, касающихся неприкосновенности частной жизни, личной и семейной тайн, прав человека, принятого в развитие конституционных положений законодательства и международных обязательств Российской Федерации, в том числе вытекающих из Европейской конвенции о защите физических лиц при автоматизированной обработке персональных данных (Страсбург, 28.01.1981), а также из Договора о Евразийском экономическом союзе от 29.05. 2014[1].

Поскольку право на защиту персональных данных — это право относительное, а не абсолютное[2], при установлении требований к защите персональных данных принципиальным моментом является обеспечение баланса интересов личности, общества и бизнес-структур, что предполагает соразмерность, обоснованность и реальную выполнимость этих требований, включая требование обеспечить «адекватную» защиту персональных данных. Соответственно, юридические и технические требования, устанавливаемые в целях защиты персональных данных, прав физических лиц и законных интересов юридических лиц, должны быть сбалансированы и адекватны, чтобы не создавать помех развитию рынка, с одной стороны, и нарушения интересов субъектов персональных данных — с другой.

Основные требования к обеспечению защиты персональных данных установлены Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»[3] (далее — ФЗ № 152-ФЗ) и принятыми в его исполнение под-

[1] Официальный сайт Евразийского экономического союза [Электронный ресурс]: // URL: http://eaeunion.org/ (дата обращения: 01.08.2018)

[2] Такой позиции придерживается Конституционный суд Российской Федерации и на этом же принципе строится законодательство ЕС (см. Регламент № 2016/679 Европейского парламента и Совета Евросоюза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных)» (Брюссель, 27.04.2016).

[3] СЗ РФ. 2006. № 31 (1 ч.). Ст. 3451.

законными нормативными правовыми актами. Эти требования обращены, прежде всего, к операторам персональных данных, к которым согласно ФЗ № 152-ФЗ относятся государственные и муниципальные органы, юридические или физические лица, самостоятельно или совместно с другими лицами организующие / осуществляющие обработку персональных данных, а также определяющие цели их обработки, состав данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Требования к обработке персональных данных вытекают практически из каждой статьи, но есть статьи, непосредственно обращенные к операторам персональных данных. Это ст. 18 «Обязанности оператора при сборе персональных данных», ст. 18.1 «Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных настоящим Федеральным законом», ст. 19 «Меры по обеспечению безопасности персональных данных при их обработке». Оператор обязан принимать меры, необходимые и достаточные для выполнения установленных обязанностей. При этом оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для их обеспечения.

В свою очередь, государство в лице уполномоченных органов осуществляет контроль и надзор за соблюдением установленных законодательством мер. ФЗ № 152-ФЗ содержит самостоятельную главу, посвященную государственному контролю и надзору за обработкой персональных данных, в которой имеется только одна статья, посвященная этой теме — ст. 23. Согласно ей, уполномоченный орган по защите прав субъектов персональных данных обеспечивает, организует и осуществляет государственный контроль и надзор за соответствием обработки персональных данных требованиям ФЗ № 152-ФЗ и принятых в соответствии с ним нормативных правовых актов. В настоящее время функции контроля за выполнением операторами установленных требований возложены на Роскомнадзор. При этом необходимо отметить, что с 1 сентября 2015 г. отношения по контролю и надзору за соблюдением законодательства о персональных данных выведены из сферы действия Федерального закона от 26.12.2008 № 294-ФЗ[4] «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля»[5]. В соответствии с ч. 1.1 ст. 23 ФЗ № 152-ФЗ (введенной Федеральным законом от

[4] Федеральный закон от 21.07.2014 № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях» // СПС Гарант.

[5] С 1.09. 2015 также не требуется согласования проверок с прокуратурой. Основаниями для включения проверки в план являются начало осуществления оператором деятельности по обработке персональных данных, а также истечение трех лет со дня государственной регистрации оператора или окончания последней плановой проверки оператора.

22.02.2017 № 16-ФЗ[6]), порядок организации и проведения проверок юридических лиц и индивидуальных предпринимателей, являющихся операторами обработки персональных данных, уполномоченным органом по защите прав субъектов персональных данных, а порядок организации и осуществления государственного контроля и надзора за их обработкой иными лицами, являющимися операторами, устанавливается Правительством Российской Федерации. Прошло более года, но до сих пор данный нормативный правовой акт не принят[7].

При исполнении контрольных функций Роскомнадзор действует в соответствии с постановлением Правительства России от 16.03.2009 № 228 «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций» (которым утверждено Положение о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций) и Административным регламентом исполнения Роскомнадзором государственной функции по осуществлению государственного контроля (надзора) за соответствием обработки персональных данных требованиям федерального законодательства в области персональных данных (утв. Приказом Минкомсвязи России от 14.11.2011 № 312).

Согласно Административному регламенту, предметом государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства в области персональных данных являются: 1) документы, характер информации в которых предполагает или допускает включение в них персональных данных[8]; 2) информационные системы персональных данных; 3) деятельность по обработке персональных данных.

---

[6] Федеральный закон от 22.02.2017 № 16-ФЗ «О внесении изменений в главу 5 Федерального закона «О персональных данных» и статью 1 Федерального закона «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля» // СЗ РФ. 2017. № 9. Ст. 1276.

[7] Как сообщает Роскомнадзор, выведение с 1 сентября 2015 года государственного контроля и надзора в области персональных данных из сферы действия Закона № 294-ФЗ изменило отдельные аспекты организации и проведения контрольно-надзорных мероприятий.

[8] Административный регламент № 312 (п. 67.1) предусматривает приблизительный перечень документов, которые могут выступать предметами проверки. К ним, в частности, относятся: 1) уведомление об обработке персональных данных; 2) локальные акты оператора, регламентирующие порядок и условия обработки персональных данных; 3) письменное согласие субъекта персональных данных на их обработку; 4) документы, подтверждающие соблюдение требований законодательства при обработке специальных категорий и биометрических персональных данных, в частности, наличие у оператора соответствующих оснований для их обработки; 5) документы, подтверждающие уничтожение оператором персональных данных по достижении цели их обработки; 6) документы, необходимые для проверки фактов о возможных нарушениях законодательства о персональных данных, изложенных в обращениях граждан и информации, поступившей в Роскомнадзор; 7) документы, подтверждающие выполнение оператором предписаний об устранении ранее выявленных нарушений законодательства о персональных данных.

Последний предмет контроля настолько широк, что, по сути, включает два первых предмета. Независимо от предмета контроля Служба имеет право запрашивать и получать необходимые документы (сведения) для достижения целей проведения проверки, получать доступ к информационным системам персональных данных в режиме просмотра и выборки необходимой информации, принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушениями требований законодательства в области персональных данных, обращаться в суд с исковыми заявлениями в защиту прав субъектов персональных данных и т.д.

Вместе с тем согласно Административному регламенту Роскомнадзор не вправе требовать предъявления оператором документов или информации, если они не относятся к предмету проверки, а также если сведения и документы могут быть получены им из иных органов государственного контроля (надзора), органов муниципального контроля.

Как было сказано, Роскомнадзор является уполномоченным федеральным органом исполнительной власти по защите прав субъектов персональных данных. При этом, как видим, сам субъект персональных данных по общему правилу не информирован о контрольных и проверочных мероприятиях, не инициирует их. Иными словами, контрольные мероприятия, как правило, не зависят от воли лица, чьи персональные данные обрабатываются, от наличия или отсутствия у него претензий к оператору персональных данных, хотя субъект персональных данных сам может обращаться по поводу нарушения его прав (непосредственно к оператору персональных данных, в уполномоченный государственный орган, в судебные органы, в прокуратуру). По сути, правила контроля и надзора направлены на обеспечение защиты информации о гражданах как таковой, соблюдение условий ее обработки, а не прав граждан при обработке их персональных данных.

Далеко не всегда формальное соблюдение оператором требований законодательства о персональных данных свидетельствует о соблюдении интересов самих субъектов персональных данных. В таких случаях государственный контроль оказывается неэффективным. Как правило, это связано с направленностью государственного контроля на проверку формального соблюдения законодательства, неурегулированностью отдельных вопросов, либо нечеткостью норм, позволяющих неоднозначно их трактовать, в том числе при проведении государственного контроля и надзора. Между тем по ст. 2 ФЗ № 152-ФЗ целью этого Закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Несмотря на то, что отношения по контролю и надзору за соблюдением законодательства о персональных данных выведены из сферы действия Фе-

дерального закона от 26.12.2008 № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля», общие тенденции развития и совершенствования государственного контроля (надзора) и муниципального контроля должны проявляться и в рассматриваемой сфере. К общим тенденциям следует отнести: 1) упор на повышение результативности и эффективности контрольно-надзорной деятельности, в том числе посредством внедрения в деятельность контрольно-надзорных органов риск-ориентированного подхода при организации и осуществлении контрольно-надзорной деятельности; 2) расширение арсенала инструментов, применяемых контрольно-надзорными органами, в первую очередь осуществляемых без взаимодействия этих органов с юридическими лицами[9].

Необходим также учет задач, поставленных в программе «Цифровая экономика в Российской Федерации» (утв. распоряжением Правительства Российской Федерации от 28 июля 2017 г. № 1632-р), в частности, задачи пересмотреть принципы контрольно-надзорной деятельности с отказом от бумажной отчетности и ее переводом в цифровой вид, в том числе введением цифрового архива, чтобы в максимальной степени обеспечить автоматизацию основных процессов в данной сфере. Учет количества выявленных в результате контрольно-надзорных мероприятий нарушений обязательных требований, назначенных административных наказаний и сумм взысканных административных штрафов не должен служить критериями оценки деятельности органов государственного контроля (надзора) в целом и в сфере защиты персональных данных, в частности.

Важным, на наш взгляд, является применение дифференцированного подхода к тем сферам, где обрабатываются персональные данные, поскольку в целом ряде случаев субъекты персональных данных даже не знают, что их персональные данные обрабатываются, в каких целях и кто их обрабатывает. Чаще всего это происходит в сети Интернет. Новые технологии, прежде всего технология «больших данных», позволяют получить такие персональные данные, которые сам субъект персональных данных не предоставлял, не знает об их обработке и, разумеется, не давал согласия на обработку. Безусловно, технология больших данных требует изощренного правового регулирования.

Роскомнадзор, на который возложен контроль и надзор за соблюдением законодательства о персональных данных, ежегодно готовит отчет о состоянии их защиты. Последний отчет подготовлен за 2016 год. Как следует из

[9] См., напр.: Распоряжение Правительства России от 01.04.2016 № 559-р «Об утверждении плана мероприятий («дорожной карты») по совершенствованию контрольно-надзорной деятельности в Российской Федерации на 2016–2017 годы» // СЗ РФ. 2016. № 15. Ст. 2118.

отчета, в рамках функции по осуществлению государственного контроля и надзора в 2016 году было проведено 1 307 плановых проверок и 99 внеплановых проверок, а также 333 плановые проверки в отношении государственных органов, муниципальных органов, организующих и (или) осуществляющих обработку персональных данных. Учитывая общее количество операторов персональных данных, такие цифры крайне незначительны.

Как следует из отчета[10], был определен приоритетный круг категорий операторов, охватывающий основные сферы жизнедеятельности, в рамках которых осуществляется обработка персональных данных значительного числа российских граждан. Сюда вошли в том числе рекрутинговые агентства, организации, оказывающие услуги в сфере страхования, гостиничного бизнеса, туризма, электронной дистанционной торговли, в сфере бронирования билетов в рамках осуществления пассажирских перевозок; кредитные организации, дилерские центры, отдельные крупные операторы[11]. По результатам плановых проверок было выявлено 2 134 нарушения обязательных требований законодательства в области персональных данных, которые сводятся в основном: 1) к представлению уведомления об обработке персональных данных, содержащего неполные и (или) недостоверные сведения; 2) к несоответствию содержания письменного согласия субъекта персональных данных на обработку персональных данных требованиям законодательства; 3) к отсутствию в поручении лицу, которому оператором поручается обработка персональных данных, обязанности соблюдения конфиденциальности персональных данных и обеспечения их безопасности, а также требований к защите обрабатываемых персональных данных.

Данные группы правонарушений не являются значимыми для субъектов персональных данных. Гораздо более существенные нарушения прав субъектов персональных данных происходят в Интернете, при этом Роскомнадзор далеко не всегда может воздействовать на нарушителя, особенно когда интернет-сайты зарегистрированы за пределами России. Неудачность таких попыток наглядно видна в случае с Telegram. По состоянию на 3 мая 2018 года Роскомнадзор заблокировал 50 VPN-сервисов и анонимайзеров, через которые можно было получить доступ к Telegram, за обеспечение доступа к последнему. Однако, как известно, принятые меры не привели к блокировке Telegram. Неэффективность применяемых методов сказывается и на защите персональных данных. Очевидно, что нуждается в модернизации организация контрольной деятельности по защите персональных данных, активизация использования новых технологий обработки информации.

[10] [Электронный ресурс]: // URL: http://pd.rkn.gov.ru/press-service/subject4/news4210/ (дата обращения: 01.08.2018)

[11] Там же.

Правоприменительная практика свидетельствует, что существуют особенности защиты персональных данных несовершеннолетних, в том числе их биометрических персональных данных. При проведении контроля обработки персональных данных несовершеннолетних встают проблемы, на которые нет однозначного ответа. Целесообразно остановиться на этом подробнее, рассмотрев проблему согласия субъекта персональных данных на их обработку, в том числе несовершеннолетних, подходы контролирующего органа к этому вопросу и правоприменительную практику.

Руководство Роскомнадзора обращает внимание на тот факт, что в стране имеется большое количество сайтов, распространяющих персональные данные детей и их родителей в открытом доступе[12]. Как правило, сайты принадлежат школам, детским садам, интернатам, а также муниципальным образованиям и администрациям ряда субъектов федерации. При этом, по информации Роскомнадзора, были размещены не только персональные данные самих несовершеннолетних, но и сведения о социальном статусе родителей и их принадлежности к той или иной льготной категории граждан. Безусловно, такой подход недопустим, если не было получено прямого и однозначного согласия субъекта персональных данных. Однако и с позицией Роскомнадзора трудно согласиться. Согласно указанной позиции «в случае, когда данные собираются для информирования родителей, выкладывание данных о детях в Сети будет превышать цель обработки, ради которой эти данные были собраны, даже при наличии отдельного согласия родителей на такую обработку»[13].

Несоответствие законодательству о персональных данных в данном случае обусловлено избыточностью выбранного способа обработки данных по отношению к заявленным целям обработки персональных данных. При этом контролирующий орган ссылается на «ключевой принцип законодательства в области персональных данных, в том числе международного права, — принцип, по которому «обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных»[14]. Все верно, но тогда встает вопрос: а как быть с не менее ключевым принципом согласия на обработку персональных данных, данным своей волей и в своем интересе? Или существует приоритет принципов и согласие субъекта персональных данных можно не принимать во внимание? Ответ кроется в формальном подходе контролирующего органа, не учитывающего того, что согласно ст. 2 ФЗ № 152-ФЗ целью закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональ-

[12] Там же.

[13] Там же.

[14] Там же.

ных данных. Полагаем, что при наличии осознанного, данного своей волей и в своем интересе согласия на обработку персональных данных права и свободы субъекта персональных данных не нарушаются.

Важно обратить внимание на аргументы контролирующего органа: оператор, выложив персональные данные граждан в глобальную сеть Интернет, которые он собрал в определенных целях, уже не сможет контролировать и обеспечить обещанные субъекту данных условия обработки[15]. Это действительно так, но эта ситуация касается любых субъектов персональных данных, а не только несовершеннолетних. В связи с этим возникает глобальный вопрос: каков правовой режим персональных данных, размещенных в сети Интернет, прежде всего в социальных сетях? Они становятся открытыми и общедоступными или сохраняют режим конфиденциальности? Однозначного ответа на этот вопрос снова нет.

Социальные сети в большинстве случаев являются тематическими: по профессиональному признаку, месту обучения, интересам и т.д. В зависимости от этого меняется и перечень персональных данных, которые пользователь социальной сети размещает в ней. Так, в профиле пользователя социальной сети «ВКонтакте» пользователю предлагается указать: пол, возраст, фамилию, имя, отчество, место жительства, место учебы, факультет, специальность, место работы, данные о родственниках пользователя и т.д. Необходимо отметить, что данная информация публикуется пользователями добровольно и достоверность публикуемых данных не проверяется. Что касается несовершеннолетних, то они сами охотно делятся информацией о себе и своих близких, не задумываясь о последствиях, но это вопрос не права, а правовой грамотности. Многие социальные сети открыто собирают важные сведения о пользователях. В анкетах есть вопросы о возрасте, роде занятий, об увлечениях и о прошлом — обо всем том, что идентифицирует человека как личность. Размещенная в социальных сетях информация становится доступной широкому кругу лиц.

Социальные сети активно используются и государственными органами, в том числе для поиска лиц по их персональным данным. Существуют Методические рекомендации по использованию сети Интернет в целях поиска информации о должниках и их имуществе, подготовленные Федеральной службой судебных приставов (от 30.11.2010 № 02-7 (в ред. письма ФССП от 16.03.2011 № 12/02-5588-ап))[16]. Подготовлены настольные книги для судебных приставов, описывающие последовательность действий в социальных сетях[17].

---

[15] Там же.

[16] Бюллетень Федеральной службы судебных приставов. 2011. № 1.

[17] См., напр.: Настольная книга судебного пристава-исполнителя/ под ред. В.А. Гуреева. М.: Статут, 2011.

Объектами поиска в целях исполнения требований исполнительных документов являются должники-граждане и должники-организации. Первоначальный поиск сведений о должниках рекомендуется осуществлять в поисковых системах (например, yandex.ru, google.ru, bing.com, yahoo.com, rambler.ru, metabot.ru, search.com); в каталогах (например, yaca.yandex.ru, list.mail.ru, vsego.ru); на сайтах социальных сетей, в которых необходимая информация может содержаться не только на персональных страницах граждан, но и на интернет-страницах социальных сетей, объединяющих пользователей — работников организаций — в группы (например, odnoklassniki.ru, vkontakte.ru, facebook.com, linkedin.com и др.); в блогах, которые могут быть личными, групповыми/корпоративными, общественными, тематическими или общими (например, livejournal.com, my.ya.ru, twitter.com, li.ru, blogs.mail.ru, diary.ru); в базах данных адресов и телефонов (например, 09service.com, nomer.org, lookup.com); на электронных досках объявлений о покупке / продаже имущества; в открытых базах данных государственных и коммерческих организаций; на сайтах новостей, где содержится информация о фамилиях граждан и наименованиях организаций, участвующих в тех или иных событиях.

Судебными приставами проводится изучение содержимого Интернет-страниц, что нередко позволяет установить местонахождение как должника, так и его имущества. Анализ контактов (родственники, коллеги, партнеры, друзья), фотографий (места фотографирования, окружающий интерьер, комментарии к фотографиям), выставленных должниками-гражданами на Интернет-страницах, позволяет судебному приставу установить как имущество должника, так и его местонахождение.

Рекомендуется активно использовать информацию, получаемую от интернет-провайдеров (наличие договора о доступе в сеть Интернет, IP-адрес, место установки конечного оборудования (компьютера), что позволит установить возможное место жительства должника и местонахождение принадлежащего ему имущества). Право получать при совершении исполнительных действий необходимую информацию, в том числе персональные данные, дано судебным приставам в соответствии со ст. 12 Федерального закона от 21.07.1997 № 118-ФЗ «О судебный приставах»[18]. При обнаружении должника судебный пристав входит с ним в контакт также с использованием социальных сетей и информирует его о возбуждении исполнительного производства с целью оплаты задолженности.

Общаясь в социальных сетях («Одноклассники», «ВКонтакте» и др.), должники регистрируются в качестве пользователей, при этом оставляют свои анкетные данные (сведения о месте жительства, месте работы, семей-

[18] СЗ РФ. 1997. № 30. Ст. 3590.

ном положении, увлечениях). Данная информация может быть использована судебными приставами для установления места жительства, места работы должника. Информация об увлечениях должника поможет определить круг органов и организаций, которые могут поставить информацию об имущественном положении должника.

В книге М.Т. Саблина[19] приводится пример, когда должника находят через социальные сети, где был зарегистрирован ребенок должника и указан номер школы. В дальнейшем в школе, где обучался ребенок, были получены сведения о фактическом месте жительства его родителей и номера их телефонов. Автор характеризует такой способ (через образовательное учреждение, в котором обучаются несовершеннолетние дети) перспективным. Вместе с тем предлагаемый подход с использованием несовершеннолетнего вряд ли отвечает моральным критериям.

Разумеется, должники нарушают закон, они подлежат розыску, принудительному исполнению решения суда, но насколько соответствует закону такое поведение должностного лица, наделенного официальными полномочиями, когда он получает информацию персонального характера обманным путем, выдавая себя за другую личность и используя неопытность несовершеннолетнего, с непредсказуемыми для последнего последствиями и психологическими травмами? Вероятно, в данном случае цель не может оправдывать средства.

Утечки персональных данных в Интернете имеют место практически во всех странах, и Россия не является исключением. Ежегодно происходят «громкие» утечки в российском сегменте Интернета. Но, пожалуй, не это главное. Принципиально важным, на наш взгляд, является различный подход к государственным и негосударственным структурам в вопросе зашиты персональных данных. Так, при утечке конфиденциальной информации о клиентах Пенсионного фонда России, которая содержала полные имена и фамилии клиентов Фонда, их идентификационные номера налогоплательщика (ИНН), данные о размере страховой и накопительной частей пенсии, а также сумму взносов в фонды обязательного медицинского страхования, представители Фонда заявили, что скомпрометированные данные не являются персональными, потому что по ним нельзя идентифицировать человека. Встает вопрос: если такие данные не защищаются государственными органами и не являются персональными данными, то что же тогда подлежит защите? И если данная информация является открытой, то на каких основаниях аналогичную информацию отказываются сообщать другим заинтересованным лицам?

[19] *Саблин М.Т.* Взыскание долгов: от профилактики до принуждения: практическое руководство по управлению дебиторской задолженностью. М., 2011 // СПС КонсультантПлюс.

Возвращаясь к образовательным учреждениям, следует обратить внимание на еще одну опасность, которую выявил Роскомнадзор. При проверках было установлено, что в ряде случаев услуги хостинга сайтам образовательных учреждений, на которых были размещены персональные данные детей, предоставлялись иностранными компаниями, расположенными на территории США, Британских Виргинских островов, которые не являются участниками Конвенции Совета Европы в сфере защиты персональных данных (1981) и не обеспечивают адекватной защиты прав субъектов персональных данных[20]. Такая ситуация имеет место не только в отношении образовательных учреждений. Однако этот вопрос уже решен: еще с сентября 2016 года операторы обязаны хранить и обрабатывать данные российских граждан на территории России.

В выступлениях руководителей Роскомнадзора подчеркивается, что «распространение личной информации не только нарушает требование законодательства в области персональных данных, но также может повлечь за собой неблагоприятные последствия для детей и их родителей»[21]. Здесь отчетливо просматривается позиция Роскомнадзора, которая не вполне соответствует действующему законодательству. Принципиальный момент — кто распространяет личную информацию. Если это сам субъект персональных данных, совершеннолетний и дееспособный, или оператор, которому своей волей и в своем интересе дано согласие на обработку, то почему их действия будут рассматриваться как нарушение требований законодательства? Законодательство устанавливает требования в целях защиты прав субъектов персональных данных. Если сам субъект дал согласие на обработку своих персональных данных, то их обработка в пределах данного согласия не может быть незаконной. Что касается «неблагоприятных последствий для детей и их родителей», то такая вероятность существует в отношении каждого, кто пользуется Интернетом. Снизить риск нарушения прав субъектов персональных данных — это задача контролирующих органов (соблюдая при этом законные интересы субъектов).

Недавно по целому ряду регионов России прошли проверки Роскомнадзором детских учебных заведений на предмет соблюдения законодательства о персональных данных в отношении учеников в рамках оказания услуг учета и организации питания в общеобразовательных организациях, результаты которых вскрыли пробелы в действующем законодательстве, а также весьма спорную позицию Роскомнадзора.

---

[20] [Электронный ресурс]: // URL: http://pd.rkn.gov.ru/press-service/subject4/news4210/ (дата обращения: 01.08.2018)

[21] Там же.

Суть проблемы сводилась к следующему. В целом ряде школ внедряется система «Ладошки», которая активно используется школой, обучающимися и их законными представителями (исключительно с их согласия). С использованием системы «Ладошки» осуществляются организация и информационное взаимодействие со школой, производственными подразделениями, получателями услуг питания и их законными представителями, учет производственных и коммерческих операций в процессе оказания услуг, сбор платы за питание. За счет «обратной связи» с родителями, обеспечиваемой системой «Ладошки» (индивидуальный отчет о питании и списании денежных средств), усилен родительский контроль над питанием детей. Вместе с тем данная практика была признана контролирующими органами противоречащей ФЗ № 152-ФЗ (обработка биометрической информации в рамках оказания услуг учета и организации питания в общеобразовательных организациях, изначально не предполагающих сбор биометрических персональных данных, отсутствие согласия несовершеннолетнего, обработка, выходящая за пределы целей образовательного учреждения).

Как излагают свою позицию должностные лица Роскомнадзора, она сводится к анализу целеполагания и правовых оснований обработки биометрических персональных данных несовершеннолетних. Кроме того, по мнению руководства данного ведомства, положения ч. 1 ст. 11 ФЗ № 152-ФЗ[22] не подлежат расширительному толкованию и не предусматривают возможности получения согласия на обработку биометрических персональных данных от законного представителя субъекта персональных данных. Действующим законодательством не регламентирован порядок оказания услуг учета и организации питания в общеобразовательных организациях с применением систем идентификации биометрических данных несовершеннолетних. В связи с этим, по мнению уполномоченного органа, указанная обработка биометрических персональных данных будет противоречить требованиям федерального законодательства в области персональных данных[23].

С такой позицией трудно согласиться. В проекте «Ладошки» применяется технология PalmSecure компании Fujitsu. Указанная технология основана на бесконтактном васкулярном методе аутентификации, подразумевающем обработку фотоизображения рисунка вен ладони, полученного в диапазоне, близком к инфракрасному. Сведения об особенностях рисунка вен ладони, подлежащие обработке при осуществлении проекта «Ладошки», относятся

[22] Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных, могут обрабатываться только при письменном согласии субъекта персональных данных.

[23] [Электронный ресурс]: // URL: http://pd.rkn.gov.ru/press-service/subject4/news4210/ (дата обращения: 01.08.2018)

к биометрическим персональным данным. В то же время сведения об особенностях рисунка вен ладони руки человека, позволяющие установить его личность, нельзя квалифицировать в качестве дактилоскопической информации. Информация об особенностях рисунка вен ладони не содержит сведений об особенностях папиллярного узора ладони и поэтому дактилоскопической информацией не является. В связи с этим обработка сведений об особенностях рисунка вен ладони руки человека не подпадает под действие Закона о государственной дактилоскопической регистрации.

Следует также обратить внимание на то, что Закон о государственной дактилоскопической регистрации регламентирует исключительно государственную дактилоскопическую регистрацию, т.е. деятельность, осуществляемую органами исполнительной власти и федеральными государственными учреждениями по получению, учету, хранению, классификации и выдаче дактилоскопической информации, установлению или подтверждению личности человека.

Обработка биометрических персональных данных установлена ст. 11 ФЗ № 152-ФЗ. В этой статье установлены две особенности обработки биометрических персональных данных по сравнению с общим порядком обработки персональных данных. Одна из этих особенностей состоит в том, что в случаях, предусмотренных в ч. 2 ст. 11 ФЗ № 152-ФЗ, обработка биометрических персональных данных может осуществляться без согласия субъекта персональных данных, тогда как по общему правилу обработка персональных данных без получения согласия субъекта персональных данных допускается только при определенных условиях. Другая особенность обработки биометрических персональных данных, предусмотренная в ст. 11, заключается в требовании выражения согласия на обработку биометрических персональных данных исключительно в письменной форме, если их обработка может осуществляться только с согласия субъекта персональных данных. Ни в какую другую форму, кроме письменной, согласие на обработку биометрических персональных данных не может быть облечено. Иных, помимо указанных выше, особенностей, связанных с обработкой биометрических персональных данных, в ч. 1 ст. 11 ФЗ № 152-ФЗ не установлено.

Указывая в ч. 4 ст. 9 и ч. 1 ст. 11 ФЗ № 152-ФЗ на согласие в обязательной письменной форме субъекта персональных данных, законодатель охватывает ситуацию, когда субъект персональных данных дееспособен и может выразить согласие на обработку биометрических персональных данных в письменной форме сам или посредством своего представителя (с соответствующим полномочием, предоставленным ему дееспособным субъектом персональных данных), а также ситуацию, когда субъект персональных данных является несовершеннолетним или признан в установленном порядке

недееспособным, вследствие чего согласие на обработку его биометрических персональных данных в письменной форме выражается от имени субъекта персональных данных его законным представителем.

Несовершеннолетние и лица, признанные в установленном порядке недееспособными, не могут сами дать согласие на обработку своих персональных данных, в том числе биометрических персональных данных. В результате применения ч. 1 ст. 11 ФЗ № 152-ФЗ в истолковании рассматриваемой нормы контролирующим органом, указанные категории физических лиц оказались лишены права быть представленными в соответствующих отношениях своими законными представителями, т.е. ограничены в осуществлении своих гражданских прав и устранены от участия в значительном сегменте общественных отношений.

Одновременно нарушаются и права родителей несовершеннолетних. Так, предусмотренная проектом «Ладошки» обработка биометрических персональных данных школьников, как было сказано, направлена на организацию безналичной оплаты питания школьников и контроля посещаемости ими школ, следовательно, на обеспечение здорового развития детей, получения ими образования и их безопасности. Забота о детях — конституционное право и одновременно конституционная обязанность родителей (ч. 2 ст. 38 Конституции Российской Федерации). Родители несут ответственность за воспитание и развитие своих детей (п. 1 ст. 63 Семейного кодекса). Исключение на практике, вопреки смыслу ч. 1 ст. 11 ФЗ № 152-ФЗ, подлежащей применению в ее системной связи с положениями ст. 6 и 9 названного Закона и общеправовым институтом законного представительства, возможности обработки биометрических персональных данных ребенка, не отвечает приведенным положениям Конституции России, целям государственной политики в отношениях детей и целям ФЗ № 152-ФЗ.

Иными словами, позиция, в соответствии с которой на основании ч. 1 ст. 11 ФЗ № 152-ФЗ только сам субъект персональных данных может дать согласие на обработку его биометрических персональных данных, вследствие чего согласие его представителя, включая законного представителя несовершеннолетнего или недееспособного лица, на обработку указанных персональных данных юридического значения не имеет, является ошибочной. Она вызвана вычленением текста рассматриваемой нормы и из системы норм соответствующего законодательного акта, и из правовой системы в целом, прочтением правового предписания ч. 1 ст. 11 ФЗ № 152-ФЗ изолированно, вне его связей и необходимости совместного применения с другими нормами права.

Выражение законным представителем согласия в письменной форме на обработку биометрических персональных данных от имени представляемо-

го означает наличие согласия субъекта персональных данных в письменной форме на обработку его биометрических персональных данных, которое необходимо в соответствии с ч. 1 ст. 11 ФЗ № 152-ФЗ[24]. Тем не менее, некоторая правовая неопределенность все же сохраняется. Чтобы устранить ее, в 2018 году разработан проект федерального закона «О внесении изменений в Федеральный закон «О персональных данных», согласно которому согласие на обработку персональных данных недееспособного либо несовершеннолетнего субъекта персональных данных дает законный представитель субъекта персональных данных. Предлагается также установить особенности регулирования в отношении лиц, достигших 14 лет, и осуществляющих трудовую деятельность. Эти несовершеннолетние будут вправе давать согласие на обработку своих персональных данных самостоятельно, если обработка таких персональных данных осуществляется в связи с трудовой деятельностью субъектов персональных данных.

Решит ли данный законопроект проблему? Отчасти, да. Но другая составляющая проблемы — позиция контролирующих органов, согласно которой «в случае, когда данные собираются для информирования родителей, выкладывание данных о детях в Сети не будет соотноситься с целью обработки, ради которой эти данные собирались, даже при наличии отдельного согласия родителей на такую обработку»[25], и, соответственно, рассматривается как нарушение законодательства о персональных данных. Иными словами, мы будем защищать ваши персональные данные, даже если вы этого не хотите.

Формулируя данную позицию, контролирующий орган приходит к следующему выводу, положенному в основу контрольной деятельности: «лишь обработка персональных данных детей в виде предоставления доступа ограниченному кругу лиц будет соответствовать целям образовательной деятельности»[26]. Исходя из такой позиции, даже указание победителей олимпиад, имена медалистов сможет узнать лишь «ограниченный круг лиц». Иными словами, информация, представляющая собой гордость обучающихся, их родителей, учителей и школы в целом, — это информация ограниченного доступа.

---

[24] За рубежом единого подхода к обработке биометрических персональных данных в сходных случаях не выработано. Так, во Франции не дают разрешения на обработку отпечатков пальцев для доступа в школьную столовую, в то время как признана допустимой обработка геометрии рук для этих целей. Для этих же целей в Великобритании допустимо использовать отпечатки пальцев (см. Cnil Annual Report. Avaolable at: https://www.cnil.fr/sites/default/files/typo/document/CNIL-AnnualReport-2008.pdf (дата обращения: 01.08.2018); *Zorkadis V., Donos P.* On biometricsbased authentication and identification from a privacyprotection perspective // Information Management & Computer Security. 2004. Vol. 1. P. 132–133.

[25] [Электронный ресурс]: // URL: http://d-russia.ru/personalnye-dannye-nedetskie-problemy.html (дата обращения: 01.08.2018)

[26] Там же.

Применительно к получению согласия субъекта персональных данных на обработку его персональных данных в правоприменительной практике имеется еще один аспект. Установлено, что субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным. Однако контрольные мероприятия, проводимые Роскомнадзором, не позволяют установить характера данного согласия: было ли оно конкретным, информированным и сознательным. В значительном числе случаев лицо либо должно согласиться на обработку своих персональных данных, либо отказаться от необходимой ему услуги. Анализ судебной практики свидетельствует, что по указанным вопросам чаще дает предписания об устранении нарушения законодательства о персональных данных антимонопольный орган.

Показательным является Постановление Арбитражного суда Северо-Западного округа от 02.04.2018 № Ф07-16307/2017 по делу № А44-745/2017, которым было оспорено предписание антимонопольного органа, выявившего в ходе проверки факты включения страховым обществом в договоры страхования условий, ущемляющих права потребителей, в том числе в части обработки персональных данных. Суды согласились с позицией антимонопольного органа, который указал, что спорные условия изложены таким образом, что у потребителя отсутствует возможность выражения согласия или отказа от обработки персональных сведений.

В заключение полагаем целесообразным привести выдержку из Регламента № 2016/679 Европейского парламента и Совета Евросоюза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС («Общий Регламент о защите персональных данных», принятый в Брюсселе 27.04.2016): «Право на защиту персональных данных не является абсолютным правом, его необходимо рассматривать относительно его функции в обществе, оно должно быть уравнено с другими основными правами в соответствии с принципом пропорциональности»[27]. Восприятие такого подхода позволит реализовать предусмотренные программой «Цифровая экономика Российской Федерации» меры по обеспечению прав человека в цифровом мире, меры контроля обработки и доступа к персональным данным, в том числе в социальных сетях и прочих средствах социальной коммуникации, на основе баланса интересов.

[27] См.: Регламент № 2016/679 Европейского парламента и Совета Евроюза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС» // СПС Гарант.

## Библиография

Али М. Персональные данные: обязанности и ответственность оператора // ЭЖ-Юрист. 2017. № 12. С. 5–8.

Грибанов А.А. Общий регламент о защите персональных данных: идеи для совершенствования российского законодательства // Закон. 2018. № 3. С. 149–162.

Жердина С., Двенадцатова Т., Чмыхов В. Регламент ЕС о персональных данных // ЭЖ-Юрист. 2017. № 33. С. 8–13.

Камалова Г.Г. Биометрические персональные данные: определение и сущность // Информационное право. 2016. № 3. С. 8–12.

Михайлова И.А. Персональные данные и их правовая охрана: некоторые проблемы теории и практики // Законы России: опыт, анализ, практика. 2017. № 10. С. 11–18.

Наумов В.Б., Архипов В.В. Понятие персональных данных: интерпретация в условиях развития информационно-телекоммуникационных технологий // Российский юридический журнал. 2016. № 2. С. 186–196.

Настольная книга судебного пристава-исполнителя / под ред. В.А. Гуреева. М.: Статут, 2011. 888 с.

Постникова Е.В. Некоторые аспекты правового регулирования защиты персональных данных в рамках внутреннего рынка Европейского союза // Право. Журнал Высшей школы экономики. 2018. № 1. С. 234–254.

Проскурякова М.И. Конституционно-правовые основы защиты персональных данных в России и Германии в истолковании органов конституционного правосудия // Сравнительное конституционное обозрение. 2015. № 1. С. 29–44.

Право в сфере Интернета: сборник статей / отв. ред. М.А. Рожкова. М.: Статут, 2018. 528 с.

Савельев А.И. Направления регулирования Больших данных и защита неприкосновенности частной жизни в новых экономических реалиях // Закон. 2018. № 5. С. 122–144.

Савельев А.И. Научно-практический постатейный комментарий к Федеральному закону «О персональных данных». М.: Статут, 2017. 320 с.

Савельев А.И. Электронная коммерция в России и за рубежом: правовое регулирование. М.: Статут, 2016. 640 с.

Соколова О.С. Правовые позиции Конституционного Суда Российской Федерации в сфере персональных данных // Современное право. 2015. № 10. С. 88–93.

Zorkadis V., Donos P. On Biometrics-based Authentication and Identification from a Privacy-protection Perspective // Information Management & Computer Security. 2004. Vol. 1. P. 125–137.


## State Control in Personal Data Protection


### Lyudmila K. Tereschenko

Deputy Head, Department of Administrative Legislation and Procedure, Institute of Legislation and Comparative Legislation under the Government of the Russian Federation, Doctor of Juridical Sciences. Address: 21 Kolomenskaya Str., Moscow, 115142, Russian Federation. E-mail: ltereschenko@hse.ru

## Abstract

The article is devoted to the most topical problems arising while applying personal data legislation performing state control over observing requirements and the analysis of judicial practice including the protection of personal data of minors. The requirements regarding personal data protection are examined in terms of ensuring the balance of interests of personality, society and business organizations, which supposes the balance, relevance and feasibility of the requirements including the requirement to guarantee the adequate protection of personal data. Legal and technical requirements to protect personal data, the rights of legal persons and judicial interests of legal persons should be balanced and sufficient not to impede the development of market and to avoid the violation of the interests of the subjects of personal data. The author has shown that the measures of control usually target the observation of the data protection related to citizens, the observation of the information protection but not the observation of the rights of citizens while processing personal data. The paper examines the general tendencies in the development and improvement of state control. The paper concludes that it is necessary to update the organization of control activity related to the personal data protection, application of new technologies to process information. A special attention is given to the protection of personal data for minors, in particular their biometric personal data.

## Keywords

state control, personal data, right in privacy, limitation of rights, balance of interests, case practice, minors.

Citation: Tereschenko V.K. (2018) State Control in Personal Data Protection. *Pravo. Zhurnal Vysshey shkoly ekonomiki*, no 4, pp. 142–161 (in Russian)

DOI: 10.17323/2072-8166.2018.4.142.161

## References

Ali M. (2017) Personal'nye dannye: obyazannosti i otvetstvennost' operatora [Personal data: duties and responsibility]. *EZh-Yurist*, no 12, pp. 5–8.

Gribanov A.A. (2018) Obshchiy reglament o zashchite personal'nykh dannykh (General Data Protection Regulation): idei dlya sovershenstvovaniya rossiyskogo zakonodatel'stva [General data protection regulation: improving Russian legislation]. *Zakon*, no 3, pp. 149–162.

Gureev V.A. (ed.) (2011) *Nastol'naya kniga sudebnogo pristava-ispolnitelya* [Reference book of court enforcement officer]. Moscow: Statut, 210 p. (in Russian)

Kamalova G.G. (2016) Biometricheskie personal'nye dannye: opredelenie i sushchnost' [Biometric personal data: definition and essence]. *Informatsionnoe pravo*, no 3, pp. 8–12.

Mikhaylova I.A. (2017) Personal'nye dannye i ikh pravovaya okhrana: nekotorye problemy teorii i praktiki [Personal data: legal protection]. *Zakony Rossii: opyt, analiz, praktika*, no 10, pp. 11–18.

Naumov V.B., Arkhipov V.V. (2016) Ponyatie personal'nykh dannykh: interpretatsiya v usloviyakh razvitiya informatsionno-telekommunikatsionnykh tekhnologiy [Concept of personal data in the age of IT]. *Rossiyskiy yuridicheskiy zhurnal*, no 2, pp. 186–196.

Postnikova E.V. (2018) Nekotorye aspekty pravovogo regulirovaniya zashchity personal'nykh dannykh v ramkakh vnutrennego rynka Evropeyskogo soyuza [Aspects of legal regulation of personal data protection within the EU internal market]. *Pravo. Zhurnal Vysshey shkoly ekonomiki*, no 1, pp. 234–254.

Proskuryakova M.I. (2015) Konstitutsionno-pravovye osnovy zashchity personal'nykh dannykh v Rossii i Germanii v istolkovanii organov konstitutsionnogo pravosudiya [Constitutional basics of protecting personal data in Russia and Germany]. *Sravnitel'noe konstitutsionnoe obozrenie*, no 1, pp. 29–44.

Rozhkova M.A. (ed.) (2018) *Pravo v sfere Interneta* [Law in the sphere of the Internet]. Moscow: Statut, 528 p. (in Russian)

Savel'ev A.I. (2017) *Nauchno-prakticheskiy postateynyy kommentariy k Federal'nomu zakonu «O personal'nykh dannykh»* [Article-by-article commentary to the Federal Law On Personal Data]. Moscow: Statut, 320 p.

Saveliev A.I. (2018) Napravlenia regulirovania bolshih dannyh i zaschita neprikosnovennosti chastnoi zhizni v novyh ekonomicheskih realiah [Regulation of Big Data and Protection of Privacy Now]. *Zakon*, no 5, pp. 122–144.

Savel'ev A.I. (2016) *Elektronnaya kommertsiya v Rossii i za rubezhom: pravovoe regulirovanie* [Electronic commerce in Russia and abroad]. Moscow: Statut, 640 p. (in Russian)

Sokolova O.S. (2015) Pravovye pozitsii Konstitutsionnogo Suda Rossiyskoy Federatsii v sfere personal'nykh dannykh [Legal principles of Russian Constitutional Court in the sphere of personal data]. *Sovremennoe pravo*, no 10, pp. 88–93.

Zherdina S., Dvenadtsatova T., Chmykhov V. (2017) Reglament ES o personal'nykh dannyh [EU regulation on personal data]. *EZh-Yurist*, no 33, pp. 8–3.

Zorkadis V., Donos P. (2004) On biometrics-based authentication and identification from a privacy-protection perspective. *Information Management and Computer Security,* vol. 1, pp. 125–137.