Вестник РУДН. Серия: Юридические науки 2017 Т. 21. № 1. 136–152
RUDN JOURNAL OF LAW http://journals.rudn.ru/law

doi:10.22363/2313-2337-2017-21-1-136-152

ГОСУДАРСТВЕННЫЙ КОНТРОЛЬ (НАДЗОР) — ИНСТРУМЕНТ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННОЙ СФЕРЕ ИЛИ СРЕДСТВО ЗАЩИТЫ НЕПРИКОСНОВЕННОСТИ ЧАСТНОЙ ЖИЗНИ: СООТНОШЕНИЕ ЧАСТНОГО И ПУБЛИЧНОГО ИНТЕРЕСОВ

В.П. Иванский, Г.В. Мельничук

Российский университет дружбы народов
Юридический институт
ул. Миклухо-Маклая, 6, Москва, Россия, 117198

В статье рассматривается проблема соотношения двух основополагающих ценностей — правовой защиты публичного и частного интересов в сфере обработки компьютерных данных. С одной стороны, использование информационно-коммуникационных технологий может служить потенциальной площадкой для подготовки, организации и реализации преступлений, угрожающих безопасности государству, обществу и личности. С другой, эти технологии являются средством сбора, хранения, преобразования и распространения приватной информации о гражданах (персональных данных). При этом важно отметить, что в соответствии с ФЗ от 27.07.2006 № 152-ФЗ «О персональных данных» цель обработки персональных данных ограничена достижением заранее определенных и законных целей. Более того, Доктрина информационной безопасности РФ признает обеспечение и защиту неприкосновенности частной жизни при использовании информационных технологий *национальными интересами*. Тем не менее, наряду с обозначенными выше правовыми актами, направленными на защиту информации о частной жизни граждан, целью сбора, хранения и использования персональных данных согласно «закону Яровой» является противодействие терроризму и обеспечение общественной безопасности, то есть защита *публичного интереса*. Из сказанного вытекает, что законодательством регламентированы одновременно две взаимоисключающие друг друга цели обработки персональных данных. Между тем Роскомнадзор является уполномоченным федеральным органом исполнительной власти по защите прав субъектов персональных данных, осуществляющим функции государственного контроля (надзора) за соответствием требований законодательства РФ, в том числе в части определения цели обработки персональных данных. По причине того, что цели обработки персональных данных являются законными, но противоречащими друг другу, то Роскомнадзор вынужден нарушать принцип беспристрастности при осуществлении контроля (надзора), изначально отстаивая публичные интересы, тем самым ущемляя частные, состоящие в защите информационного аспекта неприкосновенности сферы частной жизни граждан. В связи с указанными выше обстоятельствами авторы статьи предлагают найти баланс соотношения частного и публичного интересов в формировании независимой от государства системы национальных органов по защите персональных данных на основе законодательного опыта индустриально-развитых государств.

Ключевые слова: государственный контроль; информационная сфера; неприкосновенность частной жизни; терроризм; персональные данные; информационная безопасность; национальный орган по защите персональных данных

I. АБРИС НАУЧНО-ПРАВОВЫХ ПРОБЛЕМ ИССЛЕДОВАНИЯ

Развитие личности, общества и государства в различные исторические периоды всегда проходило и проходит через стадию кризиса, проявляющегося в их разнообразных взаимодействиях в отношении определения демаркационной линии публичной и частной сфер. В условиях развития компьютерных и информационно-телекоммуникационных технологий нахождение границы частного и публичного интересов становится с каждым разом все более затруднительным, особенно в свете недавно принятых законодательных мер противодействия терроризму и обеспечения общественной безопасности. Между тем кризис выступает не только орудием расшатывания сложившейся системы ценностей, в которой пребывает общество и человек, но переломным моментом в осмыслении того огромного значения, которое несет в себе неприкосновенность частной жизни для развития правосознания человека.

В связи со сказанным имеются три пути выхода из кризиса: 1) перемещение государством прежде всего финансовых (материальных) ресурсов на укрепление и защиту сложившегося публичного правопорядка в информационной сфере; 2) направление материальных потоков на заимствование и внедрение исключительно ценностей (опыта) индустриально-развитых государств по расширению сферы частной жизни и ее правовой защиты при использовании информационно-коммуникационных технологий; 3) нахождение баланса между первым и вторым трендами. Возникает вопрос: какой концептуальный подход выхода из кризиса приемлем для российского государства?

Кроме того, следует сказать, что кризис, который охватил человека и общество (соответственно и государство), имеет качество системно-глобального [1. С. 44–52]. А это означает, что глобальный кризис затронул наиболее жизненно необходимые основы их существования — духовный мир, к которому следует отнести мировоззрение в самом широком смысле слова. При этом формирование конструктивного мировоззрения представляется возможным лишь в рамках эффективной защиты неприкосновенности частной жизни от разрушающей человеческую личность информации. Как раз право на невмешательство в частную жизнь обеспечивает возможность индивидууму оставаться наедине с самим собой — со своим «Я» для конституирования естественным для человеческой природы механизмом созидательного правосознания. По этой причине, изучая проблему соблюдения баланса между правовой защитой неприкосновенности частной жизни человека и обеспечением национальной безопасности в информационной сфере, следовало бы разобраться, какая информационная технология должна играть ключевую роль в формировании правосознания гражданина — органов публичной власти или врожденный самоорганизующий-

ся внутренний механизм человека? Иначе говоря, суть научно-правовой проблемы заключается в том, какая сфера — публичная или правовая — в большей степени отражает *национальный интерес* российского государства? И совпадают ли между собой публичный и национальный интересы?

Следующая научно-правовая проблема: можно ли оставлять инструмент контроля (надзора) в сфере обработки персональных данных, тем более в ситуации кризиса, лишь государственным органам, являющимся частью публичной администрации? И целесообразно ли передать осуществление функции государственного контроля (надзора) за соблюдением законности обработки персональных данных независимым от государства организациям?

II. ИЗЛОЖЕНИЕ ОСНОВНОГО МАТЕРИАЛА

Трансформационные процессы в российском обществе, начавшиеся еще в конце 80-х гг. XX в., связаны с наступлением информационно-сетевой эпохи и началом процесса глобализации [2. С. 73–78]. В последние годы обеспечение информационной безопасности государств (в том числе меры, принятые по противодействию экстремизма и терроризма) занимает одно из актуальнейших направлений научных исследований в юриспруденции [3; 4; 5. С. 43–66]. Это связано с повышенной террористической активностью, вызванной сменой государственно-политических режимов стран Северной Африки и Ближнего Востока. По этой причине в июле 2016 г. был принят антитеррористический «пакет (закон) Яровой» (названный так в СМИ и общественных дискуссиях в честь одного из его авторов — Ирины Яровой), состоящего из следующих федеральных законов:

1) Федеральный закон от 6 июля 2016 г. № 374-ФЗ «О внесении изменений в Федеральный закон “О противодействии терроризму” и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности»[1] (далее по тексту — «закон (пакет) Яровой»);

2) Федеральный закон от 6 июля 2016 г. № 375-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности»[2].

[1] Федеральный закон от 06 июля 2016 г. № 374-ФЗ «О внесении изменений в Федеральный закон “О противодействии терроризму” и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» // Собрание законодательства РФ. 11.07.2016. № 28. Ст. 4558.

[2] Федеральный закон от 06.07.2016 № 375-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» // Собрание законодательства РФ. 11.07.2016. № 28. Ст. 4559.

5 декабря 2016 г. Указом Президента РФ № 646 была утверждена «Доктрина информационной безопасности Российской Федерации»[3] (далее по тексту — Доктрина информационной безопасности № 646), раскрывающая официальные взгляды на обеспечение национальной безопасности в информационной сфере. Заслуживает также внимания проект Постановления Правительства РФ «Об утверждении Положения о государственном контроле и надзоре за соответствием обработки персональных данных требованиям законодательства РФ», регулирующий порядок проведения государственного контроля в сфере обработки персональных данных[4] (далее по тексту — Положение о госконтроле).

Рассмотрим указанные выше правовые акты через призму осуществления государственного контроля (надзора) в информационной сфере за соблюдением баланса между неприкосновенностью частной жизни человека и защитой интересов общества и государства.

Нормативным документом, раскрывающим Стратегию национальной безопасности Российской Федерации в информационной сфере, является Доктрина информационной безопасности № 646[5], нормы которой должны приниматься во внимание при принятии законодательства в этой области в части соотношения публичных и частных интересов. Между тем информационная Доктрина регулирует *наиболее жизненно важные* общественные отношения, касающиеся стратегических целей и основных направлений обеспечения информационной безопасности государства (п. 3 Указа).

В связи с исключительной важностью указанных правовых отношений в современную эпоху считаем целесообразным пересмотреть уровень их регламентации — с подзаконного нормотворчества на уровень законотворчества. В этом случае нам удастся избежать коллизии в понимании приоритета целей обработки персональной информации — защита *публичных интересов* или защита неприкосновенности частной жизни в качестве *национального интереса.*

Другим нормативным правовым актом, устанавливающим дополнительные меры противодействия терроризму и обеспечения общественной безопасности в информационной сфере, является антитеррористический «закон Яровой». Основными его целями выступают: во-первых, расширение полномочий правоохранительных органов; во-вторых, новые требования к операторам связи и интернет-проектам; в-третьих, усиление регулирования религиозно-

[3] Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства РФ. 12.12.2016. № 50. Ст. 7074.

[4] Проект Постановления Правительства РФ «Об утверждении Положения о государственном контроле и надзоре за соответствием обработки персональных данных требованиям Федерального закона «О персональных данных» (подготовлен Роскомнадзором). Режим доступа: http://www.economy.gov.ru/. Дата обращения: 03.0.2017.

[5] См. п. 3 Указа Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства РФ. 12.12.2016. № 50. Ст. 7074.

миссионерской деятельности [6. С. 15–18]. В рамках заявленной темы статьи следовало бы коснуться лишь обязанностей операторов и организаторов распространения информации в сети «Интернет» в соответствии с Федеральным законом от 6 июля 2016 г. № 374-ФЗ. Статьи 15 и 64 данного Закона возлагают на операторов связи и организаторов распространения информации в сети «Интернет» обязанности хранения на территории РФ с 1 июля 2018 г. текстовые сообщения пользователей услугами связи, голосовую информацию, изображения, звуки, видео-, иные сообщения пользователей. Срок такого хранения может составлять до шести месяцев с момента окончания их приема, передачи, доставки или обработки. Информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, текстовых сообщений, изображений, звуков, видео- или иных сообщений пользователей услугами связи операторы связи обязаны хранить в течение трех лет, а организаторы распространения информации в сети «Интернет» — в течение одного года с момента окончания осуществления таких действий.

Помимо хранения такой информации операторами связи и организаторами распространения информации в сети «Интернет» последние обязаны предоставлять указанную информацию уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность или обеспечение безопасности РФ. Указанные положения, по нашему мнению, противоречат пп. «а» п. 8 Доктрины информационной безопасности РФ от 05.12.2016 № 646[6], где обеспечение и защита неприкосновенности частной жизни как конституционного права выступают *национальными интересами* в информационной сфере, а также пп. 1 п. 1 ст. 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»[7] (далее по тексту — ФЗ № 152) в части получения согласия на обработку персональных данных. Иначе говоря, национальными интересами в информационной сфере являются не противодействие терроризму и обеспечение общественной безопасности, а защита неприкосновенности информационного аспекта сферы частной жизни граждан. Между тем террористические и экстремистские организации широко используют механизмы деструктивного информационного воздействия на сознание человека и общества в целях нанесения ущерба объектам критической информационной инфраструктуры (п. 13 Доктрины). В связи с этим необходим баланс между потребностью граждан в свободном обмене информацией и ограничениями, связанными с обеспечением национальной безопасностью (пп. «в» п. 34 Доктрины).

---

[6] См.: пп. «а» п. 8 Указа Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства РФ. 12.12.2016. № 50. Ст. 7074.

[7] Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 03.07.2016) «О персональных данных» // Собрание законодательства РФ. 31.07.2006. № 31 (1 ч.). Ст. 3451.

Исходя из сказанного, вытекает, что «закон Яровой» защищает *публичный интерес*, не соответствующий *национальному интересу*, отраженному в требованиях ФЗ № 152 и предписаниях Стратегии информационной Доктрины и представляющий собой защиту неприкосновенности частной жизни личности [7. С. 112–117]. Возникает следующий вопрос: какой государственный орган или организация возьмет на себя функцию соблюдения данного баланса посредством осуществления контроля (надзора) и как обеспечить механизм такого баланса интересов?

В настоящее время органом исполнительной власти, осуществляющим государственный контроль и надзор в информационной сфере, является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). В рамках изучения вышеобозначенной проблемы следовало бы сделать научный срез прежде всего не на действующем Положении о Роскомнадзоре, утвержденном Постановлением Правительства РФ 16.03.2009 г. № 228[8] (далее по тексту — Положение о Роскомнадзора № 228 от 16.03.2009), в котором отсутствует регламентированный порядок проведения госконтроля в сфере обработки персональных данных, а на проекте Положения о государственном контроле и надзоре за соответствием обработки персональных данных требованиям Федерального закона «О персональных данных»[9]. Согласно п. 1 раздела I Положения о Роскомнадзоре № 228 от 16.03.2009 Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций осуществляет функции по контролю и надзору за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных. Кроме того, Роскомнадзор является уполномоченным федеральным органом исполнительной власти по защите прав субъектов персональных данных. Продолжим обсуждение указанной выше проблемы коллизии нормативных правовых актов — Указа Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» и Федерального закона от 6 июля 2016 г. № 374-ФЗ «О внесении изменений в Федеральный закон “О противодействии терроризму” и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» в русле анализа полномочий Роскомнадзора.

---

[8] Постановление Правительства РФ от 16.03.2009 № 228 (ред. от 01.07.2016) «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций» (вместе с «Положением о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций») // Собрание законодательства РФ. 23.03.2009. № 12. Ст. 1431.

[9] Проект Постановления Правительства РФ «Об утверждении Положения о государственном контроле и надзоре за соответствием обработки персональных данных требованиям Федерального закона «О персональных данных» (подготовлен Роскомнадзором). Режим доступа: http://www.economy.gov.ru/. Дата обращения: 03.01.2017.

С точки зрения подхода российской правовой доктрины закон обладает высшей юридической силой по сравнению с Указом Президента РФ. Тем не менее, Указ Президента РФ от 05.12.2016 № 646 регулирует наиболее жизненно важные общественные отношения в сфере информационной безопасности нашего государства, в том числе обеспечение и защита неприкосновенности частной жизни в информационной сфере. Одним из полномочий Роскомнадзора является осуществление государственного контроля и надзора за соответствием обработки персональных данных требованиям законодательства РФ в области персональных данных (п. 5.1.1.4 Положения Роскомнадзора № 228 от 16.03.2009). Из последнего нормативного положения возникает следующий вопрос: как следует трактовать понятие «законодательство» − в широком (включает законы и подзаконные акты) или узком значении (только законы)?

Согласно статье 4 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» законодательство РФ в области персональных данных основывается на Конституции Российской Федерации и международных договорах Российской Федерации и состоит из настоящего Федерального закона и других определяющих случаи и особенности обработки персональных данных федеральных законов[10]. Следовательно, в Положении о Роскомнадзоре № 228 от 16.03.2009 законодательство понимается исключительно в узком понимании своего значения. Тогда Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций обязана руководствоваться Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и Федеральным законом от 6 июля 2016 г № 374-ФЗ. Между тем в ст. 2 ФЗ № 152 говорится о цели данного закона — это обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе *защиты прав на неприкосновенность частной жизни*. Согласно статьям 15 и 64 ФЗ № 374 операторы связи и организаторы распространения информации в сети «Интернет» обязаны *без согласия* субъекта персональных данных хранить перечисленную выше информацию. Тем не менее, ч. 1 ст. 24 Конституции РФ от 12.12.1993 гласит, что сбор, хранение, использование и распространение информации о частной жизни лица *без его согласия* не допускаются [8]. Помимо нарушения условий обработки персональных данных (ст. 6 ФЗ № 152 — требуется также согласие), цели обработки персональных данных, в том числе их хранение, трактуются указанными законами по-разному: согласно ФЗ № 152 — обеспечение защиты права человека на неприкосновенность частной жизни, а ФЗ № 374 — противодействие терроризму и обеспечение общественной безопасности. Другими словами, обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей: для ФЗ № 152 такой целью является защита частного интереса, а для ФЗ № 374

[10] Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 03.07.2016) «О персональных данных» // Собрание законодательства РФ. 31.07.2006. № 31 (1 ч.). Ст. 3451.

— это защита публичного интереса. Наряду с анализируемыми законами, как было сказано выше, следует обязательно учитывать информационную Доктрину РФ № 646, в которой обеспечение и защита неприкосновенности частной жизни объявлены национальными интересами. Теперь снова вернемся к государственному контролю (надзору) в части его осуществления за соответствием обработки персональных данных требованиям ФЗ № 152 и ФЗ № 374 с учетом изложенных выше положений информационной Доктрины РФ. Так, в соответствии с п. 9 упомянутого выше проекта Положения о государственном контроле и надзоре за соответствием обработки персональных данных требованиям Федерального закона «О персональных данных» должностные лица Роскомнадзора, получив доступ к информационным системам персональных данных, оценивают законность деятельности по обработке на предмет их соответствия *целям* их обработки[11]. Если одновременно действуют нормы ФЗ № 374 и ФЗ № 152, а также предписания информационной Доктрины РФ № 646, цели которых противоположны друг другу, то какими правовыми актами следует руководствоваться Роскомнадзору в осуществлении государственного контроля (надзора) − ФЗ № 152 или ФЗ № 374?

Иначе говоря, какую позицию выберет уполномоченный федеральный орган исполнительной власти по защите персональных данных (Роскомнадзор) — защита публичного или частного интересов, общества или конкретного человека? Ответ очевиден — Роскомнадзор всегда будет отстаивать только публичные интересы. Как тогда соблюсти баланс публичного (обеспечение общественной безопасности) и частного интересов (защита неприкосновенности частной жизни граждан) в информационной сфере?

Решение данной проблемы, как нам видится, лежит в плоскости формирования *независимой от государства* национальной системы органов по защите персональных данных, *per se* выражающими «систему сдержек и противовесов» по отношению к государственным органам и его должностным лицам. Подход и принципы к организации структуры органов, организаций и должностных лиц могут быть частично заимствованы из статей 5 «Цели и принципы аккредитации» и 6 «Состав участников национальной системы аккредитации» Федерального закона от 28.12.2013 № 412-ФЗ «Об аккредитации в национальной системе аккредитации» (далее по тексту — ФЗ № 412)[12] со следующей оговоркой. В соответствии с зарубежным законодательным опытом в области защиты персональных данных:

[11] Проект Постановления Правительства РФ «Об утверждении Положения о государственном контроле и надзоре за соответствием обработки персональных данных требованиям Федерального закона «О персональных данных» (подготовлен Роскомнадзором). Режим доступа: http://www.economy.gov.ru/. Дата обращения: 03.01.2017.

[12] Федеральный закон от 28.12.2013 № 412-ФЗ (ред. от 02.03.2016) «Об аккредитации в национальной системе аккредитации» // Собрание законодательства РФ. 30.12.2013. № 52 (часть I). Ст. 6977.

1) Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) как уполномоченный орган по защите прав субъектов персональных данных (ст. 23 ФЗ № 152) должна быть исключена из этой структуры;

2) осуществление регистрационно-разрешительных, контрольно-надзорных, экспертных и методологических функций Роскомнадзора в сфере информационных технологий и связи должны быть переданы созданному законодательным актом национальному органу по защите персональных данных.

При этом важно отметить, что к создаваемой системе национальных органов по защите персональных данных, в том числе организациям и должностным лицам, должны предъявляться такие основные требования, как компетентность и независимость. Похожий подход отражен в описанных статьей 5 ФЗ № 412-ФЗ принципах аккредитации: компетентность, независимость, беспристрастность и т.д. Независимость от государства была необходимой потому, что государство с приходом информационно-коммуникационных технологий оказалось одной из сторон, заинтересованных в обработке и использовании персональных данных, и, следовательно, ни один из государственных органов не в состоянии был занимать позицию беспристрастного арбитра по отношению к коллизии прав субъекта персональных данных (данную коллизию мы описывали выше в рамках осуществления государственного контроля (надзора)).

III. ОБСУЖДЕНИЕ

Независимость национального органа (организации или должностного лица) по защите персональных данных в различных правовых системах обеспечивается разнообразными средствами: придание ему законом особого правового статуса; его местом в системе государственной власти; процедурой совместного назначения руководителя этого органа несколькими ветвями государственной власти; разделением административной подчиненности и подотчетности национального органа защиты данных между исполнительной и законодательной ветвями власти; прямым указанием закона и многими другими методами [9]. Мы не ставим целью в рамках статьи анализировать процедуру назначения и формирования национальных органов по защите данных — уполномоченных должностных лиц, коллегиальных органов и их полномочия, так как для этого потребуется отдельное исследование, но вместе с тем остановимся на обзоре законодательных актов, в соответствии с которыми создаются независимые от государства национальные органы.

Для англосаксонской правовой семьи в качестве национального органа, как правило, выступает уполномоченный по защите прав граждан на неприкосновенность частной жизни — *Privacy Comissioner*, назначаемый на должность Королевой Великобритании. В соответствии с *Privacy Act* 1988 г.[13] в Австралии

[13] Privacy Act 1988 No 119 (registered 25 October 2016). Режим доступа: https://www.legislation.gov.au/Details/C2016C00979. Дата обращения: 02.01.2017.

учреждена должность *Privacy Comissioner* (федеральный прайвеси-комиссар). В Великобритании система органов по защите данных (неприкосновенности частной жизни) согласно *Data Protection Act* 1998 г.[14] включает в себя: 1) независимого национального Регистратора по защите данных и защите прав индивидуума на невмешательство в его частную жизнь в связи с автоматизированной обработкой персональных данных; 2) общенациональный суд (трибунал) по защите данных, выступающий судебной инстанцией, рассматривающий апелляции пользователей данных и компьютерного бюро на решения Регистратора по защите данных [10; 11; 12. P. 93–128; 13].

Более того, на основании Data Protection Act 1998 г. британский Регистратор и его сотрудники могут приобретать статус государственных (гражданских) служащих лишь в тех случаях, когда такой статус необходим для предоставления Регистратору доступа к файлам данных, содержащим государственную тайну.

Отличительной особенностью канадской системы защиты частной жизни в соответствии с *Privacy Act* 1983 г.[15] является наличие отраслевых федеральных уполномоченных по защите данных. Другими словами, должностное лицо исполняет функции Уполномоченного по защите прав граждан на неприкосновенность частной жизни (*Privacy Comissioner*) в федеральных учреждениях и ведомствах, в банковско-кредитной сфере и других отраслях. Кроме того, *Privacy Act* 1983 г. предусматривает назначение специального федерального Уполномоченного по информации для контроля за исполнением своих решений. Фактически, на должности федерального Уполномоченного по информации и федерального Уполномоченного по защите прав граждан на неприкосновенность частной жизни может быть назначено одно и то же лицо.

Национальный орган по защите данных, формируемый в рамках континентальной правовой семьи, как правило, представлен в законодательстве в отличие от системы общего права не одним должностным лицом, а системой коллегиальных органов.

В Австрии закон 1978 (2000) г. о защите данных[16] установил структуру, состоящую из Совета по защите данных и Комиссии по защите данных [14.

---

[14] Data Protection Act. Режим доступа: http://www.legislation.gov.uk/ukpga/1998/29. Дата обращения: 05.12.2016. Уточним, что UK Data Protection Act был принят в 1984 г. и обновлен в 1998 г. в связи с принятием Директивы Европейского Союза о защите данных в 1995 г. (EU Directive on Data Protection).

[15] Privacy Act 1983. Режим доступа: http://laws-lois.justice.gc.ca/eng/acts/P-21/. Дата обращения: 05.01.2017.

[16] Data Protection Act 2000 (Datenschutzgesetz 2000 — DSG 2000). Режим доступа: http://www.oecd.org/austria/privacyanddataprotectionresourcesaustria.htm. Дата обращения: 02.12.2016). Austrian Data Protection Act был принят в 1978 г. В 2000 г. парламент принял новую редакцию Закона о защите данных (Datenschutzgesetz 2000 — DSG 2000, Федеральный законодательный Бюллетень I № 165/1999) в рамках реализации Директивы ЕС о защите данных.

P. 229–231]. Комиссия по защите данных (ст. 41 DSG 2000) осуществляет полномочия надзора за публичным и частным секторами, административного суда, проведения расследований и наделена другими функциями. Совет по защите данных (ч. 7 ст. 35 DSG 2000) состоит из представителей политических партий, федерального и земельных правительств, муниципалитетов, организаций работодателей и наемных работников. Основными полномочиями этого органа являются подготовка предложений для федерального и земельных правительств по улучшению этих законов, проведение мониторинга в отношении ущерба, который нанесен субъектам данных в результате обработки их данных, затребование информации и отчетов по вопросам обработки данных от организаций публичного и частного секторов и другие функции.

Бельгийским законодательным актом 1992 г. о защите частной жизни при обработке персональных данных[17] также учреждается специальный независимый орган власти — Комиссия по защите неприкосновенности частной жизни (Commission for the protection of privacy), полномочия которой, как и других подобных национальных органов, состоят прежде всего в осуществлении контрольных и надзорных функций за обработкой всех данных, предоставлении консультаций по защите данных и выступает медиатором в случае возникновения правовых конфликтов в сфере обработки данных.

Национальная система органов по защите данных в Германии регламентируется Федеральным законом 1990 (2003) года о защите данных[18]. В соответствии с этим законом организацией контроля за деятельностью всех федеральных органов и подчиненных им структур, занятых сбором и обработкой персональных данных, за соблюдением всех требований Закона 1990 г., занимается Федеральный уполномоченный по защите данных [15. С. 322–326; 16. С. 29–44]. Согласно статье 1 параграфа 22 Закона 1990 г. Федеральный уполномоченный выбирается Бундестагом по представлению Федерального правительства и назначается на должность Федеральным президентом. Федеральный уполномоченный осуществляет контрольно-надзорные, регистрационные и экспертно-консультативные функции. Кроме того, на региональном уровне Земельные уполномоченные по защите данных назначаются правительствами земель, объем полномочий и функций которых регламентируются законами Земель. Законом 1990 г. также предусмотрены уполномоченные по защите данных в организациях, которые заняты обработкой персональных данных. Деятельность этих уполномоченных ограничена лишь контрольно-надзорными функциями.

---

[17] Act on the Protection of Privacy in Relation to the Processing of Personal Data. Режим доступа: http://www.slideshare.net/Johan_Vdd/data-protection-act-8-dec-1992-consolidated-version-v1. Дата обращения: 01.11.2016.

[18] Federal Data Protection Act. Режим доступа: http://www.gesetze-im-internet.de/englisch_bdsg. Дата обращения: 01.11.2017.

И последний вопрос, требующий тщательного анализа в рамках уже самостоятельного исследования, — это проблема изучения государственного контроля в качестве механизма формирования правосознания граждан. Органы государственной власти с помощью разнообразных информационных технологий могут воздействовать на формирование правосознания (мировоззрения) человека путем закрепления публичных интересов — государственной *идеологии*, с одной стороны. Поэтому в статьях Конституции РФ у нас до сих пор отсутствует закрепление какой-либо идеологии, в том числе и государственной. И это, на наш взгляд, было верным концептуальным решением при разработке проекта Конституции РФ. Должна быть конкуренция разнообразных идеологий, которая предоставляет возможность выбора человеком любого мировоззрения — *свобода совести*. С другой, государственные органы могут создать условия (материальные и законодательные) для формирования правового механизма, обеспечивающего неприкосновенность частной жизни. В чем его суть?

Государство должно быть инструментом осуществления контроля (надзора), связанного с тем, чтобы деятельность субъектов, распространяющих информацию, в том числе и массовую, не была направлена на нарушение неприкосновенности частной жизни, выражающееся в активном или пассивном воздействии на сознание человека этой информации.

Однако государство выступает на конкурентном рынке идеологий фактически *монополистом*, то есть носителем определенных взглядов (ценностей), которые с помощью информационно-компьютерных технологий навязываются человеку и обществу в целом. В ситуации постоянного потока информации, предоставляемой СМИ, индивид не имеет возможности ее освоить, понять ее созидающие или разрушающие последствия на формирование его целостной личности. По этой причине государство должно гарантировать человеку правовую защиту неприкосновенности его частной жизни [17. P. 543–568; 18], выражающейся не только в возможности ему пребывать наедине с самим собой, но и в возможности правовой защиты его информационного пространства от воздействия разнообразных идеологий, в том числе государственной. Но могут ли государственные органы, осуществляющие государственный контроль (надзор), не являться носителями государственной идеологии? В этом и состоит суть проблемы.

IV. ВЫВОДЫ

Из сказанного выше можно заключить, что:

1) государственный контроль (надзор) в информационной сфере в контексте темы нашей статьи — это проверка Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) деятельности организаторов распространения информации в сети «Интернет» и операторов связи, осуществляющих обработку персональных данных,

направленной на предупреждение, выявление и пресечение нарушений требований законодательства РФ в области персональных данных;

2) вместе с тем осуществление государственного контроля за требованиями законодательства в информационной сфере становится изначально предвзятым, если между нормами федеральных законов обнаруживается коллизия в части определения цели обработки персональных данных: защиты публичного интереса в целях борьбы с терроризмом и обеспечением общественной безопасности либо защиты информационного аспекта неприкосновенности сферы частной жизни граждан;

3) по причине того, что Роскомнадзор, наделенный контрольно-надзорными полномочиями, выступает уполномоченным органом по защите прав субъектов персональных данных, учрежденного исключительно исполнительной властью, то данный государственный орган будет обязан руководствоваться прежде всего защитой публичного интереса, что приводит к нарушению баланса между публичным и частным интересами;

4) в целях сохранения указанного баланса интересов и беспристрастного государственного контроля (надзора) в информационной сфере предлагаем сформировать в Российской Федерации систему национальных органов по защите неприкосновенности частной жизни в сфере обработки персональных данных, основанную на принципах независимости от государства, компетентности и беспристрастности. За базовую модель построения такой системы органов, формирования состава их членов можно взять законодательный опыт федеративных государств, например Австрии и Германии, близких нам как по форме государственно-территориального устройства, так и по характеристикам правовой системы.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

[1] *Ковалев С.И., Иванская А.В.* Проблемы правовой защиты информации приватного характера в условиях развития научно-технического прогресса // Вестник Российского университета дружбы народов. Серия: Юридические науки. 2014. № 1. С. 44–52.

[2] *Демин А.А*. Ценностные основания формирования идентичности сообщества // Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики. 2015. № 2–1(52). С. 73–78.

[3] Новая парадигма защиты и управления персональными данными в Российской Федерации и зарубежных странах в условиях развития систем обработки данных в сети интернет / под ред. А.С. Дупан (Гутниковой). М.: Издательский дом ВШЭ, 2016. 344 с.

[4] *Бачило И.Л., Сергиенко Л.А., Кристальный Б.В., Арешев А.Г.* Персональные данные в структуре информационных ресурсов. Основы правового регулирования. Минск: Белтитфонд, 2006. 474 с. [Bachilo IL Sergienko LA, Kristal'nyi BV, Areshev AG. *Personal'nye dannye v strukture informatsionnykh resursov. Osnovy pravovogo regulirovaniya*

[5] *Савельев А.И.* Проблемы применения законодательства о персональных данных в эпоху больших данных (Big Data) // Право. Журнал Высшей школы экономики. 2015. № 1. С. 43–66.

[6] *Карпович О.Г.* Сравнительно-правовой анализ «Закона Яровой» и «Акта патриота» // Закон и право. 2016. № 9. С. 15–18.
[7] *Болгова В.В.* Публичный интерес и неприкосновенность частной жизни: некоторые проблемы баланса // Вестник Волжского университета им. В.Н. Татищева. 2016. Т. 1. № 2. С. 112–117.
[8] *Любимов А.П., Авдеев М.Ю.* Конституционное право на неприкосновенность частной жизни в России и зарубежных странах. М.: Юркомпани, 2015. 216 с.
[9] *Bygrave L.A.* Data Privacy Law: An International Perspective. Oxford: Oxford University Press, 2014. 272 p.
[10] *Calo M.R.* Against Notice Skepticism in Privacy (and Elsewhere) // Notre Dame Law Review. 2012. Vol. 87. Issue. 3. P. 1027–1072.
[11] *Carey P.* Data Protection: A Practical Guide to UK and EU Law. 2nd ed. Oxford, New York: Oxford University Press, 2004. 532 p.
[12] *Crawford K., Schultz J.* Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms // Boston College Law Review. 2014. Vol. 55. Issue. 1. p. 93–128.
[13] *Freedman W.* The right of privacy in the computer age. New York: Quorum Books, 1987. 163 p.
[14] *Mantelero A.* The EU Proposal for a General Data Protection Regulation and the roots of the 'right to be forgotten' // Computer Law & Security Review. 2013. Vol. 29. Issue. 3. p. 229–231.
[15] *Горелихина О.А., Шлиньков А.А.* Правовая защита персональных данных в Германии // Вопросы экономики и права. 2012. № 45. С. 322–326.
[16] *Проскурякова М.И.* Конституционно-правовые основы защиты персональных данных в России и Германии в истолковании органов конституционного правосудия // Сравнительное конституционное обозрение. 2015. № 1(104). С. 29–44. *McDonald A.M., Cranor L.*F., The Cost of Reading Privacy Policies // Journal of Law and Policy for the Information Society. 2008. Vol. 4. N. 3. P. 540–568.
[17] *Murphy R.* Social Distance and Veil // Philosophical Dimensions of Privacy. An Anthology / Ed. by F.D. Schoeman. Cambridge, New York: Cambridge University Press, 1984. x, 426 p.

СВЕДЕНИЯ ОБ АВТОРАХ:
Иванский Валерий Прокопьевич — кандидат юридических наук, доцент, доцент кафедры административного и финансового права Юридического института Российского университета дружбы народов.
Контактная информация:
e-mail: ivansky_valera@mail.ru

Мельничук Григорий Владимирович — кандидат юридических наук, доцент, доцент кафедры административного и финансового права Юридического института Российского университета дружбы народов.
Контактная информация:
e-mail: gregory@melnichuk.org

Иванский В.П., Мельничук Г.В. *Вестник РУДН. Серия*: *Юридические науки*. 2017. Т. 21. № 1. 136–152

STATE CONTROL (SUPERVISION) IS A TOOL OF THREAT COUNTERMEASURE TO NATIONAL SECURITY IN THE INFORMATION SPHERE OR MEANS OF PRIVACY PROTECTION: BALANCE OF PUBLIC AND PRIVATE INTERESTS

V.P. Ivanskiy, G.V. Melnichuk

RUDN University
Law Institute
6, Miklukho–Maklaya st., Moscow, Russia, 117198

The article discusses some problems related to the ratio of two fundamental values — the legal protection of the public and the private interests in the sphere of computer data processing. On one hand, the use of information and communication technologies is potentially utilized as networking platforms for the preparation, organization, and implementation of crime and thereby is threatening the security of the state, society, and the individual. However, these technologies are a means of data collection, storage, conversion, and the distribution of private information about citizens' (personal data). It is important to note the threat to public order and the inviolability of privacy forming in the information sphere is being addressed in the context of the adopted package of amendments designed to ensure public safety and security, as well as counter-terrorism, which is called the "Yarovaya Law", Information Security Doctrine of the Russian Federation, Russian Federal Law on Personal Data Protection, and additionally as the Russian Federation Government Draft Resolution on State Control and Supervision over the Compliance of Personal Data Processing with the Requirements of the Personal Data Legislation of the Russian Federation.

However, in accordance with the Federal Law on Personal Data, the purpose of processing personal data is limited to the achievement of pre-defined and legitimate objectives. Moreover, the Information Security Doctrine of the Russian Federation recognizes the security and protection of privacy when using information technology vis-à-vis national interests. However, along with the above indicated regulations aimed at protecting the information on the private lives of citizens, the purpose of collection, storage, and use of personal data according to the "Yarovaya Law" is counter-terrorism and public safety. It follows that the legislation regulates both mutually exclusive purposes of processing personal data. Meanwhile, Roskomnadzor is an authorized federal executive for the protection of the personal data bearing subjects' rights, carrying out state control (supervision) functions over compliance requirements of legislation of the Russian Federation, which include the definition of the purpose of processing of personal data. Due to the fact that purposes of processing of personal data are legitimate, but conflicting with each other, the Roskomnadzor is forced to violate the principle of impartiality in the implementation of the control (supervision), initially defending the public interest, thereby infringing upon them and consisting of the protection of the information aspect of the inviolability of private life. In connection with the above-mentioned circumstances, the authors propose is to balance public and private interests in the formation of a supervisory bodies system for the protection of personal data based on the legislative experience of developed countries.

Key words: state control; information sphere; privacy; terrorism; personal data; information security; the national authority for the protection of personal data

REFERENCES

[1] Kovalev SI, Ivanskaya AV. Legal defense problems of the confidential information in the conditions of scientific-technological progress development. *RUDN Journal of Law.* 2014;1:44–52. (In Russian).

[2] Demin AA. Value Bases of Community Identity Formation. *Historical, Philosophical, Political and Law Sciences, Culturology and Study of Art. Issues of Theory and Practice.* 2015;2–1(52):73–78. (In Russian).

[3] Dupan (Gutnikova) AS, editor. *Novaya paradigma zashchity i upravleniya personal'nymi dannymi v Rossiiskoi Federatsii i zarubezhnykh stranakh v usloviyakh razvitiya sistem obrabotki dannykh v seti internet* [New paradigm of protection and management of personal data in the Russian Federation and foreign countries in the conditions of development data processing systems on the Internet]. Moscow: HSE Publishing House; 2016. 344 p. (In Russian).

[4] Bachilo IL Sergienko LA, Kristal'nyi BV, Areshev AG. *Personal'nye dannye v strukture informatsionnykh resursov. Osnovy pravovogo regulirovaniya* [Personal data in the structure of information resources. The legal regulation]. Minsk: Bellitfond; 2006. 474 p. (In Russian)

[5] Savelyev AI. (2015) The Issues of Implementing Legislation on Personal Data in the Era of Big Data. *Pravo. Zhurnal Vysshey shkoly ekonomiki*. 2015;1: 43–66. (In Russian).

[6] Karpovich OG. "Yarovaya Law" and "Patriot Act" – comparative analysis. *Law and Legislation.* 2016;9:15–18. (In Russian).

[7] Bolgova VV. Public Interest and Privacy: Some Balance Problems. *Vestnik of Volzhsky University after V.N. Tatischev.* 2016;1(2):112–117. (In Russian).

[8] Lyubimov AP, Avdeev MYu. *Konstitutsionnoe pravo na neprikosnovennost' chastnoi zhizni v Rossii i zarubezhnykh stranakh* [The constitutional right of privacy in Russia and foreign countries]. Moscow: Yurkompani; 2015. 216 p. (In Russian).

[9] Bygrave LA. *Data Privacy Law: An International Perspective*. Oxford: Oxford University Press; 2014. 272 p.

[10] Calo M.R. Against Notice Skepticism in Privacy (and Elsewhere). *Notre Dame Law Review.* 2012;87(3):1027–1072.

[11] Carey P. *Data Protection: A Practical Guide to UK and EU Law.* 2nd ed. Oxford, New York: Oxford University Press; 2004. 532 p.

[12] Crawford K, Schultz J. Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms. *B.C.L. Rev.* 2014;55(1):93–128.

[13] Freedman W. *The right of privacy in the computer age*. New York: Quorum Books; 1987. 163 p.

[14] Mantelero A. The EU Proposal for a General Data Protection Regulation and the roots of the 'right to be forgotten'. *Computer Law & Security Review.* 2013;29(3):229–231. doi:10.1016/j.clsr.2013.03.010.

[15] Gorelikhina OA, Shlin'kov AA. Pravovaya zashchita personal'nykh dannykh v Germanii [Legal protection of personal data in Germany]. *Economic and Law Issues.* 2012;45:322–326. (In Russian).

[16] Proskuryakova MI. Konstitutsionno-pravovye osnovy zashchity personal'nykh dannykh v Rossii i Germanii v istolkovanii organov konstitutsionnogo pravosudiya [The constitutional and legal foundations of personal data protection in Russia and Germany in the interpretation of the bodies of constitutional justice]. *Comparative Constitutional Review.* 2015;1(104):29–44. (In Russian).

[17] McDonald AM, Cranor LF. The Cost of Reading Privacy Policies. *Journal of Law and Policy for the Information Society*. 2008;4(3):540–568.

[18] Murphy R. *Social Distance and Veil.* In: Schoeman FD, editor. *Philosophical Dimensions of Privacy. An Anthology*. Cambridge, New York: Cambridge University Press; 1984. x, 426 p.

INFORMATION ABOUT THE AUTHORS:
Ivanskiy Valeriy P. — Candidate of Legal Sciences, Associate Professor, Administrative and Financial Law Department, Law Institute, RUDN University.
Contact information:
e-mail: ivansky_valera@mail.ru

Melnichuk Grigory V. — Candidate of Legal Sciences, Administrative and Financial Law Department, Law Institute, RUDN University.
Contact information:
e-mail: gregory@melnichuk.org