УДК 004.932 Вестник УрФО № 2(24) / 2017, с. 57–64

Терещенко Л. К., Кривогин М. С.

ОСОБЕННОСТИ ПРАВОВОГО РЕГУЛИРОВАНИЯ ОБЩЕДОСТУПНЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Рассматриваются актуальные проблемы правового регулирования общедоступных персональных данных. Автором определяется содержание понятия «неограниченный круг лиц» с учетом специфики Интернета. Анализируются современные доктринальные тенденции правового регулирования персональных данных, делается вывод о необходимости установления ограничений при обработке общедоступных персональных данных. Указывается на важность применения обособленного правового регулирования для общедоступных персональных данных и материальных носителей персональных данных, которые также могут являться общедоступными. Несмотря на то, что другие лица могут видеть материальные носители персональных данных без существенных ограничений, это не будет являться основанием для придания персональным данным статуса общедоступных. Выявлено, что законодательные ограничения на обработку общедоступных персональных данных устанавливаются для тех видов сведений, общедоступность которых субъект персональных данных не может контролировать. К таким сведениям относятся биометрические персональные данные, поскольку субъект не всегда может самостоятельно определять в каком случае и каким лицам они могут быть предоставлены.

Ключевые слова: общедоступные, персональные данные, биометрические, соглашение, интернет.

Tereshenko L. K., Krivogin M. S.

FEATURES OF LEGAL REGULATION OF PUBLICLY AVAILABLE PERSONAL DATA

Actual problems of legal regulation of publicly available personal data are examined. The author defines the substance of the term «general public» in case of personal data processing in the Internet. Modern theoretical tendencies of legal regulation of personal data are analyzed, the author concludes the necessity of imposing several restrictions in course of publicly available personal data processing. It is also indicated to the importance of application of specific legal regulation to publicly available personal data and material object of personal data, which could also be publicly available. Although, other person could see material objects of personal data without any limitations, it wouldn't be the basis for personal data to be publicly available. It is also indicated, that restrictions in legislation for publicly available personal data processing are imposed to the types of data, public availability of which data subject are not able to control. This type of information is biometric personal data, because data subject couldn't define at what time and to which person it might be provided.

Keywords: publicly available, personal data, biometric, contract, internet.

В рамках Федерального закона № 152 от 27.07.2006 г. «О персональных данных», помимо прочих условий, одним из критериев допустимости обработки персональных данных без согласия субъекта является обработка сведений доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных (далее – общедоступные персональные данные). Однако, не всегда ясно, что включается в данное понятие, существуют ли какие-либо пределы в обработке таких сведений, а также необходимо ли учитывать природу различных категорий персональных данных при применении данной нормы.

Первоначально необходимо рассмотреть само понятие общедоступных персональных данных. Исходя из п. 10 ч. 1 ст. 6 ФЗ «О персональных данных», для того, чтобы персональные данные получили статус общедоступных, необходимо чтобы доступ неограниченного круга лиц к ним был предоставлен субъектом персональных данных. В законодательстве о персональных данных отсутствует указание на то, что понимается под неограниченным кругом лиц. Особенно важно ответить на данный вопрос при обработке персональных данных в условиях Интернета, где информация уже сразу после размещения на сайте может стать доступной для любого человека. Рассмотрим другие нормативно-правовые акты, где используются схожие понятия.

Формулировка «неограниченный круг лиц» встречается во многих федеральных законах, например, в Гражданском кодексе РФ, ФЗ № 126 от 07.07.2003 «О связи», ФЗ № 218 от 13.07.2015 «О государственной регистрации недвижимости», ФЗ № 262 от 22.12.2008 «Об обеспечении доступа к информации о деятельности судов в Российской Федерации», ФЗ № 63 от 06.04.2011 «Об электронной подписи» и др. Также в некоторых законах используется термин «неопределенный круг лиц», который в данном случае, является тождественным рассматриваемому определению.

Наиболее близким к данной сфере являются ФЗ № 38 от 13.03.2006 г. «О рекламе» и ФЗ № 2124-1 от 27.12.1991 г. «О средствах массовой информации», поскольку они в большей степени связаны со сферой оборота информации, а также относятся многими исследователями, наряду с законодательством о защите персональных данных, к области информационного права[1].

В п. 1 ст. 3 ФЗ «О рекламе» указывается, что для того, чтобы закон применялся в отношении распространяемой информации, необходимым условием является адресация данных сведений неопределенному кругу лиц. Для внесения ясности в понятие «Неопределенный круг лиц», Федеральной антимонопольной службой были даны разъяснения - «под неопределенным кругом лиц понимаются те лица, которые не могут быть заранее определены в качестве получателя рекламной информации (…)»[2].

Данное разъяснение можно учитывать и применительно к сфере защиты персональных данных. Например, если субъект размещает свои персональные данные на сайте или в социальной сети, где отсутствуют какие-либо ограничения на возможность доступа к такой информации для других лиц, то в данном случае можно признать, что персональные данные являются общедоступными, поскольку к ним возможен доступ неограниченного круга лиц. Как следствие, третьи лица могут обрабатывать такие данные без согласия субъекта.

В случае, если субъект персональных данных, размещает информацию о себе в закрытых группах, либо ограничивает доступ к ней в социальной сети исключительно для ограниченного круга лиц, например, для друзей, то в таком случае персональные данные не будут считаться сделанными общедоступными субъектом. Следовательно, применяются положения ст. 7 ФЗ «О персональных данных», которые обязывают лиц получивших доступ к персональным данным не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта.

Однако, здесь может возникнуть проблема, что несмотря на то, что доступ к странице профиля или записи с персональными данными в социальной сети имеют хоть и определенные лица, однако их количество настолько велико, что в данном случае сохранение конфиденциальности персональных данных будет проблематичным. Поэтому при определении того, был ли доступ к персональным данным предоставлен неограниченному кругу лиц необходимо также принимать во внимание количество человек, которые могут иметь доступ к таким сведениям. Даже несмотря на то, что круг лиц может быть

[1] Рассолов И.М. Информационное право: учебник для магистров. – 2-е изд., испр. и доп. – М.: Юрайт, 2012. С. 68; Бачило И.Л. Информационное право: учебник. – 5-е изд., перераб. и доп. – М.: Юрайт, 2016. С 33.

[2] Письмо ФНС РФ от 05.04.2007 N АЦ/4624 «О понятии «неопределенный круг лиц» // СПС КонсультантПлюс.

определен конкретным числом и ограничен, тем не менее, если субъект персональных данных не производит осознанный выбор в отношении лиц, которым будет предоставлен доступ к персональным данным, то персональные данные также должны считаться сделанными общедоступными. Противоположный подход предполагал бы, что даже если лицо размещает свои персональные данные в социальной сети, когда такие сведения доступны только ее пользователям, персональные данные не будут считаться общедоступными, поскольку круг лиц ограничен гражданами, которые зарегистрированы на конкретном сайте.

Проблема использования информационных технологий для сбора и обработки персональных данных, а также последующего получения дополнительных сведений на основе уже имеющейся информации о субъектах, неоднократно освещалась в правовой литературе[3].

Несмотря на то, что персональные данные могут быть сделаны общедоступными субъектом, это не означает, что любое лицо может осуществлять их обработку без каких-либо ограничений. Общедоступность персональных данных предполагает только отсутствие обязанности у оператора получить согласие субъекта персональных данных на их обработку и направлять уведомление уполномоченному органу по защите прав субъектов персональных данных о начале обработки.

В то же время, общие принципы обработки персональных данных, а также право субъекта, на доступ, корректировку его персональных данных подлежат применению даже несмотря на то, что персональные данные были сделаны общедоступными.

Сегодня большинство крупных интернет сервисов формулируют цель обработки персональных данных так, что под нее могут подпадать большинство используемых сведений. Например, в политиках конфиденциальности поисковых систем (Google[4], Bing[5] и др.), одной из целей обработки персональных данных является повышение качества собственных сервисов, а также персонализация услуг. В таком случае, оператор персональных данных может собирать намного больше сведений, чем это необходимо, обосновывая свои действий целью, которая практически всегда будет являться законной и длящейся неограниченный период времени[6].

Однако, инициатива по приданию персональным данным общедоступности должна исходить от самого субъекта. Также необходимо принимать во внимание характер обработки персональных данных осуществляемой оператором. Во многих случаях, необходимость придания персональным данным статуса общедоступных является неотъемлемым условием их обработки, например, в социальных сетях. Однако, по общему правилу, если цель обработки может быть достигнута без придания персональным данным общедоступности, то включение таких условий в соглашение должно быть признано незаконным и не влечь правовых последствий для субъекта персональных данных.

Ранее в соглашения с субъектом персональных данных зачастую включались условия о том, что физическое лицо, получая определенные услуги, делает свои персональные данные общедоступными. Такая практика использовалась многими достаточно крупными компаниями, например, РЖД[7], для того, чтобы не принимать мер защиты конфиденциальности таких данных, поскольку в предыдущей редакции ФЗ «О персональных данных» от 04.06.2011 в рамках п. 2 ч. 2 ст. 7 не требовалось обеспечивать конфиденциальность для общедоступных персональных данных. В действующей редакции закона такие исключения не предусмотрены. Даже если указанные условия содержались бы в соглашении, то несмотря на это, персональные данные не будут считаться сделанными общедоступными субъектом, поскольку согласие не будет считаться свободным в рамках ч. 1 ст. 9 ФЗ «О персональных данных», т.к. субъект стоит перед выбором – приобретать билет и делать свои персональные данные общедоступными, либо отказаться от поездки.

---

[3] Савельев А.И. Проблемы применения законодательства о персональных данных в эпоху «Больших данных» (Big Data) // Право. Журнал Высшей школы экономики. 2015. №1. С. 60.

[4] Политика конфиденциальности и условия использования // Google. URL: https://www.google.ru/intl/ru/policies/privacy/ (дата обращения: 01.08.2016).

[5] Заявление о конфиденциальности. // Microsoft. URL: https://privacy.microsoft.com/ru-ru/privacystatement/ (дата обращения: 01.08.2016).

[6] Data Protection Principles for the 21st Century: revising the 1980 OECD Guidelines // Oxford internet institute. URL: http://www.oii.ox.ac.uk/publications/Data_Protection_Principles_for_the_21st_Century.pdf (дата обращения 24.07.2016)

[7] РЖД и персональные данные // Блог Артема Агеева. URL: http://www.itsec.pro/2013/03/blog-post_25.html

В то же время, если оператор персональных данных может найти необходимую цель для признания обработки общедоступных персональных данных легитимной, то у субъекта персональных данных остается незначительное количество оснований для возможности требовать прекращения обработки.

В связи с этим в доктрине постепенно начинают появляться упоминания о необходимости установления дополнительных ограничений для возможности обработки оператором персональных данных, которые были сделаны общедоступными субъектом. В этом случае сам факт общедоступности персональных данных должен быть только одним из нескольких условий законности обработки персональных данных. Например, для того, чтобы принцип справедливости обработки был соблюден, оператор должен убедиться, что обработка общедоступных персональных данных не будет влечь для субъекта определенных трудностей в реализации прав и законных интересов[8]. В противном случае, оператору необходимо получить согласие субъекта персональных данных.

Одним из ограничений может выступать т.н. условная общедоступность, когда несмотря на то, что персональные данные субъекта являются общедоступными, тем не менее, оператор должен учитывать цель придания таким сведениям публичности. Соответственно, дальнейшая обработка таких персональных данных третьими лицами должна производиться исключительно для подобных целей. Например, если персональные данные физического лица публикуются в реестре прав на недвижимое имущество, то их обработка должна соответствовать тем целям, для которых данный реестр создавался – предоставление гражданам информации о собственнике определенного помещения[9]. Если же происходит использование такой информации для других целей – получение данных об истории владения определенным лицом отдельными помещениями и т.п., то обработка будет признана незаконной.

Для того, чтобы персональные данные считались общедоступными, они должны быть сделаны такими именно субъектом персональных данных, в противном случае, даже несмотря на наличие исключений для одного оператора, например, в рамках осуществления профессиональной деятельности журналиста, когда на сайте публикуется соответствующая информация, для других лиц эти персональные данные не будут считаться сделанными общедоступными субъектом, соответственно, у них не возникает права на осуществление обработки таких сведений. Это подтверждается также и судебной практикой, когда суды признают, что «наличие информации о частной жизни лица в других средствах массовой информации не освобождает ответчика от исполнения предусмотренной законом обязанности по получению согласия указанного лица на распространение информации о его частной жизни»[10].

Другое ограничение может быть связано непосредственно с субъективными намерениями субъекта персональных данных, который делая свои персональные данные общедоступными, ожидает что они могут быть в дальнейшем использованы только определенным образом[11].

Одним из таких случаев может быть использование изображений пользователей в социальной сети с целью их последующей идентификации на основе биометрических персональных данных. Практически во всех социальных сетях, политикой конфиденциальности предусматривается, что изображение, которое размещает пользователь на своей главной странице является общедоступным и к нему не могут применяться ограничения в рамках настроек конфиденциальности. В данном случае, основное назначение использования изображения – предоставление возможности другим лицам получить актуальную информацию о человеке. Соответственно, загружая в социальную сеть фотографию, лицо разумно ожидает, что она будет использоваться либо для просмотра, либо для распространения среди других граждан, что также подтверждается и судебной практикой[12].

Обработка общедоступных персональных данных допустима в случаях, когда такие сведения относятся к общей категории пер-

[8] Personal information online code of practice // Information commissioner's office. URL: https://ico.org.uk/media/for-organisations/documents/1591/personal_information_online_cop.pdf (дата обращения 02.08.2016).

[9] Greenleaf G. Asian Data Privacy Laws: Trade & Human Rights Perspectives. Oxford, Oxford university press, 2014. P. 126.

[10] Решение Басманного районного суда г. Москва от 28 марта 2012 г. по делу № 2-920/12.

[11] Beamish B. Multiple data owners: who's doing what with your data? // University of Southampton. URL: http://eprints.soton.ac.uk/356026/1/356026.pdf (дата обращения 05.08.2016).

[12] Определение городского суда г. Санкт-Петербург от 31 марта 2016 г. по делу № 33-6123/2016.

сональных данных (п. 10 ч. 1 ст. 6), а также к специальным персональным данным (п. 2 ч. 2 ст. 10). В законе существуют только два исключения из возможности обработки персональных данных, которые были сделаны субъектом общедоступными: если они относятся к сведениям о судимости и к биометрической категории персональных данных.

Биометрические персональные данные представляют тот случай, когда в законодательство о защите персональных данных вводится специальное правовое регулирование, которое должно учитывать особенности определенных видов сведений, когда применение общего правового режима может нанести существенный вред субъекту персональных данных.

Федеральный закон «О персональных данных» был принят еще в 2006 году, т.е. более 10 лет назад, когда социальные сети только начинали появляться, а биометрические технологии распознавания изображений еще не имели столь существенных возможностей в применении, которые они имеют в настоящее время. Несмотря на относительную давность принятия нормативно-правового акта, уже в первой его редакции содержались нормы, которые обеспечивали гарантию защиты биометрических персональных данных субъекта от возможных злоупотреблений со стороны оператора.

Введение соответствующих исключений для биометрических персональных данных было обусловлено тем, что субъект имеет намного меньшие возможностей по контролю над распространением собственного изображения. Например, ст. 152.1. ГК РФ предусматривает возможность использования изображения гражданина, если оно не является основным объектом съемки, также допустимо использование изображения в общественных интересах. В рамках законодательства в сфере защиты персональных данных допустимой признается обработка изображения гражданина, если она осуществляется в рамках профессиональной деятельности средств массовой информации.

Как видно, возможность обработки и распространения изображения лица субъекта без его согласия является предпосылкой для установления более строгих мер в отношении вторичного использования изображения, где субъект не может разумно предполагать какой вид обработки будет применяться оператором. Данный случай относится и к биометрическим персональным данным, что также отражает и саму сущность законодательства в сфере защиты неприкосновенности частной жизни - если у гражданина отсутствует возможность контролировать предоставление определенных сведений третьим лицам, именно на последних возлагаются дополнительные ограничения по использованию персональных данных[13].

Однако, в судебной практике зачастую происходит смешение материальных носителей персональных данных, которые другие лица могут видеть в повседневной жизни и возможностью обработки персональных данных сделанных общедоступными субъектом, например, в Интернете. Наиболее подробно это можно продемонстрировать на примере внешних признаков человека.

Так, в судебном деле, где ставился вопрос о правомерности обработки персональных данных истца (изображения лица), суд указал, что «внешность истца и указанные данные (имя, фамилия, должность) являются общедоступными. Доступ к указанным данным предоставлен истцом и его работодателем для неограниченного круга лиц, следовательно, они являются общедоступными»[14]. В другом деле суд, рассматривая вопрос о правомерности обработки учреждением специальных категорий персональных данных, установил, что «такую категорию персональных данных как инвалидность, в соответствии с пунктом 2 части 2 статьи 10 Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных» можно отнести к общедоступным»[15].

В приведенных делах, суд ошибочно применяет нормы законодательства в сфере защиты персональных данных на те отношения, которые не включены в сферу действия ФЗ «О персональных данных». В ч. 1 ст. 1 ФЗ «О персональных данных» указывается, что законом регулируются отношения, связанные с использованием средств автоматизации или без использования таких средств, если обработка персональных данных соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации. Несмотря на то, что отдельные физиологические характеристики человека по своей природе является публич-

[13] Schoehman D. Philosophical dimensions of privacy. Oxford, Oxford University press, 1984. P. 1.

[14] Решение Центрального районного суда г. Кемерово от 31 января 2014 г. по делу № 2-285/2014.

[15] Решение арбитражного суда Краснодарского края от 29 апреля 2011 г. по делу № А32-2810/2011.

ным, т.е. другие субъекты могут их видеть без каких-либо ограничений, это не означает, что они будут являться общедоступными персональными данными, которые другие граждане могут обрабатывать без согласия субъекта в рамках ФЗ «О персональных данных». Поэтому, необходимо также учитывать и действия субъекта персональных данных, которые должны быть направлены именно на придание информации о себе общедоступности[16].

Несмотря на то, что в ч. 2 ст. 11 ФЗ «О персональных данных» отсутствует возможность обрабатывать общедоступные персональные данные без согласия субъекта, немалое значение также играет и то, что понимается под биометрическими персональными данными, а также на каких лиц будет распространяться действие закона. Ведь установив определенные требования для признания персональных данных биометрическими, данное регулирование будет влиять и на положения об ограничении обработки персональных данных сделанных общедоступными субъектом.

В первой редакции ФЗ «О персональных данных» под биометрическими персональными данными понимались сведения которые характеризуют физиологические особенности человека и на основе которых можно установить его личность. Ввиду определенных коллизий, которые появлялись при применении данной нормы, в закон были внесены поправки, в настоящее время биометрические персональные данные определяются как сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных.

Однако, при внесении поправок в 2011 году в ФЗ «О персональных данных» в части применения норм о защите биометрических персональных данных, только если они используются именно оператором для определения физического лица, не принималась во внимание основная направленность установления соответствующих ограничений – обеспечение возможности субъекту не быть подвергнутым автоматизированной идентификации с помощью той информации, которая является общедоступной для других лиц.

Данная проблема усугубляется и тем, что в последние годы в интернете начинают появляться сервисы которые используют изображения пользователей на сайтах в целях биометрической идентификации по физиологическим параметрам лица.

В пользовательском соглашении одного из таких сервисов, в разделе Ограничение ответственности, в п. 7.1. и 7.2. приводятся следующие условия: «(…) сервис не оказывает пользователю услуги по поиску третьих лиц в социальной сети, сервис предоставляет пользователю техническую возможность для осуществления поисковых запросов на условиях соглашения», «при осуществлении пользователем поисковых запросов, сервис не производит обработку персональных данных пользователей социальной сети, в результате осуществления поискового запроса пользователю предоставляется общедоступная информация из социальной сети» [17].

Как видно, в соглашении к сервису описывается прямо противоположное тому, чем он на само деле является. Сервис позволяет третьим лицам осуществлять поиск по биометрическим характеристикам лица, при этом обрабатывая не только обычные категории персональных данных (фотография), но также биометрические, поскольку изображение используется для целей установления личности субъекта.

Примечательно, что как Роскомнадзор[18], так и отдельные юристы[19], не видят очевидного нарушения законодательства о персональных данных, в части обработки биометрических персональных данных без согласия субъекта, смешивая общедоступность обычной категории персональных данных и биометрических.

Учитывая, что в большинстве случаев, субъектами которые используют данный сервис в интернете будут являться физические лица, то вероятность наложения ответственности существенно мала, а с учетом максимальной суммы административного штрафа 500 рублей в рамках ст. 13.11 КоАП РФ, защит-

[16] Приезжева А.А. Федеральный закон «О персональных данных»: научно-практический комментарий. М.: Редакция «Российской газеты», 2015. Вып. 11. С. 59.

[17] Пользовательское соглашение // Findface. URL: https://findface.ru/pdf/agreement.pdf (дата обращения 6.08.2016).

[18] Интернет видит все: как спастись от слежки через веб-камеру и сервисов по поиску людей по фото // Газета.ru. URL: https://www.gazeta.ru/tech/2016/04/29_a_8204579.shtml (дата обращения 6.08.2016).

[19] Законна ли технология FindFace и как себя от нее обезопасить? // Meduza. URL: https://meduza.io/feature/2016/04/27/zakonna-li-tehnologiya-findface-i-kak-sebya-ot-nee-obezopasit (дата обращения 6.08.2016).

ная функция не сможет быть реализована. Поэтому рационально рассматривать данный сервис в качестве оператора биометрических персональных данных, поскольку именно он определяет цели обработки, состав персональных данных, а также действия, совершаемые с персональными данным.

Критерий использования биометрических персональных данных для определения личности субъекта следует рассматривать не только в рамках тех действий, которые совершает оператор, но также и возможностей которые предоставляются третьим лицам. В таком случае, интернет-сервис, который любое лицо может использовать для идентификации других граждан по биометрическим характеристикам без их согласия, не должен рассматриваться в рамках информационного посредника, например, как облачные сервисы для хранения информации, поскольку деятельность оператора направлена именно на обработку биометрической информации, а не на общее хранение данных, как, например, происходит в Dropbox, Icloud и т.п.

Поэтому, во избежание возможных нарушения прав субъектов персональных данных необходимо также распространять нормы, регулирующее обработку биометрических персональных данных и на операторов, которые хоть и не имеют цель установить личность определенного субъекта, однако предоставляют такие возможности другим лицам. В противном случае может получиться парадоксальная ситуация, когда сервис будет являться оператором обычных категорий персональных данных, обработку которых он может производить без согласия субъекта как в рамках п. 10 ч. 1 ст. 6 ФЗ «О персональных данных», так и по п. 7 ч. 1 ст. 6 названного закона, и лишь субъект, который производит поиск по физиологическим характеристикам лица других граждан с помощью данного сервиса может признаваться оператором биометрических персональных данных.

Примечания

1. Beamish B. Multiple data owners: who's doing what with your data? // University of Southampton. URL: http://eprints.soton.ac.uk/356026/1/356026.pdf (дата обращения 05.08.2016).

2. Data Protection Principles for the 21st Century: revising the 1980 OECD Guidelines // Oxford internet institute. URL: http://www.oii.ox.ac.uk/publications/Data_Protection_Principles_for_the_21st_Century.pdf (дата обращения 24.07.2016).

3. Greenleaf G. Asian Data Privacy Laws: Trade & Human Rights Perspectives. Oxford., 2014.

4. Schoehman D. Philosophical dimensions of privacy. Oxford., 1984.

5. Бачило И.Л. Информационное право: учебник. – 5-е изд., перераб. и доп. М., 2016.

6. Законна ли технология FindFace и как себя от нее обезопасить? // Meduza. URL: https://meduza.io/feature/2016/04/27/zakonna-li-tehnologiya-findface-i-kak-sebya-ot-nee-obezopasit (дата обращения 6.08.2016).

7. Интернет видит все: как спастись от слежки через веб-камеру и сервисов по поиску людей по фото // Газета.ru. URL: https://www.gazeta.ru/tech/2016/04/29_a_8204579.shtml (дата обращения 6.08.2016).

8. Приезжева А.А. Федеральный закон «О персональных данных»: научно-практический комментарий. М., 2015.

9. Рассолов И.М. Информационное право: учебник для магистров. – 2-е изд., испр. и доп. М., 2012.

10. РЖД и персональные данные // Блог Артема Агеева. URL: http://www.itsec.pro/2013/03/blog-post_25.html.

11. Савельев А.И. Проблемы применения законодательства о персональных данных в эпоху «Больших данных» (Big Data) // Право. Журнал Высшей школы экономики. 2015.

ТЕРЕЩЕНКО Людмила Константиновна, доктор юридических наук, профессор, заместитель заведующего отделом административного законодательства и процесса Института законодательства и сравнительного правоведения при Правительстве Российской Федерации. 117218, Россия, г. Москва, ул. Большая Черемушкинская, 34. E-mail: adm@izak.ru

Кривогин Максим Сергеевич, аспирант факультета права Национального исследовательского университета «Высшая школа экономики». 109028, Россия, г. Москва, Б. Трехсвятительский пер., 3. E-mail: mkrivogin@yandex.ru

TERESHENKO L. K., doctor of legal sciences, associate professor, the Institute of Legislation and Comparative Law under the Government of the Russian Federation. 34 Bolshaya Cheremushenskaya st, Moscow, Russia, 117218. E-mail: adm@izak.ru

KRIVOGIN M. S., graduate student of faculty of law National research university Higher School of Economics. 3 Bolshoy Trekhsvyatitelskiy pereulok, Moscow, Russia, 109028. E-mail: mkrivogin@yandex.ru