Е.В. Дрючина*

ВОПРОСЫ ПРИМЕНИМОГО ПРАВА ПРИ ТРАНСГРАНИЧНОЙ ПЕРЕДАЧЕ ПЕРСОНАЛЬНЫХ ДАННЫХ. ЕВРОПЕЙСКИЙ ОПЫТ

Ключевые слова: *трансграничная передача персональных данных, применимое право, контролер персональных данных, субъект персональных данных, Евродиректива, коллизионная привязка*.

E.V. Dryuchina. Applicable Law Issues in Transborder Flow of Personal Data. Experience of the European Union

The author examines the problems connected with enaction of choice of law rules regarding transborder flow of personal data into the Russian legislation, reasons dictating difficulties in working out of the unified choice of law rule determining applicable law in transborder flow of personal data and also statutory regulation of these relationships in the European Union. The author examines in details provisions of the Directive 95/46/EC of the Council and the European Parliament on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data determining choice of law rules in transborder flow of personal data from the territory of the Member State to the territory of the foreign State. The author analyzes several versions of the Article 4(1) proposed and considered by the European legislators, connecting factor contained therein. The author also considers other variants of solving this problem proposed by the developers of international acts, estimates their advantages and disadvantages.

Неоднозначность в решении вопроса выбора применимого права при трансграничной передаче персональных данных создает значительные препятствия для заключения контрактов в электронной торговле, а также негативно сказывается на бизнесе компаний, чья деятельность связана с осуществлением передачи персональных данных на территорию иностранного государства. Несмотря на то, что данные вопросы уже не один десяток лет обсуждаются на международной арене, к однозначному выводу так и не удалось прийти.

В настоящей статье рассмотрены проблемы, связанные с выбором применимого права при трансграничной передаче персональных данных, проанализирован опыт регулирования в Европейском Союзе.

Сложность в разработке единой коллизионной нормы, определяющей применимое право при трансграничной передаче персональных данных, обусловлена следующими причинами:

Во-первых, неоднозначностью в определении объема коллизионной нормы. Вопрос квалификации такого понятия, как «трансграничная передача персональных данных» является определяющим на этапе выбора применимого

* Аспирант Московской государственной юридической академии имени О.Е. Кутафина. [elena-dryuchina@mail.ru]

права. Как отмечают многие авторы, прежде чем применить определенную коллизионную норму, необходимо сначала дать оценку фактическим обстоятельствам дела, дать им юридическую квалификацию[1].

Между тем в российском национальном праве этот институт является новым и недостаточно разработанным, и в настоящее время отсутствуют категории, которые бы полностью отражали объем такого понятия, как «трансграничная передача персональных данных».

Во-вторых, в настоящее время также не решена проблема отнесения законодательства о защите персональных данных к сфере публичного либо частного права. Некоторые авторы отмечают, что законодательство о защите персональных данных имеет ту же функцию, что и законодательство о защите прав человека, а также прав потребителей, и служит защите отечественного правопорядка[2].

Если законодательство о персональных данных квалифицировать как отрасль публичного права, то правоприменительные органы обязаны применять к сфере обработки и трансграничной передачи персональных данных исключительно свое право, такой подход исключает применение права иностранного государства. Если же его квалифицировать как отрасль частного права, в этом случае будет возможность применить иностранное право к данной сфере отношений.

В-третьих, сложности вызывает определение коллизионной привязки. Традиционно коллизионные привязки связывают выбор применимого права с географическим местом локализации того или иного события (например, местом регистрации юридического лица, наступления вреда). Что же касается трансграничной передачи персональных данных, то определить критерий выбора применимого права сложно, поскольку зачастую невозможно распознать место наступления вреда либо определить место регистрации оператора персональных данных, имеющего несколько организаций в различных государствах.

Еще одним осложняющим фактором является природа информационных систем связи, в которых осуществляется передача данных. Многие из информационных систем связи охватывают территории нескольких государств и не имеют тесной связи с территорией какого-то одного государства, что для международного частного права является основой для выбора применимого права[3].

Первоначально к вопросу правовой регламентации трансграничного перемещения информации персонального характера на международном уровне обратилась Организация по экономическому сотрудничеству и развитию (ОЭСР), приняв Основные положения о защите неприкосновенности частной жизни и международных обменах персональными данными от 23 сентября 1980 г.[4] (да-

---

[1] См.: Международное частное право: учеб. / отв. ред. Г.К. Дмитриева. 3-е изд., перераб. и доп. М., 2010. С. 138.

[2] См.: *Bing J.* Data Protection, Jurisdiction and the Choice of Law // PLPR 65, 1999.

[3] См.: *Lee A. Bygrave.* Determining Applicable Law Pursuant to European Data Protection Legislation. // Computer Law & Security Report, 2000, volume 16. URL: http://folk.uio.no/lee/oldpage/articles/Applicable_law.pdf .

[4] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

лее – Основные положения). Разработчики Основных положений пришли к следующему выводу: определение одной или нескольких коллизионных привязок является сложным «в случае наличия международной компьютерной сети, при которой в результате широкого распространения, высокой скорости движения данных, а также географически рассеянного местонахождения операций по обработке персональных данных, несколько коллизионных привязок могут использоваться в совокупности…». Более того, выбор подходящего права будет зависеть от наличия в различных государствах «одинаковых правовых концепций и правовых структур, а также обязательств государств соблюдать определенные стандарты защиты персональных данных. В отсутствие данных условий выбор применимого права может производиться при формулировке более гибких принципов, включающих «право наиболее тесной связи» и преследующих цель эффективной защиты собственности и индивидуальных свобод» (Пункт 75 параграфа 22 Основных положений, именуемый «Коллизионные нормы»).

С этой же проблемой столкнулись разработчики Конвенции Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных», принятой в Страсбурге 28 января 1981 г.[5]. Статья 12 данной Конвенции, именуемая «Трансграничные потоки данных личного характера и внутреннее законодательство», не содержит каких-либо критериев выбора применимого права к трансграничной передаче данных.

В 2009 г. уполномоченные органы по охране персональных данных, ученые, а также представители неправительственных организаций со всего мира, возглавляемые испанскими органами, начали работу над международным документом по защите персональных данных с тем, чтобы впоследствии представить его на обозрение и утверждение ООН.

Две основные цели, выдвинутые для создания международных стандартов по охране персональных данных, включали следующее:

« – Преодоление пробелов в защите персональных данных. Отсутствие единообразных стандартов защиты персональных данных во всем мире и отсутствие законов о защите персональных данных в большинстве государств увеличивают риск при обработке персональных данных.

– Облегчение трансграничных потоков данных. Увеличивающееся количество баз данных, являющихся доступными в Интернете по всему миру, означает, что одна и та же обработка данных будет подпадать под действие различных стандартов обработки, что создает для бизнеса неопределенности и возлагает бремя согласования»[6].

---

[5] Конвенция на русском языке опубликована в издании: Сборник документов Совета Европы в области защиты прав человека и борьбы с преступностью. М., 1998. С. 106–114.

Россия подписала Конвенцию 7 ноября 2001 г. (распоряжение Президента РФ от 10 июля 2001 г. № 366-рп), ратифицировала 19 декабря 2005 г. (Федеральный закон от 19 декабря 2005 г. № 160–ФЗ). Конвенция не вступила в силу для России на 5 января 2012 г.

[6] См.: *Kuner C*. An International Legal Framework for Data Protection: Issues and Prospects // Computer Law and Security Review. 2009.

Европейский опыт. Основным документом, регулирующим отношения по трансграничной передаче персональных данных, обязательным для применения государствами–членами Европейского союза, является Директива Европейского парламента и Совета союза от 24 октября 1995 г. № 95/46/ЕС «О защите прав частных лиц применительно к обработке персональных данных и свободном движении таких данных» (далее – Евродиректива)[7]. На практике Евродиректива стала и мировым стандартом, реализуемым неевропейскими странами. Это обусловлено не только универсальностью ее норм, но и тем, что идеи, заложенные в ней, стали результатом анализа накопленного практического опыта применения европейскими странами принципов, установленных ранее подписанными международными документами[8].

Статья 4(1) Евродирективы является первой и на настоящий момент пока единственной нормой, определяющей применимое право при передаче персональных данных на территорию иностранного государства. Данная статья именуется «Применимое национальное право» и содержит нормы, касающиеся исключительно вопроса о том, право какого государства–члена будет применимо к процессу конкретного акта обработки персональных данных:

«Каждое государство должно применять свое законодательство, разработанное в соответствии с данной Директивой, при обработке персональных данных в случаях, когда:

a) обработка происходит при осуществлении деятельности контролера персональных данных на территории данного государства. Если контролер имеет несколько учреждений, осуществляющих деятельность на территории нескольких государств, он должен предпринять необходимые меры для того, чтобы гарантировать, что каждое из его учреждений соблюдает требования национального законодательства;

b) контролер не имеет учреждений на территории государств–членов ЕС, однако осуществляет деятельность в месте, где применяется право государства–члена ЕС в результате действия норм международного права;

c) контролер не имеет учреждений на территории Сообщества и для целей осуществления передачи персональных данных использует оборудование, расположенное на территории государства–члена ЕС, если данное оборудование не используется для целей передачи данных через Сообщество».

В целях применения ст. 4(1) Евродирективы необходимо разделять четыре основных понятия, используемые в ее тексте: «персональные данные», «контролер», «учреждение» и «оборудование».

Под персональными данными согласно ст. 2 Евродирективы понимается любая информация, относящаяся к прямо или косвенно определенному или

---

[7] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data // Official Journal L 281 , 23/11/1995 P. 0031–0050.

[8] См.: *Кучеренко А.В.* О гарантиях прав субъектов при осуществлении трансграничной передачи персональных данных // Информационное право. 2009. № 3(18). С. 14–17.

определяемому физическому лицу (субъекту) персональных данных. Таким образом, данные могут являться «персональными», даже если они способствуют определению лица в совокупности с иными данными.

Под контролером понимается физическое или юридическое лицо, государственный или муниципальный орган, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных. Из этого определения следует, что контролером персональных данных может быть больше, чем одно лицо, а также то, что контролер не обязательно должен обладать персональными данными.

Евродиректива проводит отличие между «контролером» и «оператором» персональных данных. Оператор – это физическое либо юридическое лицо, осуществляющее обработку персональных данных от имени или по поручению контролера. В соответствии с положениями Евродирективы, применимое право определяется местом нахождения именно контролера, а не оператора.

Возвращаясь к понятию «учреждение», необходимо отметить, что Директива не дает определения данному понятию за исключением нескольких положений, изложенных в преамбуле к Директиве. Так, предусмотрено, что критерий места учреждения контролера персональных данных подразумевает «эффективную и реальную деятельность через устойчивые структуры». При этом организационно-правовая форма такой структуры не имеет принципиального значения. Не только головная компания, но и дочернее общество может рассматриваться в качестве контролера персональных данных.

На первый взгляд может показаться, что Евродиректива закрепила критерий инкорпорации для определения применимого права. Между тем такой вывод не является точным. Для того чтобы понять замысел европейского законодателя при формулировке нормы, необходимо обратиться к истории ее разработки.

До принятия Евродирективы в окончательном варианте существовало две редакции ст. 4(1): первоначальный и измененный проекты[9].

Каждая из версий ст. 4(1) Евродирективы отличались друг от друга значительно. В них содержались различные коллизионные привязки, определяющие выбор права, применимого к трансграничной передаче персональных данных.

Так, первоначальный проект ст. 4(1) Евродирективы содержал следующие нормы:

«1. Каждое государство применяет нормы настоящей Директивы:

(a) ко всем файлам, расположенным на территории данного государства;

(b) к контролеру резидента файлов, который использует на территории такого государства файлы, находящиеся в другом государстве, чье законодательство не предоставляет надлежащего уровня защиты, за исключением случайного использования»[10].

---

[9] См.: *Lokkie Moerel*. Back to Basics: When does EU data protection law apply? // International Data Privacy Law Access. 2011.

[10] *Ibid.* P. 4.

В первоначальном проекте статьи привязка связывала выбор применимого права с местом нахождения файлов данных (т.е. использовала принцип территориальности). В целях избежания обхода закона о защите персональных данных Евросоюза, предполагалось, что передача файлов данных на территорию иностранного государства не исключает защиту таких данных, предоставляемую европейским законодательством. Более того, данная норма была нацелена на то, чтобы избежать применения нескольких законов. Государство, на территории которого находились данные, имело обязанность по защите данных в соответствии с нормами европейского законодательства. Остальные государства–члены ЕС не могли контролировать такие данные, поскольку такая защита являлась достаточной для свободного перемещения данных.

В измененном проекте ст. 4(1) Евродирективы содержалась следующая норма:

«1. Каждое государство должно применять свое законодательство, разработанное в соответствии с настоящей Директивой, ко всем случаям обработки персональных данных, при которых:

(a) контролер имеет место нахождения на территории этого государства или находится под его юрисдикцией;

(b) контролер не имеет места нахождения на территории Сообщества, где в целях обработки персональных данных он использует автоматические либо неавтоматические средства, которые расположены на территории такого государства»[11].

Таким образом, в данном проекте в качестве привязки используется уже не критерий места нахождения файлов, а критерий места нахождения контролера.

В пояснительной записке Комиссии ЕС в отношении измененной версии ст. 4(1)(a) Евродирективы содержится следующее указание:

«Целью ст. 4(1)(a) Директивы является стремление избежать две возможные ситуации:

– когда субъект персональных данных остался бы без защиты своих прав, и, в частности, имелась бы возможность обхода закона и лишения его такой защиты;

– когда деятельность, связанная с обработкой одних и тех же персональных данных, подпадала бы под действие законов нескольких государств»[12].

В финальной версии ст. 4(1), изложенной выше, законодатель не использует принцип страны учреждения, и каждому государству–члену предоставляет возможность применять свое собственное право (таким образом, было разрешено одновременное применение законов нескольких государств).

Проанализировав обе версии ст. 4(1) Евродирективы, можно прийти к выводу, что в финальной версии законодатель отказался от привязки к законодательству страны места учреждения контролера[13] и разрешил применение за-

---

[11] *bid.* P. 4–5.

[12] *Ibid.* P. 9.

13 См.: *Peter P. Swire*. Of Elephants, Mice, and Privacy: International Choice of Law and the Internet // (1998) 32 International Lawyer 991, 1007.

конов нескольких государств–членов ЕС. Выбор применимого права зависит от того, производится ли обработка данных «при осуществлении деятельности контролера персональных данных на территории государства».

«Если контролер обработки данных имеет одно или более учреждений в другом государстве, положения Директивы применяются к таким учреждениям; государство, в котором учрежден контролер, должно обязать его «предпринять все возможные меры для того, чтобы гарантировать, что каждое из этих учреждений соблюдает обязанности, установленные национальным правом». Сфера действия этой нормы распространяется далеко за пределы просто определения применимого права. Данная норма также определяет и материально-правовые обязанности контролера»[14].

Немаловажное значение для определения сферы действия ст. 4(1) Евродирективы имеет толкование положений пункта (c). Положения данного пункта определяют экстерриториальное действие Евродирективы (так называемое действие «длинной руки» – *long arm approach*)[15]. Указывая на то, что Евродиректива подлежит применению в случаях, когда «контролер не имеет учреждений на территории Сообщества и для целей осуществления передачи персональных данных использует оборудование, расположенное на территории государства–члена ЕС, если данное оборудование не используется для целей передачи данных через Сообщество», законодатель стремился применить положения Евродирективы даже в случае отсутствия места нахождения контролера на территории государства–члена ЕС.

Преимущества данного критерия заключаются в том, что его применение приводит к достаточно определенному, предсказуемому результату.

Если предприятие имеет место нахождения в более чем одном государстве, то оно должно соблюдать требования законов о защите персональных данных в каждом из этих государств. Данный вывод можно проиллюстрировать на примере.

Так, например, американская головная компания имеет дочернее общество (которое является самостоятельным юридическим лицом) в Нидерландах. Американская головная компания имеет центральную базу данных в США, которая хранит данные как работодателя, так и работников дочернего общества в Нидерландах. Американская головная компания осуществляет обработку большего количества данных, чем необходимо голландской дочерней компании, и определяет средства обработки данных. Таким образом, американская головная компания является соконтролером в отношении голландских работников и данных клиентов центральной системы. Поскольку американская головная компания осуществляет обработку данных голландской дочерней компании, а также обработку данных своих клиентов «в связи с осуществлением деятельности голландской дочерней компании», голландский закон о защите персональных

---

[14] См.: *Ulrich Danmann, Spiros Simitis*. EG-Datenschutzrichtlinie // Nomos Verlagsgesellschaft, Baden Baden 1997. 127-8. P. 23.

[15] См.: *Lokkie Moerel*. Op. cit. P. 12.

данных будет применяться к данной части обработки данных. Оба контролера (американская головная и голландская дочерняя компании) обязаны соблюдать требования голландского закона о защите персональных данных.

Таким образом, проанализировав нормы ст. 4(1) Евродирективы, можно сделать вывод, что основным принципом выбора применимого права при трансграничной передаче персональных данных является не критерий места нахождения контролера данных, а связь деятельности контролера с территорией определенного государства. Евродирективa принимает во внимание не субъекта персональных данных – физическое лицо (его место жительства либо национальность), а контролера персональных данных, его место нахождения и деятельность. Евродирективa создает децентрализацию, которая в большей степени приводит к принципу территориальности, тем не менее решающее значение имеет место обработки контролером персональных данных. Как правило, это имеет положительный результат, гарантирующий субъекту персональных данных защиту его прав своим национальным законом.