ПРАВО ЕВРОПЕЙСКОГО СОЮЗА

Актуальные аспекты правовой защиты персональных данных в Европейском союзе, США и России

Бирюков М.М.[*]

В Европейском союзе высокие стандарты в сфере защиты персональных данных были установлены два десятка лет назад. В дальнейшем в целом ряде европейских правовых источников эти стандарты развивались и дополнялись, и в настоящее время защита персональных данных в соответствии с правом ЕС входит в число основных прав человека. В Евросоюзе доминирует тенденция универсального подхода к защите персональных данных, гармонизации и унификации соответствующих норм права ЕС для всех 28 государств-членов. В сравнении с этим в США принимаются акты, ограничивающие использование персональных данных в отдельных узких сферах (в медицинских документах, кредитных отчетах, видеозаписях и т.д.). В России в области защиты персональных данных выработана обширная правовая база с учетом принципов Конвенции Совета Европы №108 от 28.01.1981 г. В связи с обострившейся во всем мире проблемой терроризма во многих странах усиливаются меры безопасности, увеличивающие возможности правоохранительных органов получать доступ к персональной информации без уведомления пользователей.

Ключевые слова: персональные данные; право ЕС (ДЕС, ДФЕС); США (USA Patriot Act, Акт о свободе США 2015 г., Safe Harbor Privacy Principles); право «на цифровое забвение» в Интернете;

[*] Бирюков Михаил Михайлович – доктор юридических наук, профессор, заведующий кафедрой европейского права МГИМО (У) МИД России. kafedra-ide@mgimo.ru.

Россия – Федеральный закон «О персональных данных» от 27.07. 2006 г. с изменениями 01.09.2015 г.

Под персональными данными понимается любая информация, относящаяся к определенному физическому лицу – субъекту персональных данных и затрагивающая его частную, профессиональную и общественную жизнь.

Основой для европейской концепции защиты персональных данных послужила ст. 8 Конвенции о защите прав человека и основных свобод 1950 г., устанавливающая, что «каждый человек имеет право на уважение его личной и семейной жизни, неприкосновенности его жилища и тайны корреспонденции». В ст. 10 закрепляется основное право на свободу выражения мнения. Это право включает в себя «свободу получать и распространять информацию и идеи без какого-либо вмешательства со стороны государственных органов и независимо от государственных границ».

Позднее, с развитием технического прогресса в области обработки баз данных, стало необходимым более детальное и системное развитие правовой защиты частной жизни.

1. Общие сведения о правовых источниках, регулирующих защиту персональных данных в ЕС

В Европейском союзе всегда уделяли повышенное внимание защите персональных данных (далее также ПНд). Высокие стандарты в этой сфере были установлены два десятка лет назад Директивой 1995 г.[1] Введенная данным актом регламентация развивала и расширяла принципы и положения Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных (№ 108) 1981 г. и во многом стала эталоном для других.

В 1997 г. была принята Директива № 97/66 «Об обработке персональных данных и защите конфиденциальности и личной тайны в сфере электронных коммуникаций», которая дополнила Директиву № 95/46 о защите данных правилами для телекоммуникационного сектора. Позже в 2002 г. была принята ее новая версия – Директива 2002/58/ЕС[2].

В настоящее время согласно Хартии ЕС об основных правах 2000 г. (ст. 8) защита персональных данных в соответствии с правом ЕС входит в число основных прав человека. Лиссабонским договором 2007 г. Хартии придана юридически обязательная сила. О праве на защиту

персональных данных физических лиц также говорится и в ст. 16 Договора о функционировании Европейского союза (ДФЕС). Все это означает, что при осуществлении любого рода деятельности институты ЕС, а также государства – члены Союза обязаны заботиться о защите персональных данных. Таков общий подход.

Как известно, из правил часто бывают исключения. В вопросах защиты ПНд исключения, т.е., например, передача ПНд без согласия заинтересованных лиц, в ЕС обосновываются необходимостью борьбы с терроризмом и транснациональной преступностью. Так, если общее положение о ПНд в п.1 ст. 16 ДФЕС гласит, что «каждый имеет право на защиту относящихся к нему персональных данных», то в заключительном абзаце п.2 ст.16 записано: « Правила, принимаемые на основании настоящей статьи, не наносят ущерба специальным правилам, предусмотренным в статье 39 Договора о Европейском Союзе» (ДЕС). А согласно смыслу ст. 39 ДЕС Совет ЕС может принять решение отступить от общего жесткого подхода защиты данных в целях общественной безопасности, что означает возможность нарушения права на защиту ПНд[3].

Следует отметить, что имеющаяся достаточно совершенная правовая база защиты персональных данных в ЕС была создана до современной «цифровой эры». С ее началом технологические возможности сбора, обработки данных и несанкционированного, незаконного вторжения в частную жизнь с нарушением действующего правового регулирования выросли на несколько порядков, что, например, доказывают разоблачения Э. Сноудена.

2. О различиях в подходах ЕС и США к проблеме защиты ПНд

ЕС и США имеют разные подходы к защите персональных данных. В последнее время стороны пытаются преодолеть этот разрыв.

Принципиальная юридическая разница в подходах состоит в том, что в США принимаются внутригосударственные акты, ограничивающие использование персональных данных американцев в отдельных узких сферах (в медицинских документах, кредитных отчетах, видеозаписях и т.д.). В то же время на практике данные сервисов, принадлежащих американским компаниям, передаются властям США без уведомления самих пользователей. Правовой основой для такой практики послужил USA Patriot Act (Законодательный акт о патриотизме

(или Патриотический акт)) от 2001 г.[4] Этот закон позволил американским правоохранительным органам получить доступ к любой личной информации клиентов американских электронных компаний без уведомления пользователей.

Европейский союз, в свою очередь, следует тенденции универсального всеобъемлющего подхода, гармонизации и унификации права ЕС для всех 28 государств-членов. Он стремится реализовывать общие принципы сбора личной информации граждан ЕС, впервые сформулированные еще в выше упоминавшейся директиве 1995 г. Данная директива 95/46/ЕС, например, гарантирует гражданам Союза право на получение в организациях и компаниях копий документов, содержащих персональные данные о них, чего пока нет в США.

В то же время, по заявлению главного советника Министерства торговли США, курирующего вопросы защиты ПНд, Камерона Ф. Керри, «сумма форм защиты частной жизни в США равна или больше, чем одна форма во всем Европейском союзе». Таким образом, американская сторона настаивает на том, что, несмотря на различия в подходах сторон, окончательные результаты на сегодня равны.

Некоторое время назад Европейская комиссия[5] (ЕК) предложила комплексные реформы по укреплению для граждан Евросоюза права на частную жизнь в Интернете, которые должны пройти обсуждение в Европейском парламенте и Совете ЕС. Так, например, согласно новым реформам утверждается право каждого пользователя Интернетом в ЕС на «цифровое забвение»[6]. Реализация данной инициативы предполагает, что поисковые системы и социальные сети обязуются удалять видео, фото и иную информацию по первой просьбе пользователей Интернетом в ЕС.

Недавно в СМИ появилась информация о том, что на одном из саммитов ЕС будет рассмотрен вопрос о принятии нового акта (или актов) о защите персональных данных. Такие законопроекты могут быть включены в пакет готовящегося европейского законодательства в рамках совершенствования правового регулирования единого внутреннего рынка. Предполагается, что этот пакет, включающий обновленное законодательство по защите ПНд, будет принят в 2016 г.

Американские технологические компании и торговые группы, в том числе работающие в Европейском союзе, выступают против отдельных положений европейских реформ, считая их слишком жесткими, и ратуют за «свободный Интернет», наиболее благоприятный

для электронной торговли. Против «чрезмерно широкого регулирования» в Интернете, в частности, выступают торговые группы, представляющие интересы американских корпораций Google, Microsoft, Facebook и др.

Стремясь нейтрализовать упреки европейцев о недостаточной защищенности персональных данных в США, еще в 2012 г. президентом Б. Обамой был предложен проект «Билля о праве потребителей на конфиденциальность» (Consumer Privacy Bill of Rights), который усиливает эту защиту, приближая ее к нормам, содержащимся в проекте реформ, над которым ведется работа в ЕС. Например, американский проект включает право на доступ к записям, содержащим персональные данные, которые принадлежат компаниям, право на исправление этих записей и право ограничения личных данных, которые компании могут собирать и хранить.

3. Отношения ЕС и США в области защиты и передачи персональных данных

В 2000 г. между Европейской комиссией и Министерством торговли США были выработаны соответствующие принципы и заключено соглашение, именуемое Safe Harbor Privacy Principles (далее Safe Harbor или « безопасная гавань»), которое позволяло американским компаниям, отвечающим требованиям законодательства ЕС, передавать американским властям личные данные европейцев. Такие компании должны информировать лиц, данные которых передавались, о том, в каких целях это делается. Посторонние не должны иметь доступ к этим данным. Организации, находящиеся в США, могли проводить самостоятельную сертификацию на соответствие принципам Safe Harbor, в общих чертах, как предполагалось, совпадающим с требованиями законодательства ЕС. Смысл Safe Harbor также состоял в том, что американские компании, работающие с информацией о гражданах ЕС, могли добровольно взять на себя обязательство соблюдать европейские требования по защите ПНд. Тем самым законодательство ЕС могло применяться к американским компаниям в условиях своего рода правовой «безопасной гавани». Чтобы получить право передавать данные из ЕС в США на законных основаниях, организация, находящаяся в США, должна была заверить общественность в том, что она обязуется придерживаться принципов соглашения Safe Harbor, соответствующих правилам ЕС в отношении

конфиденциальности данных. Такая организация (например, корпорация Майкрософт) ежегодно проходила сертификацию на соответствие Safe Harbor. По разным данным, подобных американских компаний насчитывается от 3000 до 4500.

Наряду с ЕС организации, сертифицированные по программе Safe Harbor, признаются и другими странами Европейского экономического пространства (Исландия, Лихтенштейн, Норвегия), а также Швейцарией[7]. Другими словами, указанные государства признают организации, сертифицированные на принципы Safe Harbor, как обеспечивающие достаточный уровень конфиденциальности для передачи данных из этих стран в США. Не входящая в ЕС Швейцария заключила с США аналогичное соглашение Safe Harbor.

Компетентными органами Евросоюза разрешена также свободная передача данных из ЕС в Канаду, Аргентину и некоторые другие страны, принявшие, по мнению ЕС, удовлетворяющие требованиям законодательства Союза соответствующие национальные законы о конфиденциальности данных.

Между ЕС и США подписаны два узких «секторных» соглашения, касающиеся защиты персональных данных:

• двустороннее соглашение (ратифицировано весной 2012 г.), на основе которого Евросоюз предоставляет американцам информацию об авиапассажирах. Соглашение было подписано по инициативе американской стороны в связи с терактом 11 сентября 2001 г., и его подготовка заняла более 10 лет;

• соглашение об обмене финансовой информацией, т. е. о передаче персональных данных, касающихся финансовых транзакций, известное как соглашение СВИФТ (SWIFT) от 28 июня 2010 г. Срок действия – пять лет с возможностью ежегодного продления и прекращения действия по требованию одной из сторон. Соглашение разрешает доступ американской стороне к данным международной системы межбанковских платежей при проведении антитеррористических расследований.

Следует отметить, что сторона ЕС не раз угрожала США пересмотреть режим применения указанных соглашений либо вовсе заморозить их применение. Каждый раз это было связано с информацией о злоупотреблениях американской стороной персональными данными европейцев. Например, такие предложения звучали в Европарламенте в июле 2013 г. в связи с разоблачениями Э. Сноудена.

Отметим, что до недавних пор подобные угрозы европейцев ни разу не были реализованы и никак не сказывались на высоком уровне сотрудничества ЕС с заокеанским партнером.

В 2009 г. по инициативе Европейского парламента Еврокомиссия начала проработку вопроса о заключении с США более широкого, чем «секторные», соглашения о защите персональных данных при осуществлении сотрудничества по борьбе с терроризмом и организованной преступностью.

4. О последствиях разоблачений Э. Сноуденом деятельности специальных служб США в Интернете

Бывший сотрудник американских спецслужб Эдвард Сноуден среди прочего обнародовал информацию об американской программе слежения Призм (PRISM), суть которой заключается в мониторинге и хранении максимальной информации из Интернета, участии в этом поисковых систем и социальных сетей, в сотрудничестве с американскими спецслужбами их европейских партнеров под предлогом совместной борьбы с международным терроризмом. Согласно Сноудену, американские компании, такие, например, как Фейсбук и Майкрософт поставляли данные американскому Агентству национальной безопасности (АНБ).

По информации Сноудена, ЦРУ и АНБ также умеют обходить все средства криптографической защиты информации в Интернете. В результате спецслужбы получают доступ к коммерческой тайне многих компаний, а также к частной переписке в Интернете.

В связи со шпионским скандалом, например, украинские власти обвинили в июле 2013 г. поисковики Google («Гугл Украина»), Gemius и социальную сеть «ВКонтакте» в нарушении закона о защите ПНд и пригрозили Google штрафом. Украинская сторона также поставила вопрос о необходимости подписания с США соглашения о защите ПНд, подобного Safe Harbor.

В июне и августе 2013 г. член Совета Федерации Федерального собрания России Руслан Гаттаров инициировал претензии к компаниям Google, Yahoo, Facebook, Skype, Apple и Twitter, обвинив последние в причастности к секретной американской программе Призм и в нарушениях российского законодательства и международных норм (конкретно Конвенции Совета Европы № 108), касающихся защиты персональных данных пользователей.

Разоблачения Сноудена активизировали разработку Брюсселем серии дополнений и изменений в законодательстве ЕС о доступе к персональным данным. Цель их принятия – воспрепятствовать американским электронным компаниям, действующим в Европе, свободно отслеживать информационные потоки в Интернете, как они это делали до сих пор.

Руководство Евросоюза в том числе под давлением пользователей Интернетом – граждан ЕС делает попытку переподчинить деятельность американских технологических гигантов законодательству ЕС, взять ее под контроль, запретить доступ третьих стран к персональным данным граждан Союза без согласия контролирующего органа ЕС[8] или государств-членов. Европейцы также стремятся получить доступ ко всем собираемым американскими партнерами в сетях разведданным. В этом плане возникла угроза для существования всей американской программы Призм. Технически замысел европейцев состоит в том, чтобы заставить американские компании установить отдельные серверы в Европе, от чего раньше американская сторона всячески уклонялась.

Информация, обнародованная Эдвардом Сноуденом, о том, что АНБ шпионило не только за простыми гражданами ЕС, но и некоторыми европейскими лидерами, вызвала в Евросоюзе резкую критику соглашения Safe Harbor. В октябре 2015 г. Суд ЕС признал недействительным данное соглашение, отметив, что американское законодательство в области защиты ПНд имеет более низкие стандарты, чем право ЕС, поэтому Евросоюз может запретить хранение данных своих граждан на серверах в США. Суд пришел к выводу, что персональные данные граждан Союза недостаточно надежно защищены и могут оказаться в распоряжении американских спецслужб.

5. Проблемы, существующие между Россией и ЕС в области защиты персональных данных

Руководство Европейского союза традиционно критически оценивает ситуацию с правами человека в Российской Федерации, в том числе считая недостаточной защиту персональных данных физических лиц.

В Российской Федерации правовое регулирование защиты персональных данных осуществляется как на законодательном уровне, так и с помощью актов подзаконного регулирования. К настоящему моменту выработана обширная правовая база, включающая как общие

модели регулирования, так и регламентацию оборота персональных данных в отдельных областях, в том числе дифференцированные организационные и технические требования к защите информационных систем персональных данных в зависимости от уровня угроз.

Функции контроля и надзора в области защиты персональных данных возложены на Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

Основы правового регулирования оборота персональных данных в РФ закреплены в Федеральном законе от 27.07.2006 № 152-ФЗ «О персональных данных». С 1 сентября 2015 г. действует новая редакция этого закона, согласно которой электронные компании обязаны обрабатывать и хранить персональные данные российских граждан исключительно в России. Крупные компании, занимающиеся обработкой персональной информации россиян, заявили о готовности к новым правилам работы.

Общая концепция ФЗ «О персональных данных» была выработана с учетом принципов Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных № 108 от 28 января 1981 г. с поправками от 15 июня 1999 г. (далее также Конвенция).

Конвенция № 108 подписана почти всеми государствами – членами Совета Европы (46 странами из 47), из них, в том числе всеми 28 государствами – членами ЕС и Россией.

Данная Конвенция вступила в силу на территории России 1 сентября 2013 г. Ратифицировав Конвенцию, Россия тем самым взяла обязательство обеспечить выполнение требований к защите персональных данных личности, закрепляемых этим международным договором.

В связи с обострившейся во всем мире проблемой терроризма, в РФ был принят ФЗ от 09.02.2007 № 16-ФЗ «О транспортной безопасности». В соответствии с данным актом, и основываясь на принципе баланса интересов личности, общества и государства, в России предусматривается создание единой государственной информационной системы обеспечения транспортной безопасности, включающей автоматизированные централизованные базы персональных данных о пассажирах (ст. 11) В соответствии с п. 4 ст. 11 ФЗ «О транспортной безопасности», эти данные объявлены информацией ограниченного доступа.

В целях информационного обеспечения безопасности на воздушном транспорте, данным актом предусматривается передача

авиаперевозчиками в автоматизированные централизованные базы определенных персональных данных пассажиров.

Приказом Министерства транспорта РФ от 19.07 2012 № 243[9] установлены порядок, сроки и технические требования к передаче персональных данных пассажиров и членов экипажей, а также данных об их багаже, ручной клади, регистрации на рейс и явке к вылету. Приказ Минтранса РФ № 243 является актом, изданным в целях реализации положений ФЗ «О транспортной безопасности».

Казалось бы, можно утверждать, что в соответствии со ст. 6 Конвенции СЕ № 108 и ст.10 ФЗ «О персональных данных», персональные данные пассажиров и членов экипажей, запрашиваемые Минтрансом России, не входят в перечень «особо чувствительной» информации (то есть той, несанкционированное использование и распространение которой может нанести наибольший вред субъекту персональных данных). Перечень запрашиваемой информации отвечает требованиям ст. 5 Конвенции СЕ № 108, то есть: сведения собираются добросовестно и законно, накапливаются для точно определенных и законных целей и не являются избыточными. Статья 9 Конвенции ЕС № 108 предусматривает возможность установления сторонами Конвенции изъятий из общих правил защиты персональных данных с целью обеспечения общественной безопасности. Согласно п. 2 ст. 12 Конвенции ЕС № 108, стороны не имеют права запрещать передачу персональных данных на территорию другой Стороны Конвенции (каковой является Россия) с единственной целью защиты неприкосновенности личной сферы.

Исходя из выше изложенного, правомерно считать, что нормы Приказа Минтранса № 243, не нарушали общих требований законодательства ЕС о защите персональных данных и могли быть применены вплоть до урегулирования данного вопроса путем заключения двусторонних международных договоров между Россией и ЕС либо между Россией и отдельными государствами – членами ЕС как сторонами Конвенции № 108. В данном случае автор данной статьи исходит из того, что защита персональных данных является составным элементом общего большого проекта ЕС – создания Пространства свободы, безопасности и правосудия, реализация которого является не исключительной компетенцией Евросоюза, а совместной компетенцией, т.е. Союза и государств-членов. Добавлю, что вопросы защиты ПНд сторонам целесообразно обсуждать в рамках реализации положений дорожной карты

2005 г. о создании между РФ и ЕС общего Пространства свободы, безопасности и правосудия.

По оценкам стороны ЕС, в связи с Приказом Минтранса РФ возникла юридическая коллизия, когда европейская сторона не могла выполнить требование российских властей, не нарушив норм права Евросоюза о защите персональных данных.

Основываясь на жестких нормах права ЕС, регулирующих защиту персональных данных, Евросоюз настаивал на исключении европейских авиаперевозчиков из-под действия требований данного Приказа. Это выразилось в том, что Союз попросил российскую сторону ввести бессрочный мораторий на приказ Минтранса в отношении ЕС. По данным Евросоюза, данный ведомственный акт затрагивал интересы более 19 млн. пассажиров европейских авиакомпаний ежегодно, большая часть которых осуществляет беспересадочный перелет над территорией РФ из Европы в страны Азии.

Уступая просьбе ЕС, Москва перенесла дату вступления в силу по отношению к Евросоюзу выше указанного приказа Минтранса РФ.

Topical Aspects of the Legal protection of Personal Data in the European Union, the United States and Russia
(Summary)

Mikhail M. Birukov[*]

In the European Union the highest standards in the field of personal data protection were established two decades ago. Going forward, in a number of European legal sources, these standards have been developed and supplemented, and now the protection of personal data in accordance with EU law is among the fundamental Human Rights.

The EU is dominated by the trend of a universal approach to the protection of personal data, the harmonization and unification of the relevant rules of EU law for all 28 Member States. In comparison, the United States

[*] Mikhail M. Birukov – Doctor of Laws, professor, head of the Chair of European Law, MGIMO-University MFA Russia. kafedra-ide@mgimo.ru.

has been adopting laws restricting the use of personal data in certain narrow areas (in the medical records, credit reports, video records, etc.)

In Russia an extensive regulatory framework has been developed in the field of personal data protection taking into account the principles of the Council of Europa Convention №108 as of 28.01.1981. Due to the escalating and aggravating global issue of terrorism many countries have enhanced the security measures that increase the ability of law enforcement to access personal information without notifying the users

***Keywords*:** Personal data; the Law of the EU (TEU, TFEU); United States (USA Patriot Act, the Act on the freedom of the United States in 2015, Safe Harbor Privacy Principles); right to digital "oblivion" in the Internet; Russian Federal Law "On personal Data" as of 27.07.2006 with amendments of 01.09.2015.

[1] Директива 95/46/ЕС Европейского парламента и Совета от 24 октября 1995 г. о защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных.

[2] Действует с изменениями и дополнениями, принимавшимися в 2006 и 2009 г.

[3] События 13-14 ноября в Париже подтверждают обоснованность включения такой нормы в учредительный акт ЕС.

[4] Срок действия «Патриотического акта» закончился 01 июня 2015 г. Его сменил т.н. «Акт о свободе США», лишь немногим ограничивший полномочия американских спецслужб по прослушиванию телефонных разговоров и контролю за электронной почтой граждан США и других государств.

[5] Инициатор – г-жа Вивиан Рединг (Viviane Reding), заместитель председателя ЕК предыдущего состава.

[6] В другой редакции – «право быть забытым», т.е. возможность удалить все свои ПНд из глобальной сети Интернет.

[7] Все эти четыре государства – не члены в ЕС, но они входят в шенгенское пространство.

[8] Европейский контролер по защите данных (European Data Protection Superviser).

[9] Приказ Министерства транспорта РФ № 243 от 19 июля 2012 г. «Об утверждении Порядка формирования и ведения автоматизизированных централизованных баз персональных данных о пассажирах, а также предоставления содержащихся в них данных».