ГОСУДАРСТВО И ПРАВО, 2017, № 6, с. 70–78

ПРАВО И ИНФОРМАТИКА

ОПЫТ ПРАВОВОГО ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ВЕЛИКОБРИТАНИИ[1]

© 2017 г. Анна Константиновна Жарова[2]

Аннотация: *проведен правовой анализ опыта Великобритании в обеспечении безопасности персональных данных и изучены подходы к определению персональных данных. В статье обобщена нормативная система Великобритании в области обеспечения безопасности персональных данных. Рассмотрены Закон Великобритании о защите данных 1998 г. и законодательные инициативы, направленные на обеспечение безопасности персональных данных в сети Интернет.*

Abstract: *the legal analysis of the UK experience in ensuring the security of personal data lets make the conclusions about the strengths and weaknesses of the Russian legislation in the field. In the article summarized the UK regulatory system in the field of security of personal data. The UK Data Protection Act 1998 and legislative initiatives aimed at ensuring the security of personal data on the Internet were studied.*

Ключевые слова: *персональные данные, Великобритания, Россия, правовое регулирование.*

Key words: *personal data, United Kingdom, Russia, the legal regulation.*

Информация, несущая в себе данные о личной, индивидуальной или семейной жизни человека, обладает особой ценностью. Конституция РФ закрепляет основной принцип современного демократического общества: "Человек, его права и свободы являются высшей ценностью" (ст. 2). Права человека в Великобритании изложены в общем праве, которые основаны на Билле о правах 1689 г.[3] Информация, затрагивающая частные интересы человека, должна уважаться и защищаться государством.

Однако в условиях Интернета зачастую происходят правонарушения, связанные с обработкой персональных данных, не соответствующей целям, заявленным операторами персональных данных (по российскому законодательству) или контроллерами данных (по законодательству Великобритании). Например, поисковые системы собирают информацию обо всех действиях своих пользователей, осуществляемых в Интернете без их согласия, и в дальнейшем эту информацию используют для рассылки рекламы или предоставления дополнительных услуг. Свои действия поисковые системы обосновывают тем, что информация о совершаемых действиях пользователей не относится к персональным данным. Указанное правонарушение происходит на территории как России, так и Великобритании[4]. В этой связи задача настоящей статьи состоит в привлечении внимания к решению вопроса об определении персональных данных.

Понятие "персональные данные" в соответствии с законодательством Великобритании

В Великобритании правовое регулирование неприкосновенности частной жизни лица и его персональных данных осуществляется на национальном и универсальном уровне. Великобритания – член Совета Европы, подписавшая и ратифицировавшая Конвенцию "О защите частных лиц в отношении автоматизированной обработки персональных данных"[5] вместе с Европейской конвенцией "О защите прав и основных свобод человека"[6]. Среди обязательных документов в том числе Директива "О защите персональных данных 95/46/ЕС"[7].

[1] Статья подготовлена по гранту РГНФ № 16-03-00679. Тема "Сравнительно-правовое исследование методов обеспечения информационной безопасности в Российской Федерации и странах – членах ЕС".

This article was prepared for grant № 16-03-00679-SRF. Theme "Comparative legal research of the methods of information security in the Russian Federation and EU Member States".

[2] Старший научный сотрудник сектора информационного права Института государства и права РАН, доцент кафедры инноваций и бизнеса в сфере ИТ Национального исследовательского университета "Высшая школа экономики", кандидат юридических наук, доцент (E-mail: anna_jarova@mail.ru).

Anna Zharova, senior research fellow of the sector of Information Law, associate Professor of innovation and business in the IT of the National Research University "Higher School of Economics", PhD in Law, associate Professor (E-mail: anna_jarova@mail.ru).

[3] См.: The English Bill of Rights// http://www.parliament.uk/about/living-heritage/evolutionofparliament/parliamentaryauthority/revolution/collections1/collections-glorious-revolution/billofrights/

[4] См.: *Елин В. М., Жарова А. К.* О выделении информационных объектов в самостоятельную категорию объекта преступления // Труды ИГП РАН. 2009. № 5. С. 205–229.

[5] См.: Convention for the protection of individuals with regard to automatic processing of personal data (ETS N 108) (Strasbourg, 28 January 1981) // http://www.conventions.ru/view_eng.php?id=1097

[6] См.: European Convention for the Protection of Human Rights and Fundamental Freedoms //http://ec.europa.eu/justice/data-protection/law/

[7] См.: EU Data Protection Directive (Directive 95/46/EC) // http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/

Великобритания, являясь членом Организации по экономическому сотрудничеству и развитию (ОЭСР), выполняет требования Директивы ОЭСР "О защите неприкосновенности частной жизни и международных обменов персональными данными" от 23 сентября 1980 г.[8]

Среди основных нормативных актов национального уровня, которые регламентируют вопросы защиты персональных данных в стране, можно назвать следующие: Закон о защите данных 1998 г. *(Data Protection Act 1998)*[9]; Закон о свободе информации *(Freedom of Information Act 2000)*[10]; Закон о защите свобод 2012 г. *(The Protection of Freedoms Act 2012)*[11], включающий положения об уничтожении, удалении и использовании биометрических данных, а также дополнения к данному Акту, касающиеся передачи данных *(Amendment) (No. 2) Order 2013)*; Кодекс об уголовных преступлениях *(The Criminal Justice and Data Protection (Protocol No. 36) Regulations 2014)*[12]; Регламент о свободе информации и защите данных (необходимые ограничения и штрафы) *(The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004)*[13].

Закон о защите данных 1998 г., принятый во исполнение Директивы 95/46/ЕС[14], разделяет понятия "данные" и "персональные данные". Под "данными" в указанном Законе понимается информация, которая обрабатывается и записывается с помощью автоматизированного оборудования и является частью соответствующей системы или является записью, находящейся в распоряжении государственного органа.

Обратим внимание на то, что данный Закон понимает под информацией содержательную характеристику данных. Это вытекает из трактовки понятий "использование", "раскрытие", "получение" и "запись", которые даются в Законе. Так, под "использованием" или "раскрытием" персональных данных понимаются использование или раскрытие информации, содержащейся в данных. Под "получением" или "записью" персональных данных подразумеваются получение или запись информации, которая связана с персональными данными (ч. 1 ст. 2). Однако само понятие "информация" Закон не раскрывает, но использует другие термины, непосредственно связанные с осуществлением действий над информацией. Согласно Закону о защите данных 1998 г. предусматриваются следующие действия: получение, запись или сохранение информации или данных; в том числе проведение какой-либо операции или набора операций с этими данными или информацией, в том числе в случае организации, адаптации или изменении их, в случаях поиска, консультации или использования; раскрытия путем их передачи, распространения или совершение иных действий, которые делают эти данные или информацию доступными; а также комбинирование, блокирование, стирание или уничтожение информации или данных.

"Персональные данные" вышеуказанный Закон определяет как любые данные, которые относятся к живому человеку и на основании которых этот человек может быть идентифицирован, или информацию, которая находится в распоряжении контроллера данных или может ему поступать для обработки, в том числе любое выражение мнения об индивидуальных особенностях человека или его личности (ч. 1 ст. 1). Закон о свободе информации 2000 г. относит к персональным данным любой информационный запрос, представляющий собой информацию о субъекте персональных данных (п. 40 ч. II).

Кроме Закона о защите данных 1998 г. и Закона о свободе информации 2000 г. обработку персональных данных регулирует Акт о свободах *(Freedoms Act 2012)*. Однако к персональным данным имеет отношение только гл. 1 данного Акта, регулирующая вопросы уничтожения, сохранения и использования отпечатков пальцев, обуви и образцов ДНК-профилей, полученных в ходе расследования уголовного дела. В соответствии с указанным Актом отпечатки пальцев и ДНК-профили, полученные от арестованных лиц, подлежат уничтожению в случае оправдательного приговора.

Защита персональных данных в уголовном процессе осуществляется на основании Уголовного кодекса *(The Criminal Justice and Data Protection (Protocol No. 36) Regulations 2014)*.

Основным субъектом обеспечения конфиденциальности персональных данных в Великобритании является контроллер данных – лицо, которое (самостоятельно или совместно с другими

---

dirl995-46_part1_en.pdf

[8] См.: Основные положения Организации по экономическому сотрудничеству и развитию (ОЭСР) "О защите неприкосновенности частной жизни и международных обменов персональными данными" // http://www.uipdp.com/upload/legislation/international/directive_oesrl.pdf

[9] См.: http://www.legislation.gov.uk/ukpga/1998/29/contents

[10] См.: http://www.legislation.gov.uk/ukpga/2000/36/contents

[11] См.: http://www.legislation.gov.uk/ukpga/2012/9/contents/enacted

[12] См.: http://www.legislation.gov.uk/ukdsi/2014/9780111122723/contents

[13] См.: http://www.legislation.gov.uk/uksi/2004/3244/pdfs/uksi_20043244_en.pdf

[14] См.: EU Data Protection Directive (Directive 95/46/EC) // http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dirl995-46_part1_en.pdf

лицами) определяет цели и средства обработки персональных данных (п. 1. ч. 1 Закона о защите данных 1998 г.). Вместе с тем если контроллер данных привлекает для обработки третье лицо – обработчика данных (не являющегося сотрудником контроллера данных), который обрабатывает персональные данные от имени контроллера данных, то обработчик данных несет такую же ответственность за обеспечение конфиденциальности персональных данных, как и контроллер. Обработка данных возможна, если контроллер данных (информации) принимает разумные меры для обеспечения соблюдения требований указанного Закона о безопасности и надежности систем.

Субъект персональных данных имеет право самостоятельно определять, как, кому и на каких условиях предоставлять данные. Соответственно, нормативно установленных обязанностей по обеспечению конфиденциальности персональных данных у субъекта персональных данных нет.

Департамент правительства Великобритании по делам культуры, СМИ и спорта (DCMS) взял на себя ответственность за формирование политики защиты данных[15].

Мы можем наблюдать разницу в понимании "информации" в российском законодательстве и законодательстве Великобритании. В Федеральном законе "Об информации, информационных технологиях и о защите информации" от 27 июля 2006 г.[16] (далее – Федеральный закон об информации) информация определена как "сведения (сообщения, данные) независимо от формы их представления" (ст. 2). Закон о защите данных 1998 г. данные определяет как информацию, которая связана с технологическими процессами, или как запись, находящуюся в распоряжении государственного органа.

Однако можно найти сходство в подходах[17] к персональным данным и частной жизни лица российского Закона и Закона Великобритании. Так, в российском законодательстве связь информации о частной жизни лица с персональными данными определена Указом Президента РФ от 6 марта 1997 г. № 188[18], в соответствии с которым персональные данные – это "сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях" (п. 1). Персональные данные Законом о защите данных 1998 г. определены как любые данные, в том числе и любое выражение мнения об индивидуальных особенностях человека или его личности (ч. 1 ст. 1).

В данном случае мы можем отметить общую проблему: объединение понятий "персональные данные" и "личная информация" или "частная жизнь лица". С одной стороны, защита частной жизни лица включает защиту сведений, составляющих некоторую частную тайну лица, которую субъект не желает раскрывать перед третьими лицами. С другой – "персональные данные являются особым институтом охраны права на неприкосновенность частной жизни"[19]. С третьей стороны, персональные данные могут содержать информацию, которая известна третьим лицам, в том числе общедоступные персональные данные, и в этой связи тайной уже не может являться.

Закон о защите данных 1998 г. разделяет понятия "конфиденциальные персональные данные"[20] и "персональные данные". Под "конфиденциальными персональными данными" понимается разновидность персональных данных, к которым относится следующая информация: а) о расовом или этническом происхождении субъекта данных; б) о политических взглядах; в) о религиозных убеждениях или иных убеждениях аналогичного характера; г) о том, является ли человек членом профсоюза; д) о физическом или психическом здоровье человека или его состоянии; е) о его сексуальной жизни; ж) о совершенном или предполагаемом к совершению человеком какого-либо преступления; з) о любых процедурах, связанных с преступлениями, совершенными или совершаемыми, в том числе о решениях по таким разбирательствам или о приговорах любого суда по такому делу.

Вышеуказанные термины схожи с российскими терминами "персональные данные" и

[15] См.: DCMS takes on responsibility for UK data protection policy and sponsorship of the ICO. 18 сентября 2015 г. // http://www.out-law.com/en/articles/2015/september/dcms-takes-on-responsibility-for-uk-data-protection-policy-and-sponsorship-of-the-ico/

[16] См.: Собрание законодательства РФ. 2006. № 31 (Ч. 1). Ст. 3448.

[17] См.: *Бачило И. Л., Сергиенко Л. А., Кристальный Б. В., Арешев А. Г.* Персональные данные в структуре информационных ресурсов. Основы правового регулирования // Информационное право. 2006. № 3. С. 48.

[18] См.: Указ Президента РФ "Перечень сведений конфиденциального характера" от 6 марта 1997 г. // Гарант.

[19] *Бачило И. Л.* Информационное право. Основы практической информатики. Учеб. пособие. М., 2001.

[20] В Законе используется термин "*sensitive personal data*", который переводится на русский язык в том числе и как конфиденциальные данные. В ч. 1 данного Закона к *sensitive personal data* отнесены перечисленные в абзаце категории информации. Дословно, как указано в Законе 1998 г.: "In this Act "sensitive personal data" means personal data consisting of information as to...".

"специальные категории персональных данных" в соответствии с Федеральным законом "О персональных данных" от 27 июля 2006 г.[21], а также с формой открытых данных, относящихся к общедоступной информации (ст. 7 Федерального закона об информации).

Обеспечение безопасности персональных данных

Закон о защите данных 1998 г. определяет, что персональные данные должны обрабатываться только в целях, соответствующих Закону и определенных контроллером данных. Цели должны соответствовать принципам обработки информации – "справедливости и законности", которые связаны с обязательным наличием согласия субъекта на обработку его данных, а также с необходимостью обработки, заявленной "контроллером данных" для определенных случаев[22]. В соответствии с п. 4 разд. 1 данного Закона к специальным целям относятся: цели журналиста, художественные цели и литературные цели.

Как отмечает И.Л. Бачило, "в ряде стран введены независимые уполномоченные по защите персональных данных, во всех странах Европейского Союза с 1998 г. создана единая унифицированная система защиты персональных данных, в том числе в секторе телекоммуникаций"[23]. Для обеспечения безопасности обработки персональных данных Закон о защите данных 1998 г. предусматривает создание правового института "Комиссар персональных данных" (название должности можно перевести и как Уполномоченный по персональным данным) (далее – Комиссар). Комиссар является независимым должностным лицом, назначаемым Её Величеством, ему выдается патент. Однако Комиссар и его должностные лица и сотрудники не рассматриваются как служащие или агенты Короны. Основное направление его деятельности – это отстаивание информационных прав в общественных интересах и содействие открытости государственных органов и конфиденциальности данных для физических лиц. Функции Комиссара определены ч. VI Закона о защите данных 1998 г.

Кроме того, Закон о защите данных 1998 г. в целях обеспечения безопасности передаваемых данных содержит требование об обязательной *обработке персональных данных на территории страны* вне зависимости от того, предназначается ли информация для технологической обработки или является частью системы. И только *после выполнения данного требования и требования о принятии контроллером данных разумных мер для обеспечения соблюдения Закона о защите данных 1998 г. информация может быть передана за пределы Европейской экономической зоны.* Предусмотрено, что данные не могут быть обработаны с помощью третьей стороны, если последняя не предоставит достаточных гарантий относительно технической и организационной безопасности.

Обработка осуществляется на основании письменного договора с субъектом персональных данных и только по поручению контроллера или в рамках выполнения обязательств, эквивалентных тем, которые накладываются на контроллера данных в соответствии с Законом 1998 г.

Управление Комиссара (ICO) является государственным органом исполнительной власти по защите данных в Великобритании, которое подчиняется непосредственно парламенту при поддержке министерства юстиции.

Кратко представить функции Комиссара можно следующим образом: если у Комиссара есть основания предполагать, что действия контроллера данных противоречат или нарушают какие-либо принципы защиты данных, то Комиссар может

[21] См.: СПС "КонсультантПлюс".

[22] 1. Для исполнения договора, по которому субъект персональных данных является одной из сторон; для цели заключения договора в соответствии с распоряжением субъекта персональных данных. В случае, если обработка необходима для защиты жизненно важных интересов субъекта данных, для осуществления правосудия.
2. Персональные данные должны быть получены только для одной или нескольких определенных и законных целей и не подлежат дальнейшей обработке в целях, несовместимых с заявленной целью.
3. Персональные данные должны быть адекватны и нечрезмерными по отношению к тем целям, для которых они обрабатываются.
4. Персональные данные должны быть точными и актуальными.
5. Персональные данные, обработанные в соответствии с заявленными целями, не должны храниться дольше, чем это необходимо для целей.
6. Персональные данные должны быть обработаны в соответствии с правами субъектов данных согласно настоящему Закону.
7. Технические и организационные меры защиты данных должны быть приняты против несанкционированной или незаконной обработки персональных данных, а также от случайной потери, уничтожения или повреждения персональных данных.
8. Персональные данные не могут быть переданы в страну или на территорию за пределами Европейской экономической зоны, если эта страна или территория не обеспечивают достаточный уровень защиты прав и свобод субъектов данных в отношении обработки персональных данных (см.: Приложение к Закону о защите данных 1998 г. Перечень 1 "Принципы защиты данных". Register (notify) under the Data Protection Act // http://ico.org.uk/for-organisations/register/).

[23] *Бачило И.Л.* Указ. соч.

обратиться с уведомлением к контроллеру ("принудительным уведомлением") с требованием к нему о соблюдении принципа или принципов защиты данных и сделать одно или оба предписания: а) определить временной период, в который должны быть устранены нарушения; б) указать на необходимость прекращения обработки персональных данных или каких-либо иных данных, указанных в уведомлении.

При принятии решения о направлении уведомления Комиссар исследует, причинило ли нарушение ущерб или страдания человеку. В случае нарушения принципа защиты данных, требующего от контроллера данных исправления, блокирования, удаления или уничтожения любых неточных данных, Комиссар может потребовать от последнего исправить, блокировать, удалить или уничтожить такую информацию о субъекте персональных данных или третьей стороне.

В случае если данные точно записаны и переданы контроллером данных от субъекта данных или третьей стороны, то Комиссар может потребовать от контроллера данных: а) исправления, блокирования, удаления или уничтожения всех неточных данных и любых других данных, хранящихся у контроллера и содержащего выражение мнения, или б) принять меры, которые указаны в уведомлении для обеспечения соблюдения требований Закона о защите данных, и если Комиссар посчитает необходимым, то он может потребовать и совершение дополнительных действий.

Если предписание требует от контроллера данных исправления, блокирования, удаления или уничтожения данных или Комиссар убежден, что персональные данные, которые были устранены, заблокированы, стерты или уничтожены, были обработаны в нарушение любого из принципов защиты данных, то Комиссар может потребовать от контроллера данных определить перечень лиц, которые должны быть уведомлены о совершении соответствующих действий, и указать контроллеру на необходимость их уведомления о соответствующих инцидентах.

Предписание должно содержать: а) заявление о принципе (принципах) защиты данных, которые Комиссар считает нарушенными; б) сведения о правах, подлежащих восстановлению.

Таким образом, в Великобритании предпринимаются все меры для превентивной защиты персональных данных (путем установления обязанностей контроллера данных по обеспечению их защиты). Однако в случае нарушений установлена серьезная административная и уголовная ответственность за нарушения в области персональных данных и запрета на передачу данных третьим лицам.

Совершение таких правонарушений наказывается в Великобритании штрафом до 500 тыс. фунтов, а также предусматриваются административные санкции за несвоевременное устранение нарушений и повторное нарушение, а при преднамеренном характере нарушений, которые привели к серьезным последствиям, установлена уголовная ответственность в виде лишения свободы.

Кроме того, существует требование к интернет-провайдерам об уведомлении без неоправданной задержки Комиссара по персональным данным, а в некоторых случаях и абонентов о любых инцидентах с их персональными данными. Неуведомление может привести к штрафу в размере 1000 фунтов стерлингов.

В соответствии с законодательством Великобритании данные могут быть обработаны с помощью третьей стороны, если последняя предоставит достаточные гарантии относительно технической и организационной безопасности. Передача данных возможна, если контроллер данных принимает разумные меры для обеспечения соблюдения Закона о защите данных 1998 г.

В России состав и содержание мер по обеспечению безопасности персональных данных определены приказом Федеральной службы по техническому и экспортному контролю России (ФСТЭК) "Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" от 18 февраля 2013 г.[24] ФСТЭК определяет, что безопасность персональных данных при их обработке в информационной системе обеспечивает оператор или лицо, осуществляющее обработку персональных данных по поручению оператора, в соответствии с законодательством Российской Федерации; в том числе перечень мер по обеспечению безопасности персональных данных, которые должны быть приняты для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении последних.

Уполномоченным органом по защите прав субъектов персональных данных в Российской

[24] См.: СПС "КонсультантПлюс".

Федерации является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). Статьей 23 Федерального закона "О персональных данных" определены полномочия Роскомнадзора, объем которых является достаточным для осуществления необходимой защиты прав субъектов персональных данных и соответствует объему полномочий аналогичных органов государственной власти зарубежных стран.

Однако все полномочия Роскомнадзора связаны с деятельностью оператора персональных данных либо субъекта персональных данных. Роскомнадзор вправе давать обязательные указания и привлекать к ответственности операторов персональных данных, нарушающих Федеральный закон "О персональных данных". Соответственно, лица, которые не подпадают под определение оператора персональных данных, например операторы поисковых систем либо лица, анализирующие большие данные, но не получающие персональные данные, не входят в число лиц, в отношении которых Роскомнадзор вправе осуществлять проверки и выдавать требования об обязании совершения каких-либо действий[25].

В 2015 г. в Великобритании рассматривались поправки к дефиниции "персональные данные", в связи с чем предлагалось расширить определение персональных данных так, чтобы в него были включены IP-адреса и *cookie*[26]. В поправках к Закону предлагается следующее определение: "Персональные данные – данные, с помощью которых физическое лицо может быть идентифицировано прямо или косвенно на основании средств, которые могут быть использованы контроллером данных.., в том числе применительно к идентификационным номерам, данным о местоположении, онлайн идентификаторам..."[27].

Следует отметить, что российское законодательство более консервативно в части соотнесения персональных данных с информацией, получаемой во время выхода человека в сеть Интернет, так как непосредственно информация, получаемая из *cookies* файлов и IP-адрес, не включена в российское понятие "персональные данные"[28]. Российский закон под персональными данными понимает "любую информацию, относящуюся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)" (ч. 1 ст. 3 Федерального закона "О персональных данных"). Такое понимание персональных данных в период информационного развития общества не позволит адекватно регулировать интернет-отношения, связанные с обеспечением безопасности персональных данных.

При наличии информационной системы, состоящей из необходимого набора элементов (операторов, передающего устройства и др.), при отсутствии причин физического (технического) характера, делающих информационный обмен невозможным, ничто не может остановить копирование и распространение информации. Таким образом, обработка персональных данных в информационно-телекоммуникационной сети Интернет будет продолжаться, но в соответствии с российским законодательством мы не сможем классифицировать такие действия как позволяющие идентифицировать человека[29].

Включение файлов *cookies* в определение персональных данных связано с имеющейся практикой России и Великобритании собирания информации об интересах человека и его данных провайдерами услуг, информационными посредниками, операторами связи, которую они получают в процессе оказания и предоставления интернет-услуг.

В этой связи Министерство внутренних дел Великобритании указало, что может привлечь к уголовной ответственности за нарушение персональных данных в случае использования платформы *Phorm,* которая позволяет организовать таргетированную рекламу[30].

В качестве примера обеспечения безопасности персональных данных оператором услуг мобильной связи можно привести компанию TPO

[25] См.: 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., 2016.

[26] Фрагмент данных, отправленный веб-сервером и хранимый на компьютере пользователя. Применяется для сохранения данных на стороне пользователя, на практике обычно используется для аутентификации пользователя; хранения персональных предпочтений и настроек пользователя; отслеживания состояния сеанса доступа пользователя; ведения статистики о пользователях.

[27] The Data Protection Act 1998 (Commencement No. 4) Order 2015 // http://www.legislation.gov.uk/all?title=The%20Data%20Protection%20Act

[28] *Жарова А. К.* Сущность и структура информационного противоборства // Гос. и право. 2009. № 2. С. 48–54.

[29] См.: *Жарова А. К.* Условия оказания услуги по предоставлению доступа к облачным вычислениям // Гос. и право. 2012. № 12. С. 86–90.

[30] См.: McDermott Will & Emery Privacy issues in targeted internet advertising – bad Phorm? // http://www.lexology.com/library/detail.aspx?g=92223ba1-f0e2-42e6-83e8-e22d06b204ae

(The Peoples Operator)[31]. На сайте данного оператора в разделе "Политика конфиденциальности" предусмотрен подраздел *Privacy Policy – Pay Monthly*, в котором определяется политика обработки персональных данных. *К персональным данным эта компания относит имя, адрес, номер телефона или адрес электронной почты.*

Однако компания TPO определяет свое право собирать и обрабатывать как персональные данные, так и иные данные: данные, предоставляемые при заполнении форм на сайте оператора; сведения о посещениях веб-сайта или об использовании услуг и ресурсов, к которым клиент может получить доступ; историю переписки с клиентом; запись вызовов; ответы клиентов на сообщения и сообщения, которые TPO посылает своему клиенту; конфиденциальные персональные данные; данные о местоположении; дебетовые и кредитные карты, банковские данные и другую информацию о произведенной оплате.

TPO также определяет свое право получения иной информации о клиенте с помощью файла *cookie,* который хранится на жестком диске компьютера клиента. TPO указывает, что клиент может самостоятельно узнать больше о *cookie* и правилах их использования на сайте компании[32]. Кроме того, TPO оставляет за собой право сохранить все данные, которые клиент предоставляет на сайте компании, в том числе "чувствительные (конфиденциальные) личные данные", используя функции системы *VeCapture* и *VeInteractive,* даже если клиент не завершил регистрацию или не закончил действия на сайте компании. Такие контактные данные и информация могут быть использованы компанией для связи с клиентом, в том числе для того, чтобы узнать, почему клиент не завершил регистрацию или транзакцию.

TPO определила сроки хранения информации о клиенте следующим образом: "так долго, как это необходимо для выполнения целей, для которых данные были собраны, или, если иное не предусмотрено законом". Кроме того, TPO вправе передавать информацию за границу и хранить ее за пределами Европейской экономической зоны, предпринимая при этом все разумные с точки зрения TPO меры для гарантии безопасности информации о клиенте в соответствии с политикой конфиденциальности.

Это право компании соотносится с требованием Закона о защите данных 1998 г., который предоставляет право физическим лицам иметь доступ к их личной информации. "Человек имеет право контролировать данные и получать информацию о себе, в том числе право знать, какая информация была собрана, для каких целей она обрабатывается, кто является получателем и при каких условиях она может быть раскрыта". В большинстве случаев ответ на запрос физического лица должен быть представлен в период 40 календарных дней с момента получения.

Таким образом, мы можем заметить правовую неоднозначность подхода к теме обработки персональных данных в интернет-структурах. С одной стороны, в Великобритании нет прямого запрета на собирание персональной информации посредством *cookies* файлов, что позволяет компаниям указывать в политике конфиденциальности о применении *cookies* файлов, но, с другой – существуют заявления от государственных органов, которые предупреждают о возможной классификации таких действий, как уголовное преступление.

Подтверждением происходящих изменений в области сбора и обработки данных посредством *cookie* можно привести пример из судебной практики Великобритании.

В 2013 г. в Великобритании был предъявлен иск пользователями браузера *Safari* к поисковой системе *Google*. Пользователям браузера *Safari* стало известно, что *Google* собирает информацию об их действиях в Интернете без их согласия посредством использования *cookies* файлов. Истцы подали иск о злоупотреблении информацией о частной жизни, злоупотреблении доверием и нарушении Закона о защите данных 1998 г.

Формулировка ст. 13 (2) Закона о защите данных 1998 г. предусматривает, что претензии могут быть предъявлены в случае, если нарушение вызывало "ущерб и страдания". Суды Великобритании интерпретировали ущерб в основном как материальный ущерб. Однако Апелляционный суд посчитал, что интерпретация ст. 13 (2) Закона о защите данных 1998 г. была неверной и вступает в противоречие с Уставом ЕС об основных правах *(EU Charter of Fundamental Rights)*. Апелляционный суд решил, что следует уделять большое значение нематериальному аспекту. Так, если человек продемонстрирует, что нарушение Закона о защите данных 1998 г. вызвало страдания, то он имеет право подать иск в соответствии со ст. 13 в связи с удовлетворением нематериального ущерба.

[31] Общество с ограниченной ответственностью, зарегистрированное в Великобритании.

[32] См.: About Cookies // http:// www.thepeoplesoperator.com/Cookies

Ведущий научный сотрудник юридической компании *Clyde&Co* Дж. Кассиди считает, что это решение имеет далеко идущие последствия для всех контроллеров данных и изменяет способы обеспечения защиты персональных данных. Особенно серьезные последствия могут возникнуть у контроллеров данных в сфере здравоохранения в случае утечки каких-либо данных о состоянии здоровья[33].

Как указано на сайте *Out-Law* международной юридической фирмы *Pinsent Masons*, Департамент правительства Великобритании по делам культуры, СМИ и спорта (DCMS) взял на себя ответственность за формирование политики защиты данных Великобритании[34].

При этом субъект персональных данных имеет право требовать изменения и удаления неактуальных или противоречивых персональных данных.

Сохранение персональных данных и порядок обработки этих данных, полученных интернет-провайдерами при выполнении своих обязательств, регулируется Директивой Европейского парламента по хранению данных от 15 марта 2006 г. *(Data Retention Directive)*[35], которая была принята после террористических актов, проведенных в Мадриде в 2004 г. и в Лондоне в 2005 г., в целях согласования усилий ЕС в расследовании и уголовном преследовании самых серьезных преступлений, таких как организованная преступность и терроризм. Кроме того, Закон 1998 г. предусматривает частные случаи хранения и обработки персональных данных интернет-провайдерами, в том числе при наличии соглашения об этом с пользователем интернет-услуг.

Директива Европейского парламента по хранению данных 2006 г. требует от интернет-провайдеров сохранять определенные категории данных о трафике и местоположении физических лиц (за исключением содержания этих сообщений) в период от шести месяцев до двух лет *и делать их доступными правоохранительным органам в случае их запроса для целей расследования, выявления и преследования тяжких преступлений и терроризма.*

Как указывает общественность, сохраненные данные являются ценной информацией и доказательствами, на основании которых могут быть вынесены как обвинительные приговоры за уголовные преступления, так и оправдательные приговоры, которые никогда бы не были сделаны, если не обязанность сохранять эти данные. Несмотря на это, в Великобритании обсуждался вопрос о том, что провайдеров могут признать нарушителями законодательства о персональных данных, если они по-прежнему будут сохранять информацию, полученную в результате обработки данных пользователей, в соответствии с Директивой по хранению данных.

8 апреля 2014 г. Суд Европейского Союза признал Директиву ЕС хранения данных недействительной. Суд посчитал, что Директива не удовлетворяет принципу соразмерности и должна предоставлять большие гарантии для защиты фундаментальных прав, уважения частной жизни и защиты персональных данных.

По указанным причинам в Великобритании высказывается мнение[36] о том, что провайдеры обязаны прекратить сохранять данные и должны уничтожать все данные, сохраненные в силу ныне недействительных нормативных актов. Если компании будут продолжать сохранять данные, то существует риск, что их собственные клиенты могут подать иски за нарушение Закона 1998 г.

Заключение

Таким образом, можно заметить, что в Великобритании нормативная система обеспечения безопасности персональных данных сходна с российской системой, но имеет свои особенности. Так, в Великобритании уполномоченным органом является ICO, деятельность которого направлена только на обеспечение безопасности персональных данных. В России уполномоченным исполнительным органом в данной области – Роскомнадзор, в который входят 10 различных управлений, в том числе Управление по защите прав субъектов персональных данных.

Кроме того, в Великобритании под информацией понимается содержательная сторона данных, что

[33] См.: James Cassidy, Senior Associate Compensation under the Data Protection Act 1998: All Change // http://www.clydeco.com/insight/updates/view/compensation-under-the-data-protection-act-1998-all-change

[34] См.: http://www.out-law.com/en/articles/2015/september/dcms-takes-on-responsibility-for-uk-data-protection-policy-and-sponsorship-of-the-ico/

[35] См.: DIRECTIVE 2006/24/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC // http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ: L:2006:105:0054:0063: EN: PDF

[36] См.: Survey reveals nearly half of web users happy with behavioural advertising // http://www.out-law.com/en/articles/2012/may/survey-reveals-nearly-half-of-web-users-happy-with-behavioural-advertising-/

позволяет регулировать не только передачу данных по каналам связи, но и содержание данных. Подход Великобритании не противоречит теории понимания информации через количественную и качественную характеристику[37], где под качественной характеристикой понимается содержание информации, а под количественной – количество различных сообщений от интернет-источника.

Положительный пример – позиция Великобритании, которая признает персональными данными следующую информацию: IP, идентификационные номера, данные о местоположении человека, онлайн идентификаторы, иную информацию, на основании которых можно определить человека в сети Интернет.

В России для обеспечения безопасности граждан и обеспечения правоохранительных органов информацией для расследования и пресечения преступлений был принят так называемый "антитеррористический" пакет законов. Данный пакет законов дополнил российское информационное законодательство следующими субъектами:

"организатором распространения информации в сети Интернет", на которого возлагаются три основные обязанности: 1) уведомление Роскомнадзора об осуществлении соответствующей деятельности, на основании которого лицо включается в специальный реестр; 2) обязанность по хранению данных в определенном объеме в течение шестимесячного срока; 3) обязанность по сотрудничеству с правоохранительными органами в определенном объеме (ст. 10.1);

"владельцем новостного агрегатора", на которого возлагается обязанность соблюдения требований законодательства Российской Федерации о распространении информации (ст. 10.4 Федерального закона об информации).

Во многом логика предложенных изменений в законодательство Российской Федерации схожа с логикой Директивы ЕС 2006/24/ЕС "О хранении данных", которая определяет обязанности, возлагаемые на интернет-провайдеров, о хранении и выдаче данных о трафике правоохранительным органам. Однако, как было указано выше, в 2014 г. Директива ЕС 2006/24/ЕС была признана недействительной.

Следует отметить, что российский подход предоставил более широкие возможности предотвращения правонарушений: блокировка Роскомнадзором веб-ресурса организатора распространения информации в сети Интернет, не исполняющего обязанности в порядке, указанном в ст. 15.4 Федерального закона об информации и в ч. 2.1 ст. 13.31 КоАП РФ.

[37] См.: *Шеннон К.* Работы по теории информации и кибернетике. М., 1963; *Колмогоров А. Н.* Три подхода к определению понятия "количество информации" // Проблемы передачи информации. Вып. 1. Т. 1. М., 1965; *MacKay, David.* Information Theory, Inference, and Learning Algorithms. Cambridge, 2003.