

Объединенных Наций [Электронный ресурс]. URL: <https://www.refworld.org.ru/docid/4933d0b22.html> (дата доступа: 10.12.2020).

11. Права человека в период COVID-19. Уроки эпидемии ВИЧ-инфекции: эффективное реагирование силами сообщества // ЮНЭЙДС [Электронный ресурс]. URL: [https://www.unaids.org/sites/default/files/media\\_asset/human-rights-and-covid-19\\_ru.pdf/](https://www.unaids.org/sites/default/files/media_asset/human-rights-and-covid-19_ru.pdf/) (дата доступа: 10.12.2020).

12. Ulteriori disposizioni attuative del decreto-legge 23 febbraio 2020, n. 6, recante misure urgenti in materia di contenimento e gestione dell'emergenza epidemiologica da COVID-19, applicabili sull'intero territorio nazionale // Gazzetta Ufficiale [Electronic resource]. 2020. URL : <https://www.gazzettaufficiale.it/eli/gu/2020/03/09/62/sg/pdf> (accessed: 10.12.2020).

13. South Korea: Legal Responses to Health Emergencies // Library of Congress [Electronic resource]. 2020. URL : <https://www.loc.gov/law/help/health-emergencies/southkorea.php> (accessed: 10.12.2020).

## **ПРАВОВОЙ МЕХАНИЗМ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В СЕТИ ИНТЕРНЕТ**

*М. О. Дудко*

*Национальный центр законодательства и правовых исследований Республики Беларусь,  
ул. Берсона, 1а, 220030, г. Минск, Беларусь,*

Статья посвящена анализу правового механизма защиты персональных данных в сети Интернет. Автор анализирует вопросы, касающиеся структуры правового механизма обеспечения защиты персональных данных в сети Интернет, субъектного состава правоотношений в области защиты персональных данных в сети Интернет. Автор предлагает меры, направленные на создание и эффективное функционирование правового механизма защиты персональных данных в сети Интернет.

**Ключевые слова:** Интернет; персональные данные; защита персональных данных.

## **LEGAL MECHANISM FOR THE PROTECTION OF PERSONAL DATA ON THE INTERNET**

*M. O. Dudko*

*The National Centre of Legislation and Legal Research of the Republic of Belarus,  
1a Bersona Street, Minsk 220030, Belarus*

The article is devoted to the analysis of the legal mechanism of personal data protection on the Internet. The author analyzes issues related to the structure of the legal mechanism for ensuring the protection of personal data on the Internet, the subject structure of legal relations in the field of personal data protection on the Internet. The author suggests measures aimed at creating and effective functioning of the legal mechanism for the protection of personal data on the Internet.

*Key words:* Internet; personal data; protection of personal data.

Создание, развитие и повсеместное внедрение Глобальной компьютерной сети Интернет (далее – Интернет) во все сферы общественной жизни перевернуло сознание всего мирового сообщества. Интернет стал не только платформой для поиска и передачи информации, но и второй сущностью человека, местом, где он проводит значительную часть своей жизни, а само право на доступ к Интернету в 2011 году Организацией Объединённых Наций (далее – ООН) было признано в качестве базового, неотъемлемого права человека [1]. Посредством сети Интернет личность реализует целый комплекс политических, экономических, социальных, культурных прав и свобод, совершает юридически значимые действия. Так, согласно данным, представленным Национальным статистическим комитетом Республики Беларусь, в 2019 году доступ населения в возрасте от 6 – 72 лет к услугам сети Интернет составлял 82,8% от общей численности населения [2]. В 2019 году 37,8% населения Республики Беларусь в возрасте 6 – 72 лет использовали сеть Интернет для осуществления финансовых операций, а 19% населения осуществляли взаимодействие с органами государственного управления непосредственно через сеть Интернет [3]. Вполне очевидно, что эти показатели в 2020 году, в условиях пандемии коронавируса, будут значительно выше, а тенденция использования сети Интернет в качестве основного способа коммуникации субъектов будет только расти.

Доступ к почти неограниченному количеству информации, быстрота и эффективность поиска и передачи данных, возможность обрабатывать и хранить огромные массивы сведений, трансграничный характер сети – всё это неоспоримые преимущества использования Интернета. Более того, Интернет и созданные на его основе информационно-коммуникационные технологии (далее – ИКТ) оказывают существенное влияние на развитие и трансформацию права в целом и прав человека в частности. Исключением не стал и институт персональных данных. Так, с развитием ИКТ, право на защиту персональных данных уже не рассматривается исключительно через призму защиты частной жизни индивида. Как справедливо отмечает в своей работе Т. Д. Оганесян: «право на защиту персональных данных сегодня находится в промежуточном состоянии: его уже нельзя в полной мере рассматривать ни как часть права на уважение частной жизни, ни в качестве полноценного и самостоятельного права» [4, с. 48]. Влияние ИКТ и Интернета на зарождение и развитие института персональных данных можно проследить в формировании не типичных, ранее не существовавших правомочий в отношении персональных данных, а именно «право на забвение» (или по-другому, право быть забытым),

право на уведомление, право на геоблокацию своих данных и т.д. Однако, взаимодействие Интернета и персональных данных порождает не только возникновение новых правомочий, но и ряд конфликтов. Так, например, в праве и доктрине остаётся открытым вопрос о соотношении права на защиту персональных данных с правом на свободу мнений и их свободным выражением, в том числе, посредством сети Интернет. Немаловажным является разрешения конфликта в сфере соотношения защиты персональных данных индивида и охраны публичных интересов. Так, неоднозначную оценку общественности вызвало принятие в 2016 году Российской Федерацией, так называемого, «закона Яровой», обязавшего Интернет-провайдеров и операторов сотовой связи хранить в течении определённого промежутка времени текстовые, аудио- и видео-сообщения пользователей. Целью принятия данных предписаний было обеспечение общественной безопасности в контексте противодействия террористическим угрозам. Также, приоритетным направлением правовой регламентации отношений является решение вопроса о размещении общедоступных данных в сети Интернет и защите персональных данных. Таким образом, создание и функционирование действенного и эффективного правового механизма обеспечения защиты персональных данных в сети Интернет является особенно актуальным.

Отдельные элементы правового обеспечения защиты персональных данных в сети Интернет рассматривались в работах Я. В. Кудашкина [5], М. Е. Черемисиновой [6], Т. Д. Оганесяна [4], Э. В. Талапиной [7], С. А. Шадрина [8], А. В. Даниленкова [9], А. И. Ковлера [10] и др. Достаточное количество исследований, посвящённых данной проблематике, свидетельствует о том, что в правовой науке накоплен значительный опыт в изучении вопросов правовой регламентации защиты персональных данных в сети Интернет. В тоже самое время, в ряде работ исследования защиты персональных данных в сети Интернет не являются предметной темой и носят лишь фрагментарный характер. Таким образом, данное исследование направлено на устранение вышеназванного недостатка, а также формирование правового механизма защиты персональных данных в сети Интернет.

Структура правового механизма обеспечения защиты персональных данных в сети Интернет предполагает наличие следующих элементов: 1) наличие правоотношений в области защиты персональных данных в сети Интернет, 2) создание и функционирование правовых норм, регулирующих данные правоотношения. Рассматривая правоотношения в сфере защиты персональных данных в сети Интернет следует остановиться на ряде ключевых моментов. Во-первых, субъектный состав данных правоотношений достаточно разнообразен. Так, например,

субъектами данного рода отношений могут быть физические лица, являющиеся субъектами персональных данных, государство, в лице уполномоченных органов, осуществляющих сбор, хранение и обработку персональных данных индивида, Интернет-провайдеры, предоставляющие доступ к сети Интернет, социальные сети и мессенджеры, имеющие доступ к персональным данным физического лица и др. По сути, участниками правоотношений в области защиты персональных данных в сети Интернет могут выступать абсолютно любые лица, имеющее доступ в сеть.

Во-вторых, объектом данного рода отношений выступают конкретные действия, связанные с персональными данными. В отношении персональных данных предусмотрен их сбор, хранение, использование, передача и обработка. При этом, определённое действие зависит как от статуса субъектов, вступающих в правоотношения, так и от вида персональных данных, по поводу которого эти отношения складываются. Так, например, анализ политик конфиденциальности крупнейших IT-компаний мира показывает, что сведения, которые они собирают в процессе своей деятельности можно разделить на несколько групп: 1) данные об использовании сервисов: посещаемые веб-страницы, поисковые запросы и т.д., 2) контакты и отношения субъектов, 3) сведения об устройствах: операционная система, параметры устройства, наименование и тип программного обеспечения, 4) данные о местоположении (геолокационные сведения), 5) сведения о файлах и передаваемых данных посредством онлайн-сервисов: содержимое файлов, музыка, видео [11, с. 222 – 223]. В тоже самое время, органы государственной власти и управления, как правило, осуществляют сбор, обработку и хранение номинативной информации о физическом лице: фамилия, имя, отчество, идентификационный номер, число, год и месяц рождения и т.д. Также, в зависимости от вида персональных данных установлены определённые ограничения на совершение конкретных действий. Так, например, в ч. 1 ст. 10 Федерального закона Российской Федерации «О персональных данных» предусмотрено, что обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается [12]. В тоже самое время, существование общедоступных источников персональных данных, которые создаются с целью информационного обеспечения и содержат сведения, сообщаемые самим субъектом персональных данных, подразумевает свободный оборот таких данных, без каких-либо правовых ограничений.

В-третьих, содержание, т.е. наличие субъективных прав и обязанностей, правоотношений в области защиты персональных данных в сети Интернет ничем не отличается от реальной, оффлайн среды. Участники данных правоотношений могут свободно реализовать предоставленные им права, а также исполнять возложенные на них обязанности. По сути, являясь средой виртуальной, сеть Интернет подчиняется вполне реальным законам. Однако, как отмечает Я. В. Кудашкин, единственной специфической чертой данных правоотношений, является их трансграничность, так как сеть Интернет позволила сделать территориальные границы более прозрачными и превратила виртуальное пространство в новое юридическое поле, которое стало наднациональным пространством [5, с. 72 – 73].

Наличие правовых норм, регулирующих отношения в сфере защиты персональных данных в сети Интернет, является неотъемлемым элементом в структуре правового механизма обеспечения безопасности данного рода информации. Как уже было отмечено выше, для сети Интернет не существует привычных нам территориальных границ, Интернет носит трансграничный, наднациональный характер. Таким образом, нормирование отношений в сфере защиты персональных данных в сети Интернет должно осуществляться на двух уровнях: международном и национальном. Сегодня, на международном уровне действует ряд нормативных документов, отдельные элементы которых направлены на защиту персональных данных в сети Интернет. Конвенция Совета Европы № 108 «О защите частных лиц в отношении автоматизированной обработки данных личного характера» фактически заложила основы правового обеспечения защиты персональных данных на международном уровне [13]. Так в ст. 1 данной Конвенции декларируется, что цель Конвенции состоит в обеспечении на территории каждой стороны для каждого физического лица независимо от его гражданства или местожительства, уважения его прав и основных свобод, и в частности его права на неприкосновенность частной жизни, в отношении автоматизированной обработки касающихся его персональных данных. С введением в действие данного международного документа в европейских странах начался процесс разработки и принятия национальных правовых актов, направленных на обеспечение безопасности персональных данных. На сегодняшний день Конвенция ратифицирована 55 государствами. К слову, данный международный документ носит открытый характер и присоединиться к Конвенции могут не только члены Совета Европы, но и государства, не являющиеся таковыми.

Следующим международным документом, затрагивающим безопасность персональных данных в сети Интернет, стала Конвенция Совета Европы № 185 «О компьютерных преступлениях» [14]. По своей сути данная Конвенция стала первым международным договором, создавшим правовой механизм противодействия преступлениям в киберпространстве. Ряд статей данной Конвенции затрагивают вопросы безопасности персональных данных, в том числе безопасности в сети Интернет. Так, в ст. 2 закреплено, что каждая Сторона принимает законодательные и иные меры, необходимые для того, чтобы квалифицировать в качестве уголовного преступления согласно ее внутригосударственному праву доступ, когда он является преднамеренным, к компьютерной системе в целом или любой ее части неправомерно [14]. Параграфом 3 ст. 16 предусмотрено, что каждая Сторона принимает законодательные и иные меры, необходимые для того, чтобы обязать хранителя или другое лицо, которому поручено обеспечивать сохранность компьютерных данных, сохранять конфиденциальность выполнения таких процедур в течение срока, предусмотренного ее внутригосударственным правом [14]. В ст. 20 данной Конвенции декларируется, что каждая Сторона принимает законодательные и иные меры, необходимые для предоставления ее компетентным органам полномочий, собирать или записывать с применением технических средств на территории этой Стороны данные о потоках информации в режиме реального времени, а также обязать поставщиков услуг в пределах имеющихся у них технических возможностей собирать и записывать, а также предоставлять компетентным органам такого рода данные [14]. Однако, стоит констатировать тот факт, что данная Конвенция является устаревшей, а положения, закреплённые в ней, нуждаются в пересмотре. Как отмечает И. И. Рогачёв: «в годы принятия и разработки Конвенции не существовало таких сложных проблем, как современные бот-сети. Конвенция явно не предусматривает должных мер в ответ на злободневные проявления киберпреступности, например, в отношении повсеместной спамерской деятельности и сетевого мошенничества» [15].

Немаловажное значение в сфере защиты персональных данных в сети Интернет играют акты Организации экономического сотрудничества и развития (далее – ОЭСР). Базовым нормативным документом данной организации, регулирующим отношения в сфере защиты персональных данных в сети Интернет, являются Рекомендации Совета ОЭСР по принципам разработки государственной Интернет-политики [16]. Так, к базовым принципам данный документ относит согласованную и эффективную защиту частной жизни на мировом уровне. Для

использования всего экономического и социального потенциала Интернета необходимо, чтобы частная жизнь была достаточно защищена. Уже известные проблемы, касающиеся защиты частной жизни, будут лишь обостряться по мере возрастания зависимости экономики и общества от широкого и инновационного использования информации персонального характера, которую станет проще собирать, сохранять и анализировать [7, с. 123]. Важным принципом, закреплённым в данных Рекомендациях, является принцип согласованности основных, фундаментальных прав человека, таких как право на свободу слова, право на свободу прессы и право на открытое и транспарентное правление с нормами, регулирующими защиту частной жизни индивида. Повышенное внимание ОЭСР уделяет персональным данным, составляющим информацию о здоровье человека. Разработанные в 2016 году Рекомендации Совета ОЭСР по управлению данными о здоровье [17] предусматривают, что лица, персональные данные о здоровье которых собраны, получают информацию об обработке персональных данных о своем здоровье, в том числе и о возможном ознакомлении с этими данными уполномоченных третьих лиц, а также о целях и преимуществах юридических оснований их обработки в четко выраженных, легко понятных и хорошо читаемых терминах. Их должны оперативно предупреждать о любых серьезных нарушениях или ином незаконном использовании персональных данных о здоровье. Если нет возможности предупредить каждое заинтересованное лицо, извещение осуществляется посредством эффективной публичной коммуникации.

В рамках Европейского Союза нормативным документом, обеспечивающим защиту персональных данных, в том числе и в сети Интернет, является Общий Регламент по защите данных (General Data Protection Regulation) [18]. Заложенный в данном Регламенте механизм правового обеспечения защиты персональных данных предусматривает, что под его действие подпадает полностью или частично автоматизированная обработка персональных данных граждан Европейского Союза как на территории Союза, так и за его пределами физическими или юридическими лицами, государственными органами и другими институтами и организациями. Таким образом, под действие Регламента подпадают десятки и сотни миллионов пользователей сети Интернет. По охвату субъектов, на которых распространяются положения данного документа, он является самым масштабным. Одной из особенностей Регламента является то, что он усиливает уже существующие права граждан в отношении своих персональных данных, а также вводит новые. Так, например, субъектам персональных данных гарантируется право на переносимость своих данных, право на

исправление своих данных, право на удаление (или иначе «право на забвение»), право на возражение и ряд других правомочий, впервые закреплённых в нормативном документе. Важным нововведением, закреплённым в Регламенте, является введение должности специально уполномоченного сотрудника по защите данных, а также создание надзорного учреждения – Европейского совета по защите данных. Таким образом, Общий Регламент по защите данных является наиболее эффективным международным документом, обеспечивающим защиту персональных данных в сети Интернет на современном этапе.

На национальном уровне в ряде государств приняты правовые акты, регулирующие отношения в сфере защиты персональных данных. Весь массив нормативных документов, обеспечивающих безопасность персональных данных можно разделить на две группы. К первой группе относятся государства, где приняты специализированные правовые акты, комплексно регулирующие отношения в сфере защиты персональных данных. К таким государствам, например, относятся Великобритания [19], Испания [20], Германия [21], Российская Федерация [12], Япония [22] и ряд других государств. Для большинства государств данной группы характерной чертой является то, что в ходе разработки и принятия специализированных национальных актов были учтены, а также имплементированы нормы Конвенции Совета Европы «О защите частных лиц в отношении автоматизированной обработки данных личного характера», а с принятием и вступлением в действие Европейского Регламента по защите данных национальное законодательство стран-участниц Европейского Союза было скорректировано и приведено в соответствие с ним. Вторую группу образуют государства, где отсутствует специализированный нормативный документ, направленный на защиту персональных данных. Правовое обеспечение безопасности персональных данных в таких государствах осуществляется в зависимости от сферы общественной жизни, в которой используются такого рода данные. Так, например, в США действует Закон о защите частной жизни в сфере видеопроката (The US Video Privacy Protection Act of 1988) [23], в сфере защиты персональных данных в финансовом секторе принят Закон Грэма-Лич-Блайли 1999 г. (Gramm-Leach-Bliley Act of 1999) [24], для защиты персональных данных детей в онлайн-среде функционирует Закон о защите частной жизни детей в онлайн-среде (The Children's Online Privacy Protection Rule of 2013) [25]. Аналогичным образом осуществляется защита персональных данных в Китае. Правила обработки, хранения, передачи и использования персональных данных закреплены в ряде отраслевых документов: 1) «Административные меры для онлайн-транзакций», 2) «Меры по охране персональных данных при оказании



почтовых и курьерских услуг», 3) «Меры по охране персональных данных при ведении медицинских записей медицинскими организациями», 4) Закон Китайской Народной Республики «О защите прав потребителей» [11, с. 130, 134]. Отсутствие специализированного документа, комплексно регулирующего защиту персональных данных в сети Интернет, а также отраслевое регулирование данного рода отношений препятствует созданию действенного механизма правового регулирования, направленного на защиту персональных данных в Интернете.

Таким образом, для создания и эффективного функционирования правового механизма защиты персональных данных в сети Интернет требуется разработка и принятие на международном уровне единых норм и стандартов, которые затем будут имплементированы в национальное право. Всё это позволит говорить о слиянии правовых систем, что в конечном счете приведет к единообразному взгляду на вопросы правовой регламентации защиты персональных данных в сети Интернет, а также установлению и функционированию единого механизма регулирования и ответственности.

В ходе проведенного исследования автором были сформулированы следующие выводы:

1. Структура правового механизма обеспечения защиты персональных данных в сети Интернет предполагает наличие следующих элементов: 1) наличие правоотношений в области защиты персональных данных в сети Интернет, 2) создание и функционирование правовых норм, регулирующих данные правоотношения.

2. Субъектный состав правоотношений в области защиты персональных данных в сети Интернет достаточно разнообразен: начиная от физических лиц, кому персональные данные принадлежат и заканчивая Интернет-провайдерами, социальными сетями и мессенджерами. По сути, участниками правоотношений в области защиты персональных данных в сети Интернет могут выступать абсолютно любые лица, имеющее доступ в сеть. Объектом данного рода отношений выступают конкретные действия, связанные с персональными данными. В отношении персональных данных предусмотрен их сбор, хранение, использование, передача и обработка. Содержание, т.е. наличие субъективных прав и обязанностей, правоотношений в области защиты персональных данных в сети Интернет ничем не отличается от реальной, оффлайн среды. Участники данных правоотношений могут свободно реализовать предоставленные им права, а также исполнять возложенные на них обязанности. По сути, являясь средой виртуальной, сеть Интернет подчиняется вполне реальным законам.

3. В силу трансграничного, наднационального характера сети Интернет, нормирование отношений в сфере защиты персональных данных в сети должно осуществляться на двух уровнях: международном и национальном. На международном уровне приняты и действуют ряд соглашений, направленных на обеспечение безопасности персональных данных. Среди международных актов можно выделить Конвенцию Совета Европы № 108 «О защите частных лиц в отношении автоматизированной обработки данных личного характера», которая фактически заложила основы правового обеспечения защиты персональных данных на международном уровне. Конвенция Совета Европы № 185 «О компьютерных преступлениях» стала первым международным договором, создавшим правовой механизм противодействия преступлениям в киберпространстве. Важными международными документами, направленными на защиту персональных данных в сети Интернет, являются Рекомендации Совета ОЭСР по принципам разработки государственной Интернет-политики, а также Рекомендации Совета ОЭСР по управлению данными о здоровье. В рамках Европейского Союза нормативным документом, обеспечивающим защиту персональных данных, в том числе и в сети Интернет, является Общий Регламент по защите данных (General Data Protection Regulation). На сегодняшний день, заложенный в данном Регламенте правовой механизм защиты персональных данных является наиболее действенным и эффективным.

4. На национальном уровне в ряде государств приняты правовые акты, регулирующие отношения в сфере защиты персональных данных. Весь массив нормативных документов, обеспечивающих безопасность персональных данных можно разделить на две группы. К первой группе относятся государства, где приняты специализированные правовые акты, комплексно регулирующие отношения в сфере защиты персональных данных. Вторую группу образуют государства, где отсутствует специализированный нормативный документ, направленный на защиту персональных данных. Правовое обеспечение безопасности персональных данных в таких государствах осуществляется в зависимости от сферы общественной жизни, в которой используются такого рода данные.

5. Для создания и эффективного функционирования правового механизма защиты персональных данных в сети Интернет требуется разработка и принятие на международном уровне единых норм и стандартов, которые затем будут имплементированы в национальное право. Всё это позволит говорить о слиянии правовых систем, что в конечном счете приведет к единообразному взгляду на вопросы правовой регламентации защиты персональных данных в сети Интернет, а также

установлению и функционированию единого механизма регулирования и ответственности.

## БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ

1. *La Rue F.* Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression [Electronic resource]. URL : [https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27\\_en.pdf](https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf) (accessed: 16.12.2020).
2. Доступ населения в возрасте 6 – 72 лет к услугам сети Интернет // Белстат [Электронный ресурс]. URL: <https://www.belstat.gov.by/ofitsialnaya-statistika/makroekonomika-i-okruzhayushchaya-sreda/informatsionno-telekommunikatsionnye-tekhnologii/graficheskiy-material-grafiki-diagrammy/dostup-naseleniya-v-vozraste-6-72-let-k-uslugam-seti-internet/> (дата обращения: 16.12.2020).
3. Использование информационно-коммуникационных технологий населением // Белстат [Электронный ресурс]. 2019. URL: [https://www.belstat.gov.by/upload-belstat/upload-belstat-pdf/oficial\\_statistika/infograf-transport-2-200915.pdf](https://www.belstat.gov.by/upload-belstat/upload-belstat-pdf/oficial_statistika/infograf-transport-2-200915.pdf) (дата обращения: 16.12.2020).
4. *Оганесян Т. Д.* Право на защиту персональных данных: исторический аспект и современная концептуализация в эпоху Big Data // Журн. зарубежного законодательства и сравнительного правоведения. 2020. № 2. С. 48–63.
5. *Кудашкин Я. В.* Правовое обеспечение безопасности обработки персональных данных в сети Интернет: дис. ... канд. юрид. наук : 12.00.13. М., 2019. 199 л.
6. *Черемисинова М. Е.* Правовой статус субъектов в сети Интернет : дис. ... канд. юрид. наук : 12.00.01. М., 2020. 273 л.
7. *Талатина Э. В.* Защита персональных данных в цифровую эпоху: российское право в европейском контексте // Труды Института государства и права РАН. 2018. № 5. С. 117–150.
8. *Шадрин С. А.* Правовое регулирование защиты персональных данных в Европейском Союзе: генезис и перспективы развития : дис. ... канд. юрид. наук : 12.00.10. Казань, 2019. 309 л.
9. *Даниленков А. В.* Принцип приватности в интернет-праве // Хозяйство и право. 2017. № 1. С. 89–104.
10. *Ковлер А. И.* Права человека в цифровую эпоху // Бюллетень Европейского Суда по правам человека. Российское издание. 2019. № 6. С. 146–150.
11. *Дупан А. С.* Новая парадигма защиты и управления персональными данными в Российской Федерации и зарубежных странах в условиях развития систем обработки данных в сети Интернет / А. С. Дупан, А. К. Жарова, В. М. Елин и др. ; под ред. А. С. Дупан. М. : Издательский дом Высшей школы экономики, 2016. 343 с.
12. О персональных данных : Федер. закон, 27 июля 2006 г., № 152-ФЗ : ред. от 31.12.2017 // КонсультантПлюс. Россия / ЗАО «Консультант Плюс». – М., 2020.
13. О защите частных лиц в отношении автоматизированной обработки данных личного характера : Конвенция Совета Европы от 23.11.2001, № 185 // Совет Европы [Электронный ресурс]. 1981. URL: <https://www.coe.int/ru/web/conventions/full-list/-/conventions/rms/0900001680078c46> (дата доступа: 16.12.2020).

14. О компьютерных преступлениях: Конвенция Совета Европы от 23.11.2001, № 185 // Совет Европы [Электронный ресурс]. 2001. URL: <https://rm.coe.int/1680081580> (дата доступа: 16.12.2020).
15. Российский дипломат назвал Будапештскую конвенцию по киберпреступлениям устаревшей // Информационное агентство ТАСС [Электронный ресурс]. URL: <https://tass.ru/politika/4782506> (дата обращения: 17.12.2020).
16. OECD Council Recommendation on Principles for Internet Policy Making // OECD [Electronic resource]. URL : <http://www.oecd.org/digital/ieconomy/oecd-principles-for-internet-policy-making.pdf> (accessed: 17.12.2020).
17. Recommendation on Health Data Governance. The Next Generation of Health Reforms. OECD Health Ministerial Meeting. 17 January 2017 // OECD [Electronic resource]. 2017. URL : <https://www.oecd.org/health/ministerial/ministerial-statement-2017.pdf> (accessed: 17.12.2020).
18. Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [Electronic resource]. URL : <https://ogdpr.eu/ru/gdpr-2016-679> (accessed: 17.12.2020).
19. Data Protection Act 2018 // [www.legislation.gov.uk](http://www.legislation.gov.uk) [Electronic resource]. URL : [http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga\\_20180012\\_en.pdf](http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf) (accessed: 17.12.2020).
20. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal // [www.boe.es](http://www.boe.es) [Electronic resource]. URL : <https://www.boe.es/buscar/doc.php?id=BOE-A-1999-23750> (accessed: 17.12.2020).
21. Zweites Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU - 2. DSAnpUG-EU) // [www.bgbl.de](http://www.bgbl.de) [Electronic resource]. URL : [https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger\\_BGBI&jumpTo=bgbl117s2097.pdf#\\_\\_bgbl\\_\\_%2F%2F\\*%5B%40attr\\_id%3D%27bgbl117s2097.pdf%27%5D\\_\\_1589746072188](https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBI&jumpTo=bgbl117s2097.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s2097.pdf%27%5D__1589746072188) (accessed: 17.12.2020).
22. Act on the Protection of Personal Information (Act No. 57 of 2003) // <http://www.cas.go.jp> [Electronic resource]. URL : <http://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf> (accessed: 17.12.2020).
23. Title 18. CRIMES AND CRIMINAL PROCEDURE / Part I. CRIMES / Chapter 121. STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS. Section 2710. Wrongful disclosure of video tape rental or sale records // U.S. Code [Electronic resource]. URL : <https://www.law.cornell.edu/uscode/text/18/2710> (accessed: 17.12.2020).
24. Title 15. COMMERCE AND TRADE / Chapter 94. PRIVACY / Subchapter I. DISCLOSURE OF NONPUBLIC PERSONAL INFORMATION. Section 6809. Definitions // U.S. Code [Electronic resource]. URL : <https://www.law.cornell.edu/uscode/text/15/6809> (accessed: 17.12.2020).
25. Title 16. Commercial Practices. Chapter I. FEDERAL TRADE COMMISSION / Subchapter C. REGULATIONS UNDER SPECIFIC ACTS OF CONGRESS. Part 312. CHILDREN'S ONLINE PRIVACY PROTECTION RULE / Section 312.2. Definitions // Electronic Code of Federal Regulations (e-CFR) [Electronic resource]. URL : <https://www.law.cornell.edu/cfr/text/16/312.2> (accessed: 17.12.2020).