
ПРОБЛЕМЫ ИНФОРМАЦИОННОГО ПРАВА

PROBLEMS OF INFORMATION LAW

Научная статья

УДК/UDC 34:004.056

DOI: 10.21779/2224-0241-2023-46-2-162-170

Правовая охрана персональных данных вузов

Р. А. Абдусаламов

Дагестанский государственный университет, г. Махачкала, Российская Федерация, *Abd-rus@yandex.ru*

Аннотация. Статья посвящена рассмотрению вопросов, связанных с правовой охраной персональных данных субъектов высших учебных заведений. Автор исследует правовое регулирование и общее определение такой дефиниции как «персональные данные», а также в сравнительно-правовом аспекте анализирует его через призму отношений в сфере образования. С учетом этого выявляются пробелы в специальном правовом регулировании правовой охраны персональных данных участников образовательного процесса. Особый акцент делается на современных проблемах правовой охраны персональных данных вузов с учетом использования информационных технологий в сфере высшего образования (например, в социальных сетях, облачных портфолио и др.). В данной связи обозначаются проблемы правового, организационного и технического характера. Для формулирования предложений по совершенствованию действующего законодательства автор обращается к международному правовому регулированию персональных данных в цифровом пространстве. С учетом комплексного анализа проблем правовой охраны персональных данных вузов, предлагаются в систематизированном виде наиболее актуальные направления совершенствования действующего законодательства по вопросам темы исследования. Представляется, что сделанные выводы и сформулированные предложения обладают особой теоретической и практической значимостью, а также научной новизной, и могут быть взяты за основу в практической и законотворческой деятельности (в рамках законопроектов, направленных на урегулирование правовой охраны персональных данных высших учебных заведений).

Ключевые слова: персональные данные, обучающиеся, информационные технологии, высшие учебные заведения, сеть Интернет.

Для цитирования: Абдусаламов Р. А. Правовая охрана персональных данных вузов // Юридический вестник ДГУ. 2023. Т. 46, № 2 (66). С. 162–170. DOI: 10.21779/2224-0241-2023-46-2-162-170

Original article

Legal protection of personal data of universities

Ruslan A. Abdusalamov

Daghestan State University, Makhachkala, Russian Federation, *Abd-rus@yandex.ru*

Abstract. The article is devoted to the consideration of issues related to the legal protection of personal data of subjects of higher educational institutions. The author examines the legal regulation and the general definition of such a definition as "personal data", and also analyzes it in a comparative legal aspect through the prism of relations in the field of education. With this in mind, gaps are identified in the special legal regulation of the legal protection of personal data of participants in the educational process. Special emphasis is placed on modern problems of legal protection of personal data of universities, taking into account the use of information technologies in the field of higher education (for example, in social networks, cloud portfolios, etc.). In this regard, the problems of a legal, organizational and technical nature are identified. To formulate proposals for improving the current legislation, the author refers to the international legal regulation of personal data in the digital space. Taking into account the comprehensive analysis of the problems of legal protection of personal data of universities, the most relevant directions for improving the current legislation on the issues of the research topic are proposed in a systematic form. It seems that the conclusions drawn and the proposals formulated have special theoretical and practical significance, as well as scientific novelty, and can be taken as a basis in practical and legislative activities

(within the framework of draft laws aimed at regulating the legal protection of personal data of higher educational institutions).

Key words: personal data, students, information technology, higher education institutions, the Internet.

For citation: Abdusalamov R.A. Legal protection of personal data of universities. *Yuridicheskii vestnik DGU = Law Herald of DSU*, 2023, vol. 46, no. 2 (66), pp. 162–170. DOI: 10.21779/2224-0241-2023-46-2-162-170 (In Russ.).

Персональные данные на сегодняшний день имеют значение в рамках реализации права на частную жизнь каждого гражданина. В этой связи правовая основа такой категории выражается как в актах, принимаемых на международном, так и на национальном уровне. Более того, особая актуальность вопроса, связанного с персональными данными, в нынешнее время обусловлена стремительным внедрением цифровых технологий во все сферы общественных отношений. Как следствие, законодательный подход к регулированию особенностей правовой охраны персональных данных нуждается в уточнении с учетом цифрового аспекта. Главным образом это связано с масштабированием нарушений прав граждан в данной сфере. Особенно такая проблематика характерна для отношений, возникающих в сфере образования. Так, под угрозой находятся персональные данные обучающихся высших учебных заведений. В частности, это связано с противоправным оборотом их персональных данных в условиях цифровизации образовательного процесса и хранения индивидуальных достижений обучающихся, а также данных о них в виртуальном пространстве. Осложняется такая проблема тем, что правовое регулирование персональных данных субъектов образовательных учреждений в принципе имеет ряд пробелов, которые нуждаются на сегодняшний день в восполнении путем внесения соответствующих изменений и дополнений в действующее законодательство. Как следствие, выбранная тема настоящей научной статьи имеет особую актуальность и востребованность в исследовании с учетом современных реалий, для которых характерно повсеместное использование информационно-телекоммуникационных технологий.

Переходя непосредственно к особенностям и проблемам правового регулирования персональных данных обучающихся вузов, представляется важным дать общую характеристику персональных данных.

Так, как уже было отмечено ранее, исследуемая категория имеет достаточно содержательное правовое раскрытие как на международном, так и на национальном уровне. При этом акты, принимаемые в рамках международного права, по вопросам персональных данных характеризуются многочисленностью, что связано со стремлением регулировать различные аспекты, в которых могут быть задействованы персональные данные. Более того, международная правовая основа в данной сфере постепенно совершенствуется и дополняется новыми документами.

Согласно определению статьи 2 Конвенции о защите физических лиц при автоматизированной обработке персональных данных, персональные данные – это информация, касающаяся конкретного или могущего быть идентифицированным лица. На первый взгляд, данное определение достаточно широко трактует персональные данные. Однако фактически оно отражает основную специфику таких данных, а именно то, что они составляют информацию, позволяющую персонифицировать того или иного человека. Безусловно, что круг такой информации безгранично широк, что и вызывает трудности в толковании персональных данных.

Соответственно, можно заметить, что вопросам, связанным с персональными данными, уделяется особое внимание на международном уровне, что связано с особым значением такой категории в условиях современного построения правового государства.

В данной связи в рамках отечественного законодательства также имеет место специальное правовое регулирование персональных данных. Главным образом речь идет о Федеральном закон от 27.07.2006 г. № 152-ФЗ «О персональных данных» (далее – ФЗ «О персональных данных»), в котором дается общее определение исследуемой дефиниции, устанавливаются требования к обработке персональных данных и иные вопросы, имеющие концептуальное значение для данной сферы общественных отношений [7].

Если обратиться к легальному определению персональных данных, которое дает российский законодатель, то можно заметить, что на первый взгляд оно имеет ряд сходств с тем, которое представлено на международном уровне (ранее нами проанализированное). Вместе с тем, между ними имеются и кардинальные различия.

Так, законодатель под персональными данными понимает «любую информацию, относящуюся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)».

Однако представляется, что в рассмотренном ранее нами определении персональных данных, вытекающее из Конвенции о защите физических лиц при автоматизированной обработке персональных данных, более четко отражен правовой смысл персональных данных (как информации, которая позволяет идентифицировать человека).

Следует отметить, что перечень информации, которая может быть признана персональной, не закреплен в действующем законодательстве ис-

черпывающим образом. Иными словами, это может быть абсолютно любая информация, которая будет позволять идентифицировать человека (его номер телефона, паспортные данные, электронная почта, личная страница в сети Интернет и т.д.). Такое перечисление может быть безграничным, особенно в нынешних условиях, когда внедряются во все сферы жизни общества информационно-телекоммуникационные средства связи, появляются новые социальные сети, Интернет-страницы и т.д. Все это накладывает отпечаток и на расширение информации, которая будет признаваться персональной. При этом в образовательной среде появляются и так называемые «облачные портфолио», которые, на наш взгляд, также хранят в себе персональные данные обучающихся. При этом правовой основы особенностей обработки таких персональных данных на сегодняшний день фактически не установлено.

Кроме того, особенно активно популяризируются и личные страницы вузов в социальных сетях. Например, посредством создания группы (личной страницы) в социальной сети образовательное учреждение делится новостями из «студенческой жизни» студентов, публикуются научные и образовательные достижения преподавателей и обучающихся, а также другая иная информация, которая зачастую фактически может быть признана в качестве персональных данных.

В данной связи следует еще раз отметить, что категория персональных данных чрезвычайно широка и включает достаточно разнообразную информацию. В связи с этим персональные данные можно классифицировать по разным основаниям.

Если обратиться к законодательному определению видов персональных данных, то мы отметим три группы, а именно:

- 1) общедоступные персональные данные;
- 2) специальные категории персональных данных;
- 3) биометрические персональные данные.

Как следствие, можно утверждать, что определение персональных данных, представленное в ФЗ «О персональных данных», имеет достаточно обширный и не в полной мере конкретизированный характер. В результате в научной литературе и правоприменительной практике возникают трудности с раскрытием содержательного аспекта персональных данных и определения той информации, которая будет охраняться положениями ФЗ «О персональных данных».

Данная проблематика особенно характерна для персональных данных, которые фигурируют в рамках образовательных отношений. Ситуация осложняется и тем, что в Федеральном законе от 29.12.2012г. № 273-ФЗ «Об образовании в Российской Федерации» (далее – ФЗ «Об образовании») законодатель достаточно формально урегулировал такой вопрос. Речь идет о том, что при определе-

нии персональных данных обучающихся вузов применяется общее определение, которое дается в ФЗ «О персональных данных», поскольку специального концепта в рамках ФЗ «Об образовании» в указанном аспекте не имеется. На наш взгляд, это достаточно существенный законодательный недостаток, который нуждается в восполнении в связи со следующими обстоятельствами.

Так, в условиях цифровой реальности персональные данные субъектов образовательного процесса являются достаточно многоаспектными. В частности, к таковым можно относить индивидуальные достижения; конференции, на которых выступал обучающийся; информацию об успеваемости и др., то есть содержательный аспект персональных данных является достаточно специфическим и обусловлен особенностями образовательных отношений. В связи с этим определение персональных данных должно быть конкретизировано с учетом той информации, которая таковой является в рамках образовательного процесса.

Более того, сама категория персональных данных на сегодняшний день является достаточно многогранной, особенно в рамках информационного пространства. Однако в рамках российского правового регулирования не установлено даже общих положений о специфике использования персональных данных в сети Интернет. При этом отсутствие общего законодательного регулирования данного вопроса затрудняет и развитие специальных правовых положений, связанных с использованием персональных данных субъектов образовательного процесса в виртуальном пространстве.

Особое внимание заслуживает подход к установлению правовой основы, который имеет место быть на международном уровне и в иных зарубежных странах.

Еще в 2002 г. была принята первая редакция Директивы 2002/58/ЕС, касающаяся обработки персональных данных и защиты неприкосновенности частной жизни в сфере электронных коммуникаций (Директива о неприкосновенности частной жизни и электронных коммуникациях). Эта Директива в первую очередь ориентирована на защиту прав пользователей, под которыми понимаются любые физические лица, использующие общедоступные средства электронной коммуникации в личных или коммерческих целях [2].

Еще одним важным нормативным правовым актом ЕС в сфере противодействия преступлениям, связанным с информационными возможностями сети Интернет, стала Директива 2013/40/EU об атаках на информационные системы. Директива устанавливает минимальные определения и санкции за преступления, связанные с атаками на информационные системы в государствах-членах, а также создает условия для сотрудничества судебных органов и полиции в преследовании таких преступных деяний.

Европейское законодательство в рассматриваемом секторе базируется на Общем регламенте 2016/679 Европейского парламента и Совета ЕС от 27 апреля 2016 г. «General Data Protection Regulation» (далее – GDPR), а также на Директиве 2002/58/ЕС от 12 июля 2002 г., затрагивающих непосредственные вопросы обработки персональных данных и защиты конфиденциальности в секторе электронных средств связи [9, с. 251].

В соответствии с п. 1 ст. 4 GDPR под персональными данными европейское законодательство подразумевает «любую информацию, которая относится к определенному (либо определяемому), физическому лицу». В данном случае физическое лицо идентифицируется в качестве полноценного «субъекта данных»). Также в рамках указанного документа отмечено, что определяемое физическое лицо может быть идентифицировано как прямо, так и косвенно, к примеру, с помощью ссылки на определенный его идентификатор (имя, идентификационный номер, данные о месторасположении, онлайн-идентификатор), либо же на основе симбиоза нескольких факторов, способствующих идентификации лица (к примеру, факторов, характерных для физической, генетической, умственной, экономической, культурной, социальной, физиологической идентичности, применимо к каждому конкретному лицу). Схожего подхода не содержится в практике российского законодателя, что обуславливает необходимость уточнения и законодательной детализации информации, присущей конечному пользователю по открытому перечню критериев.

Необходимо отметить, что в подп. «а» п. 1 ст. 6 GDPR «процесс обработки данных личного характера является законным и допустимым лишь в случае получения согласия на обработку собираемых данных от субъекта данных, включая сбор и обработку указанной информации для определенных целей». Как результат, в праве ЕС серьезное внимание уделяется вопросу реального получения от пользователя согласия на обработку данных, при идентификации понятия «согласие на обработку данных» [5, с. 169].

Обозначенный выше подход в максимальной степени детализирует принципы получения согласия от пользователей, что в целом соответствует европейскому подходу, ориентированному на защиту персональных данных. Он также может быть использован российским законодателем в контексте более полной детализации принципов получения согласия от пользователя на обработку данных, при оговорке, связанной с законностью данного сбора и исключениях для таких сфер, как национальная безопасность, судебные разбирательства, обеспечение прав и законных интересов граждан.

С другой стороны, важный аспект содержится и в п. 5 ст. 25 GDPR, в рамках которого европейским законодателем отмечено, что сторона, ответственная за обработку данных, берет на себя обязательство по реализации и осуществлению соответ-

ствующих технических, организационных мер – главным образом для того, чтобы по умолчанию обрабатывались исключительно те персональные данные, которые необходимы для каждой конкретной цели обработки (отказ от полного сбора всех данных с дальнейшим выделением лишь «нужных» для конкретной цели пользовательских данных).

Это видится также достаточно важным, поскольку указывает на возможность сбора не всей информации о пользователе, а делает возможным сбор только тех данных, которые играют роль в процессе обработки информации («необходимы для каждой конкретной цели обработки»). Данный подход также должен способствовать последовательной модернизации защиты прав субъектов образовательного процесса и позволяет осуществлять их защиту в случае несанкционированного сбора персональной информации, что обуславливает необходимость рассмотрения возможности интеграции данного подхода и в отечественные правовые конструкции.

Другой аспект европейского законодательно-го регулирования персональных данных расположен в рамках Директивы «О конфиденциальности и электронных средствах связи», где детализирован правовой режим процессов, связанных с обработкой персональных данных, который осуществляется в рамках использования сетей электронной связи. Характерные требования отражены в п. 3 ст. 5 Директивы, где отмечено, что «хранение информации, получение доступа к информации, которая сохранена и содержится на терминальном оборудовании абонента или пользователя, возможно только при условии факта дачи согласия со стороны заинтересованного абонента или пользователя». Доступ к данной информации ранее осуществлялся в соответствии с утратившей силу Директивой 95/46/ЕС, в рамках которой также отмечалось, что «пользователь или абонент может отказаться от предоставления согласия на обработку информации» [3, с. 38].

В указанных условиях получение согласия либо отказ от дачи согласия предполагает использование уведомлений «pop-up», которые определяются в качестве окон и появляются на экране автоматическим образом в процессе открытия веб-страницы. Такой законодательный подход может быть связан с ориентацией ЕС на предоставление пользователю, зарегистрированному абоненту возможности дать свое согласие (или отказаться), на использование cookies, принцип работы которых связан, кроме информационной составляющей, с отслеживанием и анализом поведения пользователя на конкретном сайте.

Важно учитывать, что cookies могут использоваться и в широком спектре других задач, в результате чего в случаях, при которых использование информации, содержащейся в cookies, не предполагает обработку данных и связано, к примеру, с обеспечением работы веб-ресурса, согласия пользователя не требуется. Данный подход также может

быть применен отечественным законодателем, но с оговоркой, что отказ от предоставления согласия на обработку данных не должен приводить к запрету использования каждого ресурса, запрашивающего подобное разрешение.

В конечном итоге необходимо учитывать и тот факт, что согласие пользователя может быть получено и в рамках принятия общих условий работы веб-ресурса, в результате чего, по оценкам экспертов, логика европейского законодателя, отраженная в европейском праве, предполагает наличие похода, именуемого «opt-in», в рамках которого допускается активный контроль деятельности пользователей.

Необходимо отметить стратегическое значение упомянутых ранее обязанностей для конечного пользователя сети Интернет. В данном случае, обязанность оператора веб-сайта по предоставлению пользователю полной, прозрачной и ясной информации о целях обработки персональных данных играет определяющую роль в рамках защиты прав и интересов пользователей.

Большинство субъектов образовательного процесса не имеют четкого понимания и не осведомлены в полной мере о специфике предоставляемых ими данных, а также их целевом назначении.

Кроме того, 10 января 2017 г. Европейской комиссией был подготовлен новый проект Регламента, суть которого направлена на замещение рассматриваемой ранее Директивы «О конфиденциальности и электронных средствах связи», новым документом (далее – Регламент). В рамках указанного документа отмечена обязанность владельцев ресурсов запрашивать согласие на обработку персональных данных с помощью программного обеспечения (в соответствии с пар. 22 Регламента), выводя данную обязанность из спектра обязательств интернет-сайтов.

В мае 2018 г. был принят GDPR (General Data Protection Regulation, Общий регламент по защите данных) – директива Европейского союза, призванная устранить пробелы в законодательстве Европейского союза о персональных данных, в соответствии с которой у пользователей появился ряд прав, закрепленных на законодательном уровне, нарушение которых грозит достаточно большим размером штрафом.

Стоит полагать, что такого рода подход в европейском законодательстве связан, главным образом, с тем фактом, что в условиях интенсивного развития информационных технологий пользователи, по сути, перегружены регулярными запросами на согласие предоставить те или иные данные. Акцент на перенос обязанности запроса согласия пользователя на программное обеспечение может позволить, как пользователям, так и владельцам Интернет-ресурсов, снизить временные, а также финансовые затраты (в отношении владельцев веб-сервисов) на поддержание соответствующей ин-

фраструктуры. Однако также важно отметить, что практическое его применение способствует хоть и ситуативному, но снижению риска влияния «человеческого фактора», поскольку стабильно работающее и протестированное программное обеспечение сможет безошибочно идентифицировать и факт согласия, и факт отказа пользователя от предоставления данных.

Как итог, указанный подход также может быть применен и российским законодателем путем дополнения соответствующими положениями ФЗ «О персональных данных».

Таким образом, рассмотренный подход европейского законодателя ориентируется на приоритетную защиту персональных данных. Главным образом это связано с тем, что в нынешнее время «безопасность» имеет важное значение для реализации образовательного процесса. Мы можем констатировать факт того, что в нынешних реалиях появляются новые угрозы безопасности вузов, которые связаны с информационным пространством. В связи с этим встает вопрос о выработке более новых и совершенных способов, которые смогут обеспечить указанную безопасность субъектов образовательной среды в условиях эволюции цифровых технологий.

Соответственно, вопрос информационной безопасности использования цифровых технологий в образовательном процессе является одним из ключевых. Правонарушения, связанные с использованием информационных технологий в сети Интернет, совершаются методом кражи информации о субъектах образовательного учреждения, которая, как правило, находится в закрытом доступе, путем хакерских атак на информационные сети, кражи паролей с использованием фишинговых сайтов или программ и т.д.

В научной среде в последние годы подчеркивается проблематика киберугроз, которые являются следствием информационной революции. Ученые полагают, что «защита от киберугроз и обеспечение кибербезопасности становятся все более актуальной проблемой и требуют государственно-правового регулирования. Действительно, пользуясь цифровыми и информационными системами, вузы подвергают риску потерю данных как самих субъектов образовательного процесса, так и данных всей организации, а также вторжение в информационную систему посторонних лиц, что, безусловно, может повлечь необратимую потерю каких-либо материалов, учетов, иной ценной информации [6, с. 358].

В данной связи увеличивается рост и мошеннических действий в сфере цифровых технологий. Безусловно, в качестве последствий могут выступать как потеря данных, так и получение доступа к таким данным мошенниками, которые в последующем могут ими распорядиться по своему распоряжению. В свою очередь, это может приве-

сти к нарушению режима обработки и персональных данных субъектов образовательного процесса.

Как следствие, цифровое обеспечение технико-правового регулирования безопасности субъектов образовательного процесса на сегодняшний день имеет ряд проблем. На наш взгляд, для обеспечения защиты информационных ресурсов возникает необходимость разработки политики информационной безопасности, включающей обязательные требования к защите информационных ресурсов и информации, распространение и предоставление которых ограничено, а также требования к контролю за обеспечением безопасности и защиты информационных ресурсов. Представляется, что это позволит частично решить проблему, связанную с кибербезопасностью субъектов образовательного процесса. Более того, особый акцент со стороны законодателя должен быть сделан и на совершенствовании правового регулирования в аспекте установления мер, которые будут способствовать созданию безопасных условий для осуществления образовательного процесса в условиях цифровой реальности. В этой связи видится целесообразным рассматривать этот вопрос с точки зрения блокчейн-технологии [4, с. 178].

Самыми популярными пользователями технологии блокчейн считаются, в первую очередь, финансовые учреждения и юридические лица, остро нуждающиеся в применении технологий информационной безопасности. По мере расширения использования блокчейна в других отраслях и повышения доверия к этой технологии, в частности, для обеспечения безопасности контрактов, ведения реестров собственности, обеспечения целостности данных и использования многих других функций, растет число сторон, заинтересованных в получении информации о преимуществах этой технологии. В данной связи и образовательные учреждения постепенно начинают переходить на использование технологии блокчейн и больших данных.

На сегодняшний день, возможность взлома блокчейна сведена к минимуму, хотя такие разновидности хакерских угроз, как «Атака 51 %» (Атака 51% – это атака на блокчейн, где один субъект или организация захватывает наибольшую часть хешрейта, что может привести к нарушениям работы сети) или «Атака Сивиллы» (Создание большого количества личностей (identities) для искажения распределенного консенсуса), остаются потенциальной угрозой для блокчейна. Преимуществом такой технологии следует назвать автономность: основы функционирования блокчейна заложены в его программном коде, который представляет собой программное обеспечение с открытым кодом.

Как отмечается в научной среде, «данное качество позволяет существенно повысить уровень доверия, так как каждый участник может ознакомиться со структурой блокчейна и быть уверенным, что она будет изменена только при достиже-

нии консенсуса между большинством участников этой системы. Нельзя не заметить, что реализация подобных условий требует высокой профессиональной подготовки в области программирования и криптографии, однако само наличие этой возможности можно считать прорывом в сфере развития высоких технологий» [10, с. 67].

В октябре 2018 года в Москве прошло заседание международного технического комитета ИСО 307 «Блокчейн и технологии распределенных реестров» (Blockchain and distributed ledger technologies), в работе которого приняли участие более 100 экспертов международного уровня в области блокчейн технологий, информационной безопасности и государственного управления из 20 стран.

Основными вопросами к обсуждению стали информационная безопасность, защита персональных данных, правовое регулирование деятельности в сфере блокчейн, а также сценарная техника описания взаимодействий.

Международный технический комитет ИСО 307 был создан в 2016 году в составе шести рабочих групп. Деятельность комитета направлена на внедрение инноваций, эффективное управление и использование технологий блокчейн и распределенных реестров в бизнес-индустрии и государственном управлении. В рамках ТК ИСО ведется работа по унификации терминологии и эталонной архитектуре, а также проводятся исследования в области блокчейн-технологий.

После заседания в Москве состоялся международный форум «Блокчейн в цифровой экономике», в работе которого приняли участие эксперты технического комитета и все заинтересованные практики применения блокчейн-технологий. Открывая дискуссионную сессию «Блокчейн как потенциальный катализатор изменений в цифровой экономике», заместитель Руководителя Росстандарта Антон Шалаев отметил, что «стандартизация должна быть «нацелена» на решение новых задач, которые ставит процесс цифровой трансформации. В условиях, когда тематическую повестку стандартизации формирует бизнес, новые стандарты должны стать технологическим катализатором инновационных процессов и распространения цифровых технологий» [1].

Кроме того, во внимание следует брать и возможности такой технологии, как «Большие данные».

На сегодняшний день под большими данными, как правило, понимаются большие массивы данных, отличающиеся, главным образом, такими характеристиками, как объём, разнообразие, скорость обработки и/или вариативность, которые требуют использования технологии масштабирования для эффективного хранения, обработки, управления и анализа.

Так, например, в США правительство взяло на себя ведущую роль в осуществлении «Плана

исследований и разработок в области больших данных» в 2012 г., а правительства Англии, Франции и Японии разработали соответствующие «Планы и стратегии развития данных» и интегрировали цифровые технологии. Так, в этих странах технологии больших данных широко используются в государственном управлении для его улучшения в регионах, предоставления государственных услуг, разработки политики и участия граждан в государственном управлении. Несмотря на то, что технологии были в основе развития США в течение последних нескольких десятилетий, официальное признание они получили во время пребывания на посту президента Б. Обамы, который придавал большому данным ключевое значение. Газета «Washington Post» назвала Б. Обаму президентом больших данных за его ответственные решения по запуску инициативы «data.gov» и инвестиции в размере 200 млн долларов в исследования и разработки в области больших данных. Начиная с размещения всех правительственных записей в открытом доступе и заканчивая массовым перехватом телекоммуникационных данных, большие данные в США активно используются в государственном управлении. Однако, прежде чем упорядочить большие данные для полноценного использования, американские государственные служащие реализовали много пробных проектов. Например, в сфере образования количество данных, собираемых через онлайн-формы, резко возрастает. Поскольку в США хорошо известны системы дистанционного обучения в совокупности с недавним всплеском рационализации электронного обучения из-за пандемии, рынок «Edtech» в стране набрал обороты. Это побудило правительство изучить возможность использования больших данных в образовании. Стремясь рационализировать большие данные в образовании, Министерство образования США инициировало национальную информационную панель, которая собирает информацию о государственных школах по стране в целом. Приборная панель отслеживает перспективы индустрии образования страны и вклад в исследования. Кроме того, штаты и государственные школы также предпринимают шаги по использованию больших данных в своей повседневной работе [8, с. 88].

Штат Мичиган внёс свой вклад в использование больших данных в образовании, создав панель мониторинга, которая оценивает эффективность, сохранение или регресс в различных областях. Панель инструментов фокусируется на четырнадцати показателях результатов учащихся, подотчетности школы, культуре обучения, соотношения цены и качества, высшего образования и пр. Государственные школы Чикаго используют программное обеспечение под названием «Impact» (программа управления обучением и инструмент академического общения) для отслеживания

успеваемости учащихся в таких областях, как: управление информацией об учащихся, управление учебными программами и инструментами, управление услугами, журнал оценок для родителей и учащихся. Через этот сайт учителя могут инициировать публичные уроки, и любой, у кого есть к нему доступ, может использовать его для стандартизации результатов тестов, эталонных оценок, учебных ресурсов и дискуссионных форумов.

Калифорнийский университет в Сан-Диего имеет другой тип панели инструментов для больших данных. Это – финансовая панель, которая фокусируется на финансовых и капитальных ресурсах рынка «Edtech». Учреждение отслеживает спонсируемые исследования и получает данные из университетских систем, а также отображает и обновляет информацию по желанию пользователя.

Вместе с тем, в настоящее время в Соединенных Штатах нет законов, специально регулирующих аспекты применения больших данных в образовании. Однако существуют некоторые косвенные правила для компаний и учебных заведений, которые хранят большие данные. Учебные заведения, стремящиеся принимать участие в общей системе и использовать большие данные должны гарантировать, что предлагаемая ими деятельность соответствует законам о конфиденциальности, а также собственным политикам конфиденциальности и всем применимым договорным требованиям. Однако в стране существует необходимости принятия «Положения о больших данных в образовании». Представляется, что основной вектор государственной политики также должен быть направлен на возможности использования больших данных в сфере образования и детального регулирования данного вопроса с целью защиты и персональных данных образовательного процесса при использовании таких информационных «новшеств».

То есть следует отметить, что организационные и технические проблемы обеспечения безопасности персональных данных обучающихся вузов могут быть разрешены посредством использования технологий блокчейн и большие данные, которые на сегодняшний день имеют ряд преимуществ. Однако для их эффективного использования важно совершенствовать и правовую основу с учетом данного направления. В частности, установить базовые положения о технологии блокчейн (ее правовое положение, определение, особенности использования, гарантии безопасности и др.). Такое законодательное решение, на наш взгляд, возможно в рамках самостоятельного закона, который необходимо принять.

Таким образом, нами были выработаны следующие концептуальные предложения по совершенствованию правового регулирования персональных данных вузов.

1. Необходимо систематизировать положения о персональных данных субъектов образовательного процесса в рамках ФЗ «Об образовании».

2. Предлагаем установить легальное определение персональных данных в ФЗ «Об образовании» с учетом специфики информации об обучающихся, которая относится к такой категории.

3. Следует дополнить положения ФЗ «О персональных данных» разделом «О конфиденциальности данных в рамках электронных коммуникаций», в котором закрепить обязанность для владельцев Интернет-ресурсов применять специальное программное обеспечение, отвечающее за работу с пользователями в контексте получения от них согласия на предоставление личных данных (а в случае отсутствия – отвечающего ПО за отказ от навязчивой отправки запросов или блокирования доступа к сайту, его сегментам либо функционалу).

4. В Общем регламенте по защите данных (General Data Protection Regulation, сокращенно GDPR) установлены права граждан по контролю за их персональными данными. Пользователи имеют право запрашивать подтверждение факта обработки их данных, уточнять источник получения персональных данных и требовать их удаления. Это

право гарантировано ст. 13 и 14 Регламента. Представляется, что Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных» также следует дополнить нормами, позволяющими гражданам управлять информацией о себе в том случае, если такая информация собирается о них в интернет-пространстве с помощью информационных технологий.

5. Помимо разрешения проблем правового характера следует особое внимание уделить организационным и техническим аспектам обеспечения безопасности персональных данных обучающихся вузов. В рамках реализации данного направления акцент должен быть сделан на использовании образовательными организациями технологии блокчейн.

Представляется, что предложенные нами направления по совершенствованию правового регулирования правовой охраны персональных данных субъектов образовательного процесса позволят снизить количество нарушений, которое на сегодняшний день имеет тенденцию к увеличению с учетом широкого использования виртуального пространства в деятельности высших учебных заведений.

Список источников

1. В Москве состоялось заседание международного технического комитета ИСО по блокчейну [Электронный ресурс]. URL: https://news.metrologu.ru/standartizatsiya/standartizatsiya_5158.html (дата обращения: 31.03.2023).
2. Гнедков А.В., Нищик А.В. Особенности распространения персональных данных в последней редакции законодательства о персональных данных // Научно-методическое обеспечение оценки качества образования. 2022. № 1 (15). С. 49–52.
3. Сысоева Л.А. Стандартизация моделей взаимодействия участников обработки персональных данных в информационных системах персональных данных // Международный журнал прикладных и фундаментальных исследований. 2022. № 5. С. 33–38.
4. Алимбаев В.В., Листопадова Е.В. Организация защиты персональных данных и ответственность за несоблюдение требований законодательства в области защиты персональных данных // Природа. Человечество. Культура: материалы Третьего Международного научно-просветительского форума, Кисловодск, 4–8 октября 2022 года / под общей редакцией С.Е. Туркулец, Е.В. Листопадовой. Хабаровск: Дальневосточный государственный университет путей сообщения, 2022. С. 176–182.
5. Каирбаева Л.К. Защита персональных данных в международном и Европейском праве // Вестник Института законодательства и правовой информации Республики Казахстан. 2020. № 5 (63). С. 168–174.
6. Карпова Н.А. К вопросу о защите персональных данных в условиях цифровой трансформации российского образования // Тенденции повышения конкурентоспособности и экспортного потенциала продукции агропромышленного комплекса: сборник материалов международной научной конференции, Смоленск, 17 ноября 2021 года. Том 2. Смоленск: ФГБОУ ВО Смоленская ГСХА, 2021. С. 355–360.
7. Рожкова М.А. Право в сфере Интернета: сборник статей / М.З. Али, Д.В. Афанасьев, В.А. Белов и др.; рук. авт. кол. и отв. ред. М.А. Рожкова. М.: Статут, 2018. 528 с.
8. Румянцева Е.Л. Об обеспечении безопасности персональных данных в сфере образования // Слабые качества современного гуманитарного образования: материалы XV международной научно-методической конференции, Тольятти, 12–13 октября 2017 года / Филиал ЧОУ ВО «СаГА» в г. Тольятти; редкол.: Р.В. Закомолдин, С.В. Быков. Тольятти: Самарская гуманитарная академия, 2018. С. 86–91.
9. Фастович Г.Г. Защита персональных данных в системе высшего образования // Наука и образование: опыт, проблемы, перспективы развития: Материалы международной научно-практической конференции, посвященной 70-летию ФГБОУ ВО Красноярский ГАУ, Красноярск, 19–21 апреля 2022 года. Красноярск: Красноярский государственный аграрный университет, 2022. С. 250–252.
10. Дерюгин Р.А. О современных способах совершения мошенничества, связанного с использованием персональных данных пользователей сети Интернет // Криминалистика: вчера, сегодня, завтра. 2023. № 1 (25). С. 65–74.

References

1. V Moskve sostoyalos' zasedanie mezhdunarodnogo tekhnicheskogo komiteta ISO po blokcheinu [A meeting of the ISO International technical committee on blockchain was held in Moscow]. (In Russ.). Available at: https://news.metrologu.ru/standartizatsiya/standartizatsiya_5158.html (accessed 31.03.2023).
2. Gnedkov A.V., Nishik A.V. Osobennosti rasprostraneniya personal'nykh dannykh v poslednei redaktsii zakonodatel'stva o personal'nykh dannykh [Features of the dissemination of personal data in the latest version of the legislation on personal data], *Nauchno-metodicheskoe obespechenie otsenki kachestva obrazovaniya* [Scientific and methodological support of assessment the quality of education], 2022, no. 1(15), Pp. 49-52. (In Russ.).
3. Sysoeva L. A. Standartizatsiya modelei vzaimodeistviya uchastnikov obrabotki personal'nykh dannykh v informatsionnykh sistemakh personal'nykh dannykh [Standardization of models of interaction of participants of personal data processing in personal data information systems], *Mezhdunarodnyi zhurnal prikladnykh i fundamental'nykh issledovaniy* [International Journal of Applied and Fundamental Research], 2022, no. 5, pp. 33-38. (In Russ.).
4. Alimbayev V. V., Listopadova E.V. Organizatsiya zashchity personal'nykh dannykh i otvetstvennost' za nesoblyudenie trebovaniy zakonodatel'stva v oblasti zashchity personal'nykh dannykh [Organization of personal data protection and responsibility for non-compliance with the requirements of legislation in the field of personal data protection], *Priroda. Chelovek. Kul'tura* [Nature. Human. Culture], Materials of the Third International Scientific and Educational Forum, Kislovodsk, 04-08 October 2022, under the general editorship of S.E. Turkulets, E.V. Listopadova. Khabarovsk, Far Eastern State University of Railway Transport Publ., 2022, pp. 176-182. (In Russ.).
5. Kairbaeva L. K. Zashchita personal'nykh dannykh v mezhdunarodnom i Evropeiskom prave [Protection of personal data in international and European law], *Vestnik Instituta zakonodatel'stva i pravovoi informatsii Respubliki Kazakhstan* [Bulletin of the Institute of Legislation and Legal Information of the Republic of Kazakhstan], 2020, no. 5(63), pp. 168-174. (In Russ.).
6. Karpova N. A. K voprosu o zashchite personal'nykh dannykh v usloviyakh tsifrovoi transformatsii rossiiskogo obrazovaniya [On the issue of personal data protection in the conditions of digital transformation of Russian education], *Tendentsii povysheniya konkurentosposobnosti i eksportnogo potentsiala produktsii agropromyshlennogo kompleksa* [Trends in increasing the competitiveness and export potential of agro-industrial products], proceedings of the International scientific conference, Smolensk, November 17, 2021, volume 2. Smolensk, Smolensk State Agricultural Academy Publ., 2021, pp. 355-360. (In Russ.).
7. Rozhkova M. A. Pravo v sfere Interneta: sbornik statei [Law in the field of the Internet: a collection of articles], M.Z. Ali, D.V. Afanasyev, V.A. Belov, etc.; hand. author col. and ed. M.A. Rozhkova. Moscow, Statute, 2018, 528 p. (In Russ.).
8. Rumyantseva E. L. Ob obespechenii bezopasnosti personal'nykh dannykh v sfere obrazovaniya [On ensuring the security of personal data in the field of education], *Slagaemye kachestva sovremennogo gumanitarnogo obrazovaniya* [Components of the quality of modern humanitarian education], Materials of the XV International Scientific and Methodological Conference, Togliatti, October 12-13, 2017 / Branch of CHOU VO "SaGA" in Togliatti; editor: R.V. Zakomoldin, S.V. Bulls. Togliatti, Samara Humanitarian Academy Publ., 2018, pp. 86-91. (In Russ.).
9. Fastovich, G. G. Zashchita personal'nykh dannykh v sisteme vysshego obrazovaniya [Protection of personal data in the system of higher education], *Nauka i obrazovanie: opyt, problemy, perspektivy razvitiya* [Science and education: experience, problems, development prospects], Materials of the international scientific and practical conference dedicated to the 70th anniversary of the Krasnoyarsk State University, Krasnoyarsk, April 19-21, 2022. Krasnoyarsk, Krasnoyarsk State Agrarian University Publ., 2022, pp. 250-252. (In Russ.).
10. Deryugin, R. A. O sovremennykh sposobakh soversheniya moshennichestva, svyazannogo s ispol'zovaniem personal'nykh dannykh pol'zovatelei seti Internet [On modern methods of committing fraud related to the use of personal data of Internet users], *Kriminalistika: vchera, segodnya, zavtra* [Criminalistics: yesterday, today, tomorrow], 2023, no. 1(25), pp. 65-74. (In Russ.).

ИНФОРМАЦИЯ ОБ АВТОРЕ

Абдусаламов Руслан Абдусаламович, заведующий кафедрой информационного права и информатики Юридического института Дагестанского государственного университета, кандидат педагогических наук, доцент, г. Махачкала, Российская Федерация. E-mail: Abd-rus@yandex.ru

INFORMATION ABOUT THE AUTHOR

Abdusalamov Ruslan Abdusalamov, Head of the Department of Information Law and Informatics of the Law Institute of Dagestan State University, Candidate of Pedagogical Sciences, Associate Professor, Makhachkala, Russian Federation. E-mail: Abd-rus@yandex.ru

Поступила в редакцию 19.04.2023 г.;
одобрена после рецензирования 04.05.2023 г.;
принята к публикации 15.05.2023 г.

Received 19.04.2023; approved after reviewing
04.05.2023; accepted for publication 15.05.2023.