КУЛЬТУРА И ЦИВИЛИЗАЦИЯ / CULTURE & CIVILIZATION

УДК 339.9
DOI: 10.24411/2413-693X-2019-10310

Правовые аспекты управления big data в странах БРИКС и ШОС

ФЕДУЛОВ Игорь Николаевич,
Югорский государственный университет (Ханты-Мансийск, ХМАО-Югра, Российская Федерация);
доктор философских наук, доцент, профессор кафедры истории, философии и права

КВАЧ Ирина Валериевна
Югорский государственный университет (Ханты-Мансийск, ХМАО-Югра, Российская Федерация);
преподаватель; irina.kvach2015@yandex.ru

Аннотация. Настоящая статья посвящена обзору законодательства в сфере персональных данных стран, входящих в БРИКС и Шанхайскую организацию сотрудничества, на предмет отражения феномена «больших данных». Приведены подходы к определению «больших данных», а также существующие точки зрения на необходимость их правового регулирования. Проведен анализ существующего законодательства о персональных данных на предмет регулирования оборота «больших данных». Показано, что «большие данные» не укладываются в полной мере в действующие нормы законодательства о персональных данных и существует необходимость выработки правового определения феномена «больших данных», независимого от персональной информации, а также осмысления и уточнения ряда фундаментальных понятий информационного права, таких как, например, «личная тайна», в свете новых технологических реалий.

Ключевые слова. Большие данные, big data, персональные данные, защита информации, БРИКС, ШОС, интернет.

Для цитирования: Федулов И.Н., Квач И.В. Правовые аспекты управления Big Data в странах БРИКС и ШОС // Сервис Plus. 2019. Т.13. №3. С. 85-92. DOI: 10.24411/2413-693X-2019-10310.
Статья поступила в редакцию: 10.09.2019.
Статья принята к публикации: 10.10.2019.

Legal aspects of big data management in BRICS and SCO countries

Igor N. FEDULOV
Yugra State University (Khanty-Mansi Autonomous Okrug – Yugra, Khanty-Mansiysk, Russia);
Doctor of Philosophy, associate professor, Professor, department of history, philosophy and law

Irina V. KVACH
Yugra State University (Khanty-Mansi Autonomous Okrug – Yugra, Khanty-Mansiysk, Russia);
Lecturer; irina.kvach2015@yandex.ru,

Abstract. This article is devoted to a review of legislation in the field of personal data of countries belonging to the BRICS and the Shanghai Cooperation, aimed at reflecting the phenomenon of "big data". There were considered the approaches to the definition of "big data", as well as existing points of view on the need for their legal regulation. There was analyzed the existing legislation on personal data for the regulation of the turnover of "big data". It is shown that "big data" does not fully fit into the current legislation on personal data and there is a need to develop a legal definition of the phenomenon of "big data", independent of personal information, as well as understanding and clarifying a number of fundamental concepts of information law, such as for example, “personal secret” in the light of new technological realities.

Key words: big data, personal data, information security, BRICKS, SCO, internet.

For citation: Fedulov, I. N., & Kvach, I. V. (2019). Legal aspects of big data management in BRICS and SCO countries. Service plus, 13(3), 85-92. DOI: 10.24411/2413-693X-2019-10310 (In Russ.)

Submitted: 2019/09/10.

Accepted: 2019/10/10.

В последние годы вопросы, связанные с технологиями обработки больших массивов данных, неизменно пробуждают повышенный интерес со стороны общества. В создании эффективно действующего механизма обработки массивов обезличенных данных заинтересованы и государство, и бизнес. Однако, несмотря на значимость проблемы, до сих пор не до конца отлажено взаимодействие различных ведомств и операторов, участвующих в сборе и обработке Big Data[1]. Кроме того, не всегда ясно что именно понимается под «большими данными».

На сегодняшний день в литературе существует два подхода к их определению. С одной стороны, под «большими данными» понимаются большие массивы «обезличенных» данных, как структурированных, так и неструктурированных, которые нельзя сопоставить с конкретным пользователем без привлечения дополнительной информации, но которые тем не менее могут содержать о нем некоторую уникальную информацию, доступную после соответствующего анализа (IP-адреса посещенных страниц, информация о действиях на посещаемых страницах, запросы в поисковых системах и соцсетях, прочая информация из соцсетей, камер видеонаблюдения, данные геопозиции и т.п.). С другой — технологии, а также результат статистической обработки и анализа указанных массивов данных. В данной работе обзор законодательства о персональных данных проведен в той мере, в которой оно соотносится с новейшими тенденциями в сфере технологий работы с данными, в том числе и с «большими данными» в рамках приведенных нами выше определений.

Существует две точки зрения на необходимость правового регулирования в сфере «больших данных». Первая представлена интересами государства и сводится к двум аргументам: необходимость «информационного суверенитета» государства, понимаемого в основном как монопольный доступ к персональным данным граждан, физически размещенным на серверах на территории страны, и повышение эффективности средств контроля и управления обществом, включение Big Data в правовую систему государства. Вторая точка зрения отражает необходимость правового регулирования в сфере «больших данных» с точки зрения пользователей и включает в себя четыре аспекта: ограниченные возможности воздействия рядовых пользователей на крупные корпорации в вопросе сохранности и конфиденциальности персональных данных; опасения «диктатуры данных» т.е. дискриминации на основании результатов статистического анализа Big Data; «эффект охлаждения» (искусственное сдерживание развития Интернет-сервисов из-за опасения пользователей оставить «цифровые следы») и, наконец, «эффект информационных пузырей» (побочный эффект фильтрации контента на основе статистического анализа Big Data, приводящий к однобокому, подсознательно желаемому освещению событий, игнорирующему альтернативные точки зрения) [1, с. 32-34]. Указанные соображения стимулируют ожидания общества в части государственных инициатив, направленных на защиту частной жизни в том числе и в виртуальном пространстве, важнейшей составляющей которой являются гарантии конфиденциальности персональных данных граждан, понимаемых в современных условиях весьма широко. Однако трактовка «больших данных» как всего

[1] Big Data (в пер. с англ. «Большие данные») — устоявшийся термин, означающий технологии статистической обработки и анализа большого количества различной нетекстовой пользовательской информации, позволяющие на основании результатов анализа делать выводы о склонностях и предпочтениях индивида.

лишь разновидности персональных несет в себе неочевидные, но при этом весьма серьезные правовые риски, поскольку сущность Big Data в ряде аспектов противоречит принципам законодательства о персональных данных. Как показывает недавнее исследование, проведенное сотрудниками Высшей школы экономики, «большие данные» несовместимы с принципом «ограничения обработки персональных данных заранее определенными целями», а также с принципом «информированного, конкретного и сознательного согласия как главного основания легитимации обработки персональных данных». Кроме того, процедура обезличивания, предшествующая обработке ряда персональных данных и требуемая законами ряда стран, не является гарантией анонимности данных в эпоху Big Data [2]. Тем не менее, в силу отсутствия специального законодательства, регламентирующего оборот «больших данных», до недавнего времени государства были вынуждены следовать по паллиативному пути, пытаясь использовать для регулирования оборота «больших данных» существующее законодательство о персональных данных, несмотря на очевидные сущностные различия этих двух феноменов.

В Российской Федерации, ратифицировавшей в 2005 году Конвенцию Совета Европы о защите физических лиц при автоматизированной обработке персональных данных 1981 г., в её развитие в 2006 году был принят Федеральный Закон «О персональных данных»[2]. В настоящее время оборот «больших данных» в нашей стране, наряду с настоящим федеральным законом, регулируется также и Федеральным Законом №149-ФЗ от 27 июля 2006 г. «Об информации, информационных технологиях и о защите информации». 23 октября 2018 года в Государственную Думу РФ внесен законопроект № 571124-7, содержащий поправки к закону №149-ФЗ, который, однако, до настоящего времени находится на доработке профильной группы[3]. Таким образом, на сегодняшний день Российская Федерация является одной из немногих стран мира (после Евросоюза и Великобритании), которая стремится законодательно регулировать оборот Big Data. Однако Общеевропейский регламент по защите данных (GDPR)[4], принятый в мае 2018 года, не дает персонального определения «большим пользовательским данным», причисляя к ним и личную информацию (персональные данные). Отечественный проект федерального закона дает определение «большим пользовательским данным» как не содержащим персональной информации о пользователе, обязывает получать согласие пользователя на идентификацию его IP-адресов, в случае обработки информации с большого (более ста тысяч) адресов – уведомлять государство. В свою очередь, партнеры Российской Федерации по БРИКС и ШОС предпочитают следовать традиционному пути, фактически отождествляя «большие данные» и «обезличенные персональные данные».

В Бразилии оборот «больших данных» регулируется двумя законодательными актами: Законом №13709 от 14 августа 2018 «О защите персональных данных» и Законом №12965 от 23 апреля 2014 (the “Бразильский закон об Интернете”)[5]. Они определяют правовые основания для обработки персональных данных, принципы их обработки, права субъектов данных, вопросы коммуникации, объединения и международной передачи данных, обязанности акторов и административные санкции. Законодательство Бразилии о персональных данных предусматривает подразделение пользовательских данных на два множества: «персональные» и «анонимизированные» по принципу возможности идентификации субъекта данных существующими техническими средствами. Из всего множества персональных данных выделяется подмножество «конфиденциальных персональных данных», в которое включаются сведения о расовом или этническом происхождении, религиозных и политических убеждениях, членстве в профсоюзах или религиозных, философских или политических организациях, данные, касающиеся здоровья или половой жизни, генетические или биометрические данные, когда они связаны с физическим лицом. Субъекты данных имеют весьма широкие права. Например, они имеют право требовать доступа к данным, исправления неполных, неточных или устаревших данных, анонимизации, блокирования или удаления ненужных либо чрезмерных данных.

В Китайской Народной Республике Big Data играют роль технологической основы системы социального рейтинга китайских граждан (система «социального кредита») [3, 4]. Несмотря на важность для данной цели правового статуса личной информации граждан и, в частности, «больших данных», до последнего

[2] Федеральный закон №152-ФЗ «О персональных данных» от 27 июля 2006 г.
[3] Законопроект № 571124-7 «О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации"».
[4] General Data Protection Regulation (GDPR). URL: https://gdpr-info.eu/ (Дата обращения: 18.09.2019).
[5] Law No. 13,709, of August 14, 2018 - Provides for the protection of personal data and changes Law No. 12,965, of April 23, 2014 (the “Brazilian Internet Law”). URL: https://www.pnm.adv.br/wp-content/uploads/2018/08/Brazilian-General-Data-Protection-Law.pdf (Дата обращения: 18.09.2019).

времени отсутствовал специальный закон, регулирующий оборот персональных данных, подобный европейскому GDPR. В настоящий момент сфере защиты данных действуют три основополагающих документа: Решение Постоянного комитета Национального Народного Конгресса об усилении защиты сетевой информации от 28 декабря 2012 года (National People's Congress Standing Committee Decision concerning Strengthening Network Information Protection)[6], Закон о кибербезопасности (China's Cybersecurity Law), вступивший в силу 1 июня 2017 года[7], и Национальный стандарт по защите персональной информации (GB/T 35273-2017 Information Technology – Personal Information Security Specification), вступил в силу 1 мая 2018 года[8].

Первый в числе названных документов определяет общие требования к провайдерам, выступающим в качестве операторов сбора данных. Поставщики цифровых услуг должны в обязательном порядке указывать цель, методы и возможности сбора информации, обязаны получать согласие лица, чьи данные собираются, а также публиковать свои правила сбора и использования личной информации. Перед тем, как получить от провайдера услуги доступа, пользователи обязаны предоставить реальную информацию о личности. Также существует прямой запрет провайдеру отправлять коммерческую электронную информацию (в т.ч. рекламу) конечному пользователю без его согласия.

Подход к определению «конфиденциальной личной информации» отличается от принятого в странах Европы: таковой считаются не просто данные определённого типа, а любая личная информация, «которая, в случае утери или ненадлежащего использования может подвергнуть опасности людей или имущество, нанести вред личной репутации и психическому и физическому здоровью или привести к дискриминационному обращению (например, национальные идентификационные номера, учётные данные, банковские и кредитные реквизиты, точное местоположение человека, информацию о владении недвижимостью и информацию о несовершеннолетнем (младше 14 лет))» [5]. К «личной информации» относятся: аппаратные серийные коды устройства, IP-адреса, записи отслеживания веб-сайта и уникальные идентификаторы устройства. Отказ пользователя от предоставления дополнительной информации может служить основанием для отказа провайдера предоставлять дополнительные услуги, но не может служить основанием для отказа от предоставления основных бизнес-продуктов (согласно поправкам, внесенным в Стандарт в январе 2019 года, предлагается исключить «исполнение контракта» из существующих исключений для требования о согласии [6]).

Характерно, что в законодательстве КНР существует требование, сходное с «принципом ограничения цели» GDPR: все виды использования информации, включая вторичное использование, должны быть разумно связаны с первоначальной целью сбора данных и должны быть повторно авторизованы в других случаях [5]. Однако право на удаление данных реализовано без исключений, характерных для GDPR, что, например, позволяет отклонить запросы на удаление в интересах свободы выражения мнений и информации или научных исследований, однако может входить в конфликт с другими нормами законодательства. Право на переносимость данных возникает в более широком диапазоне ситуаций, но ограничивается определенной информацией, такой как информация о здоровье, образовании или профессии. Наконец, требуется предварительное уведомление и согласие отдельных лиц на передачу или совместное использование их данных (в отличие от GDPR, где подобное согласие не требуется).

Индия свою работу над правовым регулированием оборота «больших данных» начала еще в 2005 году, приняв «Закон о праве на информацию (Right to Information Act)»[9]. Спустя пять лет, в 2010 году, был принят основополагающий «Закон об уникальном идентификационном органе Индии (Unique Identification Authority of India, UIDAI)»[10] — системе идентификации граждан и резидентов Индии, вводящей так называемый AADHAAR — (биометрический аутентификационный номер). В дальнейшем правительством были выпущены «Правила информационных технологий (разумные методы и процедуры безопасности и конфиденциальные личные данные или информация)»

[6] National People's Congress Standing Committee Decision concerning Strengthening Network Information Protection (Mainland China). URL: http://www.law.hku.hk/cprivacy/archives/189 (Дата обращения 18.09.2019).

[7] China's Cybersecurity Law. URL: http://www.npc.gov.cn/npc/xinwen/lfgz/flca/2015-07/06/content_1940614.htm (Дата обращения 05.06.2019). См. также URL: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/ (Дата обращения 21.09.2019).

[8] URL: http://std.sacinfo.org.cn/gnoc/queryInfo?id=5765F72B812F670F1571443FF09C12D2 (Дата обращения 18.09.2019).

[9] Right to Information Act. URL: https://rti.gov.in/rti-act.pdf (Дата обращения 18.09.2019).

[10] The AADHAAR Act. URL: https://uidai.gov.in (Дата обращения 05.06.2019).

(2011)[11], а в 2016 году были приняты: Закон об AADHAAR («The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act», «Aadhaar Act»), «Правила защиты данных» (Aadhaar (Data Security) Regulations, «Aadhaar DS Regulations»), «Правила обмена информацией» (Aadhaar (Sharing of Information) Regulations, «Sharing Regulations»).

В индийском законодательстве биометрическая информация, собранная или созданная в соответствии с Законом об AADHAAR, считается «конфиденциальной личной информацией» (раздел 30). Ее запрещается передавать третьим лицам по любой причине или использовать для каких-либо целей, кроме генерации номеров AADHAAR и аутентификации в соответствии с Законом об AADHAAR (раздел 29). Информация, упомянутая в разделах 28 и 29, может быть раскрыта в случае *вынесения постановления суда*, не уступающего решению окружного судьи; *или в интересах национальной безопасности,* следуя указаниям офицера, не ниже чина Совместного секретаря правительства Индии, специально уполномоченного на это от имени распоряжения центрального правительства. Любое физическое лицо, агентство или организация, которая собирает номер AADHAAR, или любой документ, содержащий номер AADHAAR, должны: (a) собирать, хранить и использовать номер AADHAAR в законных целях; (b) информировать владельца номера AADHAAR о цели, для которой собирается информация, является ли предоставление номера AADHAAR или его подтверждение для этой цели обязательным или добровольным, (с предоставлением обязывающего правового положения, при необходимости, альтернативами представлению номера AADHAAR или документа, содержащего номер AADHAAR, если таковые имеются; (c) получить согласие владельца номера AADHAAR на сбор, хранение и использование его номера AADHAAR для указанных целей. Такое физическое лицо, агентство или организация не должны использовать номер AADHAAR для каких-либо целей, кроме тех, которые указаны держателю номера Aadhaar в момент получения его согласия, и не должны делиться номером AADHAAR с любым лицом без согласия владельца номера AADHAAR (раздел 5 «Sharing Regulation 2016») [7, с. 32-33].

Тем не менее, несмотря на важность и значимость персональной биометрической информации, защита данных AADHAAR оставляет желать лучшего. Известны случаи оформления номеров AADHAAR на другое имя, на несуществующих лиц, даже богов и домашних животных [8].

В Южно-Африканской Республике гарантированное Конституцией право на неприкосновенность частной жизни (секция 14 раздела 2 «Билль о правах», 1996) включает право на «тайну переписки»: защиту от незаконного сбора, хранения, распространения и использования личной информации[12]. Также непосредственное отношение к регулированию оборота персональных данных имеет «Закон о защите персональной информации», принятый в 2013 году[13]. Характерной особенностью законодательства о персональных данных является чрезвычайно расширенная трактовка понятия «персональные данные»: помимо традиционного содержания оно содержит информацию о сексуальных предпочтениях, беременности, психическом здоровье, а также мнения о человеке, принадлежащие другим людям. Виды информации, обычно относимые к Big Data (IP- и MAC-адреса, информация о местоположении, онлайн-идентификаторы), специальным образом не выделяются из персональных данных. Субъект данных имеет право установить, владеет ли ответственная сторона личной информацией данного субъекта данных, и запросить доступ к своей личной информации, запрашивать, при необходимости, исправление, уничтожение или удаление личной информации, на разумных основаниях возражать против обработки своей личной информации. Предусмотрен особый порядок обработки персональных данных для журналистских, литературных или художественных целей.

В законодательстве Республики Казахстан основным законом, регулирующим оборот персональных данных, является Закон РК № 94-V «О персональных данных и их защите» от 21 мая 2013 года (с изменениями и дополнениями по состоянию на 28 декабря 2017 года)[14]. Несмотря на то, что он явно определяет такие важные понятия, как «биометрические данные», «обезличивание данных», «блокирование» и «защита персональных данных», он не содержит юридического определения «больших данных», а также ряда важных для

[11] Ministry of Communications and Information Technology, THE GAZETTE OF INDIA, EXTRAORDINARY, Part II, Section 3, Subsection (i), 11 April 2011.
[12] Constitution of the Republic of South Africa (1996). Section 14. URL: https://www.gov.za/sites/default/files/images/a108-96.pdf (Дата обращения 18.09.2019).
[13] Protection of Personal Information Act (2013). URL: http://www.justice.gov.za/inforeg/docs/InfoRegSA-POPIA-act2013-004.pdf (Дата обращения 18.09.2019).
[14] Закон Республики Казахстан № 94-V «О персональных данных и их защите» от 21 мая 2013 года (с изменениями и дополнениями по состоянию на 28 декабря 2017 года). URL: https://online.zakon.kz/Document/?doc_id=31396226#pos=3;-155 (Дата обращения 05.06.2019).

настоящего времени технологий («блокчейн», «биометрическая аутентификация» и др). Желая исправить сложившуюся ситуацию и придать законодательству актуальное содержание, законодательные органы Казахстана в настоящее время обсуждают проект Закона Республики Казахстан «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам регулирования цифровых технологий» от 11 октября 2018**.

В действующем законе о персональных данных Республики Казахстан права субъекта данных в отношении собственных персональных данных чётко не прописаны по причине отсутствия соответствующей статьи, присутствующей в законодательстве о персональных данных других стран. Субъект или его законный представитель не может отозвать согласие на сбор, обработку персональных данных в случаях, если это противоречит законам Республики Казахстан, либо при наличии неисполненного обязательства. Допускается сбор и обработка персональных данных без согласия субъекта при реализации международных договоров, ратифицированных Республикой Казахстан. Субъект данных не может требовать уничтожения данных о себе.

С другой стороны, в новом законе о регулировании цифровых технологий, идущем на смену действующим в настоящий момент, явно указано, что основная цель работы с большими данными – это получение на их основании ценных аналитических выводов для практического применения. Признается необходимым построение единой справочной системы с обязательным хранением всей исторической информации государственных органов, кроме того, деперсонализация данных для использования в системах и сервисах, не принадлежащих государственным органам.

В Республике Кыргызстан в настоящее время действует закон об информации персонального характера, принятый еще в 2008 году[15], в силу чего в нем отсутствуют определения многих важных понятий, характерных для современного законодательства о персональных данных. Например, не упоминаются «анонимизированные персональные данные», «большие данные» как таковые также не упомянуты; информация, относимая к Big Data, по факту включена в состав персональных данных. Для закона характерно также весьма широкое определение термина «персональные данные» («информация персонального характера»), допускающее вольную интерпретацию.

В Республике Таджикистан до недавнего времени отсутствовал специальный закон о защите персональной информации. Он был принят лишь в 2018 году[16]. Разработчики закона постарались сделать его соответствующим современному уровню законодательства о персональных данных. Упомянуты (даются определения) «биометрические данные», «обезличенные данные», однако «большие данные» как таковые в тексте закона отдельно не упоминаются. Также характерной особенностью закона является то, что для сбора персональной информации ***не требуется*** согласие субъекта данных.

Схожая ситуация сложилась и в Республике Узбекистан, где закон о персональных данных был принят только в этом году и вступил в силу 1 октября 2019 года[17]. Также как и в законе Республике Таджикистан, в законе Узбекистана даются определения понятиям «биометрические данные», «обезличенные данные», но «большие данные» как таковые в тексте закона отдельно не упоминаются. Аналогично, закон не предусматривает обязательного требования согласия субъекта на сбор персональных данных, однако субъект в течение десяти рабочих дней со дня включения его персональных данных в базу персональных данных должен быть уведомлен о его правах, определенных законом, цели сбора данных и третьих лицах, которым передаются его персональные данные, исключительно в письменной форме. Уведомление не производится, если персональные данные собираются из общедоступных источников. Характерной особенностью закона является то, что допускается платный доступ третьих

** Проект Закона Республики Казахстан «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам регулирования цифровых технологий». URL: https://legalacts.egov.kz/npa/view?id=1992299 (Дата обращения 18.09.2019).

[15] Закон Кыргызской Республики «Об информации персонального характера» от 14 апреля 2008 года № 58 (в редакции Закона КР от 20 июля 2017 года № 129). URL: http://cbd.minjust.gov.kg/act/view/ru-ru/202269 (Дата обращения 18.09.2019).

[16] Закон Республики Таджикистан «О защите персональных данных» (принят Постановлением МН МОРТ от 8 июня 2018 года, No1115, одобрен Постановлением ММ МОРТ от 2 августа 2018 года, No561). URL: https://s2.siteapi.org/3d454be12a3d41d/docs/6gj8mt6118g04840owwosc40gwcs8o (Дата обращения 18.09.2019).

[17] Закон Республики Узбекистан «О персональных данных» (Принят Законодательной палатой 16 апреля 2019 года, одобрен Сенатом 21 июня 2019 года). URL: http://lex.uz/docs/4396428 (Дата обращения 18.09.2019).

лиц к базе персональных данных.

И, наконец, Пакистан является обладателем одной из крупнейших в мире баз мультибиометрических данных «National Database and Registration Authority (NADRA)» [9]. Закон о создании национальной базы мультибиометрических данных был принят в 2000 году[18], тогда же началось ее внедрение. К середине 2015 года NADRA насчитывала 121 млн фотографий и 503 млн отпечатков пальцев [10]. По своим функциональным возможностям и назначению NADRA в целом соответствует индийской UIDAI, однако ее возможности несколько шире (например, NADRA может обрабатывать информацию о движущихся объектах в режиме реального времени). Идентификационный номер NADRA необходим при открытии банковских счетов и получении пособий и субсидий. Какие-либо механизмы влияния граждан на оборот личной информации законом не предусмотрены. Несмотря на то, что NADRA призвана решать государственные задачи и повседневного контакта с ней гражданам избежать не удается, это — коммерческая структура, функционирующая на принципах самоокупаемости. Стоимость запроса на идентификацию личности составляет приблизительно 0,35 доллара США.

Завершая обзор существующего законодательства о персональных данных в нашей стране и у ее стратегических партнеров по БРИКС и ШОС, нельзя не затронуть широко обсуждаемый в настоящее время вопрос о том, необходимо ли особое законодательство для регулирования оборота Big Data? Международная правоприменительная практика показывает, что в большинстве стран инициативы в области больших данных рассматриваются в соответствии с действующим законодательством о персональных данных. Однако нельзя не отметить, что в ряде стран сбор персональной информации, по сути, осуществляется принудительно (в первую очередь это относится к персональной биометрической информации). Также существует тенденция коммерциализации банков персональных данных.

Очевидно и то, что «большие данные», как уже упоминалось выше, не вполне укладываются в текущие нормы законодательства о персональных данных. Несмотря на то, что ныне действующая редакция закона о персональных данных определяет персональные данные как любую информацию, «относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)»[19], ни аппаратные серийные номера, ни сетевые либо физические адреса устройств, ни идентификаторы оборудования ни прямо, ни косвенно не привязаны к личности субъекта персональных данных и характеризуют лишь устройство передачи данных в сеть — персональный компьютер либо смартфон. Как результат статистической обработки огромных массивов сугубо технической информации, генерируемой различными вычислительными устройствами либо аппаратурой видеонаблюдения, «большие данные» являются принципиально обезличенными и без привлечения дополнительной информации не могут характеризовать личность субъекта данных даже косвенным образом. Поэтому нельзя исключить того, что в недалеком будущем возникнет необходимость пересмотра сложившейся практики трактовки «больших данных» как «обезличенных персональных данных» и выработки для них специального юридического определения.

Скорость, с которой развиваются существующие технологии и появляются новые, многократно превышает скорость адаптации законодательства к современной технологической реальности. Появление нового закона немыслимо без всесторонней рефлексии над новыми правовыми феноменами, их важности и значимости для общества. Аксиомой должно стать то, что новые концепции и парадигмы, такие как «облачные вычисления» или «большие данные», не должны снижать или подрывать текущие уровни защиты данных как основного права человека и должны отвечать фундаментальным принципам права (законность, справедливость, соразмерность). Права людей на информационное самоопределение, а также прочие их права и законные интересы должны быть краеугольным камнем в современном информационном обществе. Несмотря на то, что законодательство как Российской Федерации, так и стран-партнёров по БРИКС и ШОС стремится учесть появляющиеся новые технологии и определить их правовой статус, отчётливо видна тенденция использования Big Data для новых и неожиданных целей, которые могут противоречить важным принципам, отраженным в GDPR — «принципу ограничения цели» и «принципу минимизации данных».

Наконец, результат статистической обработки больших массивов данных может содержать информацию, с большой долей вероятности релевантно отражающую особенности его личности, но неизвестную

[18] The National Database and Registration Authority Ordinance, 2000. URL: http://nasirlawsite.com/laws/nadra.htm (Дата обращения 18.09.2019).

[19] Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 31.12.2017) "О персональных данных". Статья 3. URL: http://www.consultant.ru/document/cons_doc_LAW_61801/4f41fe599ce341751e4e34dc50a4b676674c1416/ (Дата обращения 22.09.2019).

субъекту данных либо не осознаваемую им в полной мере. В таком случае эта информация *не подпадает под определение «личной тайны»* и, соответственно не может охраняться законодательством (применительно к России эта задача возложена на Статью 23 Конституции РФ). Поэтому существующее определение «личной тайны», возможно, в недалеком будущем будет нуждаться в пересмотре с учётом возможностей «больших данных».

Литература

1. van der Sloot, B.; van Schendel, S. *International and comparative legal study on Big Data.* WRR, The Hague, 2016. ISBN 978-94-90186-29-6.
2. Савельев, А.И. *Проблемы применения законодательства о персональных данных в эпоху «Больших данных» (Big Data)* // Право. Журнал Высшей школы экономики. 2015. №1. С. 43–66.
3. Kostka, G. (2018). *China's Social Credit Systems and Public Opinion: Explaining High Levels of Approval. SSRN Electronic Journal.* DOI:10.2139/ssrn.3215138.
4. Síthigh, D.M, Siems, M. *The Chinese social credit system: A model for other countries?* EUI Working Paper LAW 2019/01. ISSN 1725-6739.
5. Lyo, Y.; Bradley-Schmieg, P. *China Issues New Personal Information Protection Standard.* URL:
6. https://www.insideprivacy.com/international/china/china-issues-new-personal-information-protection-standard/ (Дата обращения 18.09.2019).
7. Zhang, G.; Yin, K. *More updates on the Chinese data protection regime in 2019.* URL: https://iapp.org/news/a/more-positive-progress-on-chinese-data-protection-regime-in-2019/ (Дата обращения 18.09.2019).
8. *Data Protection & Privacy Issues in India. ECONOMIC. LAWS. PRACTICE.* URL: https://elplaw.in/wp-content/uploads/2018/08/Data-Protection-26-Privacy-Issues-in-India.pdf (Дата обращения 18.09.2019).
9. *UIDAI's Aadhaar Has Caused Many Problems. Here Are Some Of Its Biggest Fails.* URL: https://www.huffingtonpost.in/2018/09/25/uidais-aadhaar-has-caused-many-problems-here-are-some-of-its-biggest-fails_a_23530870/ (Дата обращения 18.09.2019).
10. *NADRA.* URL: https://www.nadra.gov.pk/ (Дата обращения 18.09.2019).
11. Рудычева, Н. *Большие данные в госсекторе: опыт Пакистана.* URL: http://www.cnews.ru/articles/bolshie_dannye_v_gossektore_opyt_pakistana (Дата обращения 18.09.2019).