

УДК 001.6

Аюбов А.А.,

студент

2 курс, институт правоохранительной деятельности

Саратовская государственная юридическая академия

Россия, г. Саратов

Лескина Э.И.,

кандидат юридических наук, доцент

доцент кафедры «Информационного права и цифровых технологий»

Саратовская государственная юридическая академия

Россия, г. Саратов

**ПРОБЛЕМЫ ПРИМЕНЕНИЯ ЗАКОНОДАТЕЛЬСТВА О
ПЕРСОНАЛЬНЫХ ДАННЫХ В ЭПОХУ «БОЛЬШИХ ДАННЫХ»
(BIG DATA)**

***Аннотация:** данное исследование посвящено анализу влияния технологий анализа «Больших данных»(Big Data) на законодательство о персональных данных, которое выступает одним из основных гарантов защиты права граждан на неприкосновенность частной жизни в цифровой среде. В исследовании раскрывается понятие «Больших данных» описывается система данной технологии и, ее преимущества, а так же приводятся примеры ее реализации в различных сферах жизни.*

***Ключевые слова:** Интернет, статистические данные, «Большие данные», персональные данные.*

***Annotation:** The study reveals the concept of "Big Data" describes the system of this technology and its advantages, as well as examples of its implementation in various spheres of life.*

***Key words:** internet, statistical data, Big Data, personal data.*

Необходимость цифровизации правовых отношений не вызывает сомнения и диктуется развитием общественных отношений. Этот процесс нельзя остановить, а сдерживать его было бы как минимум нецелесообразно. И одно из главных проявлений эпохи Индустрии 4.0., стремительное развитие Больших данных, вызывает много вопросов в части их правового статуса, возможностей и этических ограничений¹. Современные информационные технологии в значительной степени преобразили наше понимание частной жизни и личного пространства. Те процессы, которые ранее происходили в реальном (физическом) мире, перетекали в онлайн-среду: приобретение разных товаров и услуг, общение с лучшими друзьями и знакомыми, взаимодействие с работодателем, государственными органами и т.д. Как следствие, объемы и широта личной информации, которые лицо раскрывает о себе и выкладывает во всемирную сеть Интернет и, соответственно, объемы личных данных граждан, подвергаемых сбору и систематизации различными органами и организациями, возросли до беспрецедентных размеров.² Этому способствовало несколько факторов:

- 1) Проникновение Интернета в повседневную жизнь людей;
- 2) Развитие и совершенствование электронной коммерции;
- 3) появление социальных сетей;

¹ Лескина Э.И. Применение блокчейн-технологий в сфере труда // Юрист. 2018. № 11. С. 25-30

² Майер-Шенбергер В., Кукьер К. Большие данные. Революция, которая изменит то, как мы живем, работаем и мыслим. М. 2014. С. 17.

4) Распространение смартфонов и других гаджетов, которые позволяют быть круглосуточно в сети, а так же мгновенно обмениваться информацией и сообщениями.³

Как следствие, ключевые процессы жизнедеятельности человека перетекли в Интернет и любое действие индивида оставляет цифровой след, что в совокупности повлекло появление огромных размеров массива цифровой информации. Статистика объема данных, создаваемых на протяжении последних лет, поражает воображение. В 2013 г. количество хранящейся в мире информации составило 1,2 зеттабайта (около 1,2 млн. петабайт или 1,2 трлн. гигабайт), из которых на нецифровую информацию приходится менее 2%. По прогнозам компании IDC, специализирующейся на аналитике в сфере информационных технологий, общее количество информации будет удваиваться каждые 2 года и составит к 2020 г. порядка 40 зеттабайт. Взаимодействие различного рода устройств между собой посредством сети Интернет, предполагающее их цифровую идентификацию, привязанную к базам данных, лежит в основе концепции «Интернета вещей» (Internet of Things) который рассматривается в качестве следующего этапа эволюции развития сети Интернет, где машины будут являться не только производителями информации, но и ее потребителями.

Термин «Большие данные» (Big Data) не имеет общепринятого определения даже в индустрии информационных технологий. Наиболее распространенным является раскрытие феномена «Больших данных» через указание проблем, с которыми приходится сталкиваться на современном этапе развития технологий при обработке информации. Исходя из этого «Большие данные» определяются посредством указания следующих основных характеристик: 1) большого объема (Volume), 2) разнообразия данных (Variety)

³ Gantz J. and Reinsel D. The Digital Universe in 2020: Big Data, Bigger Digital Shadows, and Biggest Growth in the Far East. December 2012. URL: <http://www.emc.com/collateral/analyst-reports/idc-the-digitaluniverse-in-2020.pdf> (дата доступа: 15.09.2014)

и 3) высокой скорости их изменения (Velocity). Данный подход получил название «трех «V»

«Большие данные» можно определить как совокупность инструментов и методов обработки, структурированных и неструктурированных данных огромных объёмов из различных источников, подверженных постоянным обновлениям, в целях повышения качества принятия управленческих решений, создания новых продуктов и повышения конкурентоспособности.⁴

Технологии Big Data носят универсальный характер и могут быть использованы в самых различных сферах деятельности. Применительно к коммерческим их видам основной интерес технологии “Больших данных” будут представлять для организаций, где уже накоплены большие массивы данных по клиентам и операционной деятельности.⁵

Технологии «Больших данных» могут применяться и в инновационных подходах к профилактике правонарушений. В частности, широкую известность получила система Blue CRUSH (от англ.: Crime Reduction Utilizing Statistical History — «Снижение преступности на основе статистических данных»), разработанная компанией IBM, которая поставляет полицейским подготовленные на основе имеющейся статистики совершения преступлений сведения о зонах потенциальной угрозы совершения преступления с указанием места (в пределах нескольких кварталов)⁶ и времени (в пределах нескольких часов конкретного дня недели). Подобного рода профилактическое

⁴ Считается, что термин «Интернет вещей» был первоначально использован еще в 1999 г. Кевином Эштоном (Kevin Ashton), ученым MIT, который стоял у истоков технологии RFID. Он отмечал, что на первых порах развития сети Интернет, составляющая его информация была создана людьми. На следующих этапах развития сети большая часть информации, наполняющей ее, будет создана устройствами, что позволит оперативно решать вопросы, связанные с их обслуживанием, обладая информацией о том, когда вышло из строя, требует замены или усовершенствования. В конечном итоге он приходит к выводу, что Интернет вещей может изменить мир в той же степени, как это сделал в свое время сам Интернет. Ashton K. That ‘Internet of Things’ Thing // RFID Journal. July 22, 2009.

⁵ Как отмечается, «Данные — это новая «нефть»: они представляют собой ценность, однако в необработанном состоянии они не могут быть использованы». Arthur C. Tech giants may be huge, but nothing matches big data // The Guardian, August 23, 2013. URL: <http://www.theguardian.com/technology/2013/aug/23/tech-giants-data>(дата обращения: 15.09.2014)

⁶ <http://www.ibm.com/smarterplanet/us/en/leadership/memphispd/>(Дата обращения: 14.02.2015).

прогнозирование привело к снижению уровня преступности в г. Мемфисе на 33%, из которых 15% приходится на тяжкие преступления.⁷ Технические решения, имеющие в своей основе аналитику «Больших данных», используются в ряде иных городов США (Нью-Йорк, Сиэтл, Лос-Анджелес и др.) и масштаб их использования возрастает с каждым годом⁸

Огромные материалы употребляются в свойстве одного из ключевых составляющих программ многочисленной слежки за гражданами, исполняемыми Агентством государственной безопасности США (АНБ) и как граждан США, так и иностранных лиц. По достоверным сведениям газеты «Гардиан» от 2013 года, каждодневно налаженности созыва информации АНБ занимали и вписывали вокруг 1,7 млрд. телефонных звонков и электронных извещений и вокруг 5 млрд. записей о месторасположенье и передвижениях собственников мобильных по всему миру. При этом основным источником данных являлись американские компании **Microsoft, Google, Yahoo, Facebook, America Online и Apple**, предоставлявших АНБ прямой доступ к своим серверам.⁹

Как видно из вышеуказанных примеров, технологии «Больших данных» сулят государству и отдельно взятым компаниям большие выгоды, от которых могут выиграть и обычные граждане. Можно с уверенностью сказать, что компьютерные технологии сплошной плюс, особенно в наше время-время всеобщей компьютеризации. Все данные отдельно взятой личности хранятся в сети Интернет в так называемых облачных хранилищах. Однако при этом степень вмешательства в частную жизнь отдельно взятого гражданина может быть высокой, причем, чем больше персональных данных о лице агрегирует и подвергается обработке, тем выше степень возможного влияния на жизнь такого

⁷ Thompson T. Crime Software May Help Police Predict Violent Offences // The Guardian, July 25, 2010. URL: <http://www.theguardian.com/uk/2010/jul/25/police-software-crime-prediction> (Дата обращения: 14.02.2015).

⁸ Joh E. Policing by Numbers: Big Data and the Fourth Amendment // Washington Law Review No. 89:35. 2014. P. 35-68.

⁹ Gellman B., Poitras L. U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program // The Washington Post. June 7, 2013 URL: <http://goo.gl/KoTn4z> (Дата обращения: 14.02.2015).

лица результатов автоматизированной обработки и, соответственно, величина риска, связанная с нарушением его прав.

Специальные положения, посвященные проблематике автоматизированной обработки персональных данных, сначала появились в Европе и впоследствии распространились по всему миру. По состоянию на начало 2012 г. законы о персональных данных были приняты в 89 странах мира.¹⁰ В России существует Федеральный закон РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных» — федеральный закон, регулирующий деятельность по обработке персональных данных. Так как в соответствии с законом, в России существенно возрастают требования ко всем частным и государственным компаниям и организациям, а также физическим лицам, которые хранят, собирают, передают или обрабатывают персональные данные (в том числе фамилию, имя, отчество).¹¹ Такие компании, организации и физические лица относятся к операторам персональных данных. Согласно закону, а также ряду подзаконных актов и руководящих документов регулирующих органов (ФСТЭК России, ФСБ России, Роско надзор), операторы ПД обязаны выполнять ряд требований по защите персональных данных физических лиц (своих сотрудников, клиентов, посетителей и т. д.) обрабатываемых в информационных системах Компании, и предпринять ряд действий:

1. направить уведомление об обработке персональных данных в уполномоченный орган (Закон № 152-ФЗ. Ст. 22 п. 3)
2. получать письменное согласие субъекта персональных данных на обработку своих персональных данных

¹⁰ ФЗ от 19.12.2005 г. N 160-ФЗ “О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных”. Процесс ратификации был завершен 15 мая 2013 г. Конвенция вступила в силу в отношении России с 1 сентября 2013 г.

¹¹ 4 Greenleaf G. Global Data Privacy Laws: 89 Countries, and Accelerating // Privacy Laws & Business International Report, N 115, February 2012; Queen Mary School of Law Legal Studies Research Paper No. 98/2012. URL: <http://ssrn.com/abstract=2000034> (дата обращения: 14.02.2015)

(Закон № 152-ФЗ ст. 9 п. 4);

3. уведомлять субъекта персональных данных о прекращении обработки и об уничтожении персональных данных (Закон № 152-ФЗ ст. 21 п. 4).

Уведомление об обработке персональных данных не требуется, если оператор персональных данных и субъект персональных данных находятся в трудовых отношениях или иных договорных отношениях (Закон № 152-ФЗ ст. 22 п. 2).

Идеальная модель регулирования в сфере законодательства о персональных данных подразумевает, что субъект персональных данных имеет возможность самостоятельно принимать решения, касающиеся его информационной сферы, посредством согласия на обработку его персональных данных в отдельных случаях, взвешивая соответствующие риски и выгоды.¹² В связи с этим согласие субъекта персональных данных является главным легитимирующим основанием их обработки этих данных. Без согласия субъекта нельзя производить никаких операций с его персональными данными. Для того чтобы согласие субъекта персональных данных могло называться информированным, конкретным и сознательным, необходимо, чтобы ему была предоставлена детальная информация о том, как будут использоваться его персональные данные: цели использования, состав обрабатываемых персональных данных и способы их обработки (ч.4 ст. 9, ч. 7 ст. 14 ФЗ «О персональных данных»). В эпоху «Больших данных» концепция информированного согласия на обработку персональных данных в значительной степени утрачивает свою эффективность в силу ряда причин:

¹² Article 29 Data Protection Working Party, Opinion 15/2011 on the Definition of Consent, WP 187, July13, 2011, URL: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf (Дата обращения: 14.02.2015); Vygrave L. Op.cit. P. 158; Бачило И.Л., Сергиенко Л.А., Кристальный Б.В., Арешев А.Г. Указ. соч. С. 24.

а) невозможности предоставить исчерпывающий объем информации о возможных способах и целях обработки персональных данных;

б) невозможности субъекта персональных данных адекватно воспринять такую информацию;

в) невозможности индивидуального взаимодействия с огромным множеством организаций, осуществляющих сбор и обработку персональных данных в современном обществе.¹³

Следует также отметить и показать важную вертикаль в использовании и сборе персональных данных субъекта: информированное согласие предполагает необходимость принятия субъектом персональных данных ряда дискретных решений на ранних стадиях их обработки (как правило, стадии сбора персональных данных), однако в силу особенностей применения технологий «Больших данных» последствия таких решений невозможно предугадать на данном этапе. В итоге информированное согласие является в современных условиях не более чем фикцией и не может исполнять роль главного легитимирующего основания для обработки персональных данных.

Большие данные представляют собой имущественный комплекс, включающий совокупность объектов с различной правовой природой, которые имеют общее целевое назначение. Единство цели консолидирует эту совокупность в единый самостоятельный объект гражданского права, обладающий признаками оборотоспособности и предполагающий специфические способы защиты прав его правообладателя.

Доминантой больших данных как разновидности имущественных комплексов является:

¹³ Article 29 Data Protection Working Party, Opinion 15/2011 on the Definition of Consent, WP 187, July 13, 2011, URL: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf (Дата обращения: 14.02.2015); Vygrave L. Op.cit. P. 158; Бачило И.Л., Сергиенко Л.А., Кристальный Б.В., Арешев А.Г. Указ. соч. С. 24.

1) информация, которая состоит из «сырых данных» (необработанных данных) и результатов обработки «сырых данных» (которые могут быть, в том числе и в овеществленной форме);

2) имущественные права (например, исключительные права на результаты интеллектуальной деятельности программы для электронных вычислительных машин (программы для ЭВМ), базы данных).

Особенность такого имущественного комплекса состоит в том, что ценность и полезность элементов такого комплекса (значение для конкретных лиц и обществ в целом) могут представлять интерес как сами по себе, так и в своей совокупности.

Итак, в настоящей статье было показано такое образное конфликтное состояние технологий Больших данных с законодательством о персональных данных на примере трех положений последнего: принципа минимизации данных и ограничения обработки заранее определенной целью; концепции информированного согласия как ключевого основания обработки, а также возможности обезличивания персональных данных с целью исключения полученных данных из-под действия законодательства о персональных данных. Однако было бы наивным полагать, что этим проблемы исчерпываются. На самом деле технологии «Больших данных» выдают очевидный факт: законодательство о персональных данных в том виде, в каком оно было сформулировано еще в Конвенции 1981 г.,¹⁴ становится все менее и менее адекватным современным технологическим реалиям и нуждается в существенной переработке. Как и любое законодательство, отдельно взятого государства наше имеет свои недостатки. Косметическое или точечное

¹⁴ Statement on Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU. Article 29 Data Protection Working Party, WP221. September 16, 2014. URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp221_en.pdf (датаобращения: 14.02.2015).

изменение существующего регулирования в сфере защиты персональных данных не способно сделать его эффективным, а способно лишь увеличить степень его отрыва от реальности. Переосмыслению должны подвергнуться такие базовые категории, как понятие персональных данных и понятие оператора персональных данных. В условиях, когда общий сбор сведений о пользователях носит массовый характер, даже самый безобидный фрагмент такой информации (сведения о посещении сайта или совершении покупки) будучи соединенным с другой подобной информацией, способен дать гораздо больше сведений о лице, чем совокупность его анкетных данных. Достойны ли такие единицы информации особого регулирования путем придания им статуса персональных данных? Либо же имеет смысл выделить их в особую категорию с отдельным регулированием? Влияет ли анонимность или использование псевдонима на возможность квалификации соответствующей информации как персональных данных? Эти вопросы требуют разрешения. Указанные вопросы нельзя решить, не ответив первоначально на главный вопрос: являются ли персональные данные товаром или они являются неотчуждаемым неимущественным благом? В пользу каждой трактовки можно привести множество аргументов. Но в моем предположении решение этих проблем виднеется в совершенствовании законодательства и в улучшении сбора и обработки персональных данных. Однако одним из наиболее значимых является то, что большая часть успешных бизнес-моделей в сети Интернет основана на использовании персональных данных в качестве «валюты», которой пользователь расплачивается за возможность использования соответствующего сервиса. Именно данные пользователей являются одним источником многомиллиардных доходов социальных сетей, поисковых сервисов и иных IT-компаний. Однако этот факт игнорируется большинством пользователей, как, впрочем, и российским законодательством, не признающим предоставление персональных данных на обработку в качестве встречного

предоставления для целей квалификации договора в качестве возмездного (ст. 424 ГК РФ). Так или иначе, от ответа на данный вопрос будет во многом зависеть решение и всех остальных, ранее обозначенных проблем.

Однако, несмотря на обозначенные проблемы, цифровая экономика это новый уклад жизни, это новая основа для государственного управления, экономики, социальной сферы, всего общества. Это вопрос национальной безопасности России, конкуренции отечественных компаний¹⁵. Это правильное понимание цифровой экономики и неотъемлемой при этом цифровизации как неизбежного процесса, который пройдут все страны. И положение каждой страны будет определяться тем, насколько оперативно она будет реагировать на новые тренды.

Список литературных и нормативных источников:

1. Article 29 Data Protection Working Party, Opinion 15/2011 on the Definition of Consent, WP 187, July 13, 2011, URL: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf.
2. Arthur C. Tech giants may be huge, but nothing matches big data // The Guardian, August 23, 2013. URL: <http://www.theguardian.com/technology/2013/aug/23/tech-giants-data> (дата обращения: 15.09.2014)
3. Ashton K. That 'Internet of Things' Thing // RFID Journal. July 22, 2009.
4. Gantz J. and Reinsel D. The Digital Universe in 2020: Big Data, Bigger Digital Shadows, and Biggest Growth in the Far East. December 2012. URL: <http://www.emc.com/collateral/analyst-reports/idc-the-digitaluniverse-in-2020.pdf> (дата доступа: 15.09.2014).

¹⁵ Лескина Э.И. Влияние развития нейронных сетей на трудовые отношения // Российская юстиция, 2020, № 8, С. 9-12.

5. Gellman B., Poitras L. U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program // The Washington Post. June 7, 2013 URL: <http://goo.gl/КоТn4z> (Дата обращения: 14.02.2015).
6. Greenleaf G. Global Data Privacy Laws: 89 Countries, and Accelerating // Privacy Laws & Business International Report, N 115, February 2012; Queen Mary School of Law Legal Studies Research Paper No. 98/2012. URL: <http://ssrn.com/abstract=2000034>.
7. Joh E. Policing by Numbers: Big Data and the Fourth Amendment // Washington Law Review No. 89:35. 2014. P. 35-68.
8. Thompson T. Crime Software May Help Police Predict Violent Offences // The Guardian, July 25, 2010. URL: <http://www.theguardian.com/uk/2010/jul/25/police-software-crime-prediction>.
9. Лескина Э.И. Влияние развития нейронных сетей на трудовые отношения // Российская юстиция, 2020, № 8, С. 9-12.
10. Лескина Э.И. Применение блокчейн-технологий в сфере труда // Юрист. 2018. № 11. С. 25-30.
11. Майер-Шенбергер В., Кукьер К. Большие данные. Революция, которая изменит то, как мы живем, работаем и мыслим. М. 2014. С. 17.
12. ФЗ от 19.12.2005 г. N 160-ФЗ “О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных”. Процесс ратификации был завершен 15 мая 2013 г. Конвенция вступила в силу в отношении России с 1 сентября 2013 г.