УДК 349 DOI: 10.31249/iajpravo/2024.04.12

ИВАНОВА А.П.[1] **БОЛЬШИЕ ДАННЫЕ И ПРАВО НА НЕПРИКОСНОВЕННОСТЬ ЧАСТНОЙ ЖИЗНИ**

Аннотация: Начало эпохи больших данных безусловно ознаменовало собой рост возможностей человека в части экономического роста, научно-технического прогресса и даже рядовых, рутинных задач. В то же время, развитие больших данных существенным образом повлияло на конституционное право каждого человека на неприкосновенность частной жизни. В статье рассматриваются различные аспекты такого влияния, а также анализируются недостатки современных законов о защите персональных данных, из-за которых они теряют свою эффективность в эпоху больших данных.

Ключевые слова: защита персональных данных, большие данные, Интернет вещей, искусственный интеллект, цифровизация, информационные технологии.

IVANOVA A.P. Big data and the right to privacy

Abstract: The beginning of the era of big data certainly marked the growth of human capabilities: in terms of economic growth, scientific and technological progress, and even ordinary, routine tasks. At the same time, the development of big data has significantly affected everyone's constitutional right to privacy. The article examines various aspects of such influence, as well as analyzes the shortcomings of modern personal data protection laws, due to which they lose their effectiveness in the era of big data.

[1] *Иванова Ангелина Петровна*, младший научный сотрудник отдела правоведения ИНИОН РАН.

Keywords: personal data protection, big data, Internet of things, artificial intelligence, digitalization, information technology.

Для цитирования: Иванова А.П. Большие данные и право на неприкосновенность частной жизни. (Обзорная статья) // Социальные и гуманитарные науки. Отечественная и зарубежная литература: ИАЖ. Сер. Государство и право. – 2024. – № 4. – С. 149–163. – DOI: 10.31249/iajpravo/2024.04.12

Введение

Каждый раз, когда пользователи выходят в Интернет, используют приложение на своем телефоне, покупают что-то онлайн, они часто не задумываются, что веб-сайты и программные продукты собирают информацию о них, и, более того, не имеют понятия о том, что происходит с этими данными впоследствии.

На самом деле, подобные «цифровые следы» сохраняются, анализируются, передаются и продаются, т.е. компании распоряжаются ими по своему усмотрению. Использование этих данных может быть весьма неожиданным, иметь нежелательные для субъекта последствия, в том числе нести за собой моральный и материальный вред. Например, пользовательское поведение в контексте просмотра веб-страниц может быть использовано для таргетинга рекламы, чтобы идентифицировать конкретного потребителя в качестве офисного работника, должника или человека, нуждающегося в медицинской помощи[1].

Одно исследование показало, что данные о местоположении отслеживаются почти всеми приложениями на современных смартфонах «с поразительной детализацией, с точностью до нескольких метров» и, более того, «в некоторых случаях обновляются более 14 000 раз в день»[2]. Такие сведения представляют огромную ценность для тех, кто ее получает. За последние десятки лет информация приобрела особое значение – стала главным фактором производства и получила статус «новой нефти»[3].

[1] Houser K.A., Bagby J.W. Next-generation data governance // Duke law & technology law review. – 2024. – Vol. 21, N 1. – P. 62.

[2] Ibid. – P. 62.

[3] Stach C. Data is the new oil–sort of: a view on why this comparison is misleading and its implications for modern data administration // Future Internet. – 2023. – Vol. 14, N 2. – P. 1.

Монетизация данных представляет собой большой бизнес. По состоянию на 2024 г., размер рынка данных составил 4,87 млрд долларов США, к 2029 г. прогнозируется его рост до 14,99 млрд долларов США[1]. Появление феномена больших данных в совокупности с их аналитикой на основе искусственного интеллекта лишь увеличило объем сбора и использования информации, а значит, стало одним из основных факторов развития рынка данных.

Влияние больших данных на права человека

Большие данные не имеют единого устоявшегося определения. В российской научной среде большие данные часто определяются как «технологии и архитектуры нового поколения для экономичного извлечения ценности из разноформатных данных большого объема путем их быстрого захвата, обработки и анализа»[2].

Стратегия развития информационного общества в Российской Федерации на 2017–2030 гг., утвержденная Указом Президента РФ от 9 мая 2017 г. № 203, в подп. «к» п. 4 дает определение «обработки больших объемов данных» как «совокупности подходов, инструментов и методов автоматической обработки структурированной и неструктурированной информации, поступающей из большого количества различных, в том числе разрозненных или слабосвязанных, источников информации, в объемах, которые невозможно обработать вручную за разумное время». Как справедливо отмечает доцент кафедры информационного права Уральского государственного юридического университета А.Н. Гулемин, попытки дать легальное определение напрямую понятию «боль-

[1] Анализ размера и доли рынка монетизации данных – тенденции роста и прогнозы (2024–2029 гг.) // Mordor Intelligence. – URL: https://www.mordorintelligence.com/ru/industry-reports/data-monetization-market (дата обращения: 12.07.2024).

[2] Найдич А. Большие данные: насколько они большие? [Электронный ресурс] // Компьютер Пресс. – 2012. – URL: http://compress.ru/article.aspx?id=23469 (дата обращения: 12.07.2024); Садовникова Н.П., Щербаков М.В. Технологии анализа данных: учеб. пособие. – 2021. – С. 7.; Садовникова Н.П., Парыгин Д.С., Щербаков М.В. Системы поддержки принятия решений: учеб. пособие. – 2021. – С. 54.

шие данные» на национальном уровне до сих пор не увенчались успехом[1].

В мировой практике чаще всего данное явление характеризуют через три его ключевых признака: объем, скорость и разнообразие. Иногда к этим характеристикам добавляются также изменчивость и значение данных[2].

Технологии больших данных фактически превратили современный мир в мир повсеместного сбора и анализа информации. При этом информация может использоваться не только для анализа образа жизни, мировоззрения и предпочтений отдельной личности, но и для исследования основных тенденций в поведении различных социальных групп, а также общества в целом. Указанные изменения неизбежно трансформируют большинство сфер общественной жизни.

Так, профессор школы права Квинслендского технологического университета Австралии М. Бёрдон высказывает мнение о том, что в эпоху развития больших данных изменяется сама концепция политической власти. Автор обращается к произведению французского философа Ж. Делёза «Посткриптум к обществам контроля», в котором описывается общество контроля – особый режим власти, постепенно вытесняющий дисциплинарные общества. Ж. Делёз утверждает, что общество контроля представляет собой фундаментальный отход от дисциплинарных обществ, которые стремятся загнать индивидов в определенные рамки[3].

Политическая власть в подобном типе социума связана с невидимым мониторингом и выявлением паттернов с целью прогнозирования поведения индивидов и оказания на него воздействия. М. Бёрдон подчеркивает, что в условиях общества контроля люди в определенной степени лишаются свободы мысли и свободы соб-

[1] Гулемин А.Н. Пределы обработки больших объемов данных для целей получения информации о человеке: правовой аспект // Электронное приложение к Российскому юридическому журналу. – 2022. – № 6. – С. 53.

[2] Садовкин А.А. Сложности перехода российской экономики к новому технологическому укладу // Международный журнал гуманитарных и естественных наук. – 2024. – Т. 2/3 (89). – С. 241.

[3] Цит. по: Burdon M. Digital data collection and information privacy law. – 2020. – P. 293–294.

ственных действий, поскольку их поведение становится предсказуемым и даже предопределенным[1].

Появление и развитие больших данных фактически стало технологической основой для реализации указанной формы контроля. В современном мире отдельные участники рынка имеют возможности не только прогнозировать поведение индивидов, социальных групп и популяций, но и оказывать воздействие на такое поведение (ставить цели и определять результаты своего развития таким образом, чтобы они лучше соответствовали прогнозируемому будущему).

Всё это влечет серьезные последствия для прав и свобод человека, и в первую очередь, для права на защиту неприкосновенности частной жизни.

Большие данные – новый вызов для законодательства о защите персональных данных

Ещё до появления Интернета сбор данных был неотъемлемой частью бизнес-процессов, поскольку анализ и прогнозирование потребностей и пожеланий покупателей и клиентов – основа любой предпринимательской деятельности. Именно обработка персональной информации (например, отслеживание истории покупок или запросов пользователя в сети Интернет) позволяет наилучшим образом достигать этой цели. Сбор данных имеет решающее значение для маркетинга и разработки продуктов, систем здравоохранения, алгоритмического прогнозирования потребностей потребителей и многих других аспектов повседневной жизни. С развитием Интернета и новых технологий потребители теперь ежедневно пользуются веб-сайтами, приложениями и умными устройствами, которые сохраняют личную информацию.

Повсеместный сбор и анализ больших данных, активно растущий в настоящее время, в корне бросает вызов традиционным мерам защиты конфиденциальности информации. Юридически неясно, будут ли такие данные классифицироваться как типы информации, находящиеся в сфере регулирования закона о персо-

[1] Цит. по: Burdon M. Digital data collection and information privacy law. – 2020. – P. 293.

нальных данных. Большие данные, которые могут быть собраны из многих источников, теперь используются для прогнозирования поведенческих моделей потребителей. Это устраняет необходимость собирать непосредственно персональные сведения.

В контексте больших данных член консультативного совета Лаборатории цифровой демократии Школы права Уильяма и Мэри К.А. Хаузер, профессор Пенсильванского государственного университета Дж.У. Бэгби выделяют несколько типов данных, которые представляют различный риск для неприкосновенности частной жизни.

Первичные («сырые») данные собираются регулярно и включают в себя наблюдения о людях, животных, предметах или условиях (например, о местоположении, скорости, температуре). Сами по себе первичные данные немного могут сказать о субъекте, которому они принадлежат, ввиду чего не представляют особых рисков для неприкосновенности частной жизни.

Производные данные – это «информация, которая может быть получена из множества точек данных об отдельном человеке или из связей отдельного человека с определенными группами»[1]. В эпоху больших данных главный акцент делается на повторном использовании данных, имеющих немалую ценность в современном мире[2]. Поскольку субъекты персональных данных не знают о таком анализе и повторном использовании их личной информации, они не имеют понятия о том, что представляют собой новые производные данные, как они используются и связаны с другими сведениями. В то же время полученная информация может использоваться как для прогнозирования поведения пользователя, например, какой фильм следует порекомендовать Netflix, так и, что более важно, для вычисления вероятности совершения определенным лицом преступления[3]. Хотя эти данные собираются и анализируются частным сектором, «информационные брокеры» потенциально могут предоставлять их и государственным органам.

[1] Houser K.A., Bagby J.W. Op. cit. – P. 65.

[2] Савельев А.И. Проблемы применения законодательства о персональных данных в эпоху «Больших данных» (Big Data) // Право. Журнал Высшей школы экономики. – 2015. – № 1. – С. 54.

[3] Houser K.A., Bagby J.W. Op. cit. – P. 65.

Профессор Университета Британской Колумбии В. Вонг, аспирант Центра криминологии и социально-правовых исследований Университета Торонто Дж. Дункан, профессор Калифорнийского университета в Сан-Диего Д.А. Лейк также отмечают, что в отличие от методов этичного потребления в сфере охраны окружающей среды, где проблема заключается в установлении цепочки поставок от леса или фермы до потребителя, информация может быть выпущена в свободный оборот без ограничения по конечным пользователям. Эти данные могут служить относительно «безобидным» целям, таким как маркетинг, или более серьезным, таким как государственный надзор. В любом случае, трудно определить, как используются данные после их получения[1].

В эпоху больших данных организации заинтересованы в том, чтобы собирать как можно больше данных в пределах своих возможностей для их хранения и последующего использования, характер которого предугадать невозможно[2]. Указанные свойства технологий обработки больших объемов информации привели, как минимум, к двум последствиям для неприкосновенности частной жизни.

Последствие 1 – неэффективность концепции информированного согласия в эпоху больших данных. Большинство законодательных актов в области защиты персональных данных (Общий Регламент о защите персональных данных, Закон Калифорнии о защите персональных данных потребителей, Федеральный закон «О персональных данных» от 27.07.2006 г. № 152-ФЗ) основаны на модели информированного согласия или, другими словами, индивидуального контроля. У физических лиц есть нерушимое право определять, какие персональные данные о них собираются, для каких целей и каким образом они впоследствии используются, кто может получить доступ к персональной информации, собранной организациями. Указанному праву корреспондирует соответствующая обязанность операторов данных: физическое лицо должно быть уведомлено о целях сбора и способно дать сознательное со-

[1] Wong W.H., Duncan J., Lake D.A. Why data about people are so hard to govern // Regulation & Governance. – 2024. – Online Version of Record before inclusion in an issue. – P. 2.

[2] Савельев А.И. Указ. соч. – С. 50.

гласие на последующую ее обработку. Личная информация, как правило, может быть использована только для определенной цели, о которой субъект этой информации должен быть надлежащим образом проинформирован. Кроме того, персональные данные после их сбора должны храниться в безопасности[1].

Однако, как поясняется в докладе Всемирного экономического форума, опубликованном в июле 2020 г., озаглавленном «Изменение концепции конфиденциальности данных», «согласие субъектов персональной информации стало иллюзорным и, в силу его нынешней структуры и применения, не всегда работает ожидаемым, а иногда даже логичным образом»[2]. Хотя оператор персональных данных может указать, какая информация собирается, и физическое лицо дает согласие на ее использование, сомнительно, что субъект данных действительно понимает, на что он соглашается[3].

Модель защиты данных, основанная на информированном согласии, по мнению К.А. Хаузер, Дж.У. Бэгби, неэффективна по ряду причин.

Во-первых, согласие, в большинстве случае, предполагает простое проставление галочки рядом с надписью «я даю согласие на обработку персональных данных» для осуществления определенных действий (переход на сайт, создание онлайн-заказа), на которую большинство пользователей просто не обращает внимания. В то же время, на субъекта данных возлагается ответственность за определение того, какие данные будут собираться, как они будут обрабатываться и кому будут передаваться.

Во-вторых, неструктурированная информация с датчиков, собираемая из множества источников, фактически устраняет необходимость собирать персональные данные. Современное законодательство, похоже, не принимает во внимание возросшие возможности обработки информации, ввиду чего отдельные лица могут быть легко идентифицированы по наборам больших данных, что создает огромный пробел в регулировании.

[1] Burdon M. Op. cit. – P. 2.

[2] Redesigning data privacy: reimagining notice & consent for human technology interaction // World Economic Forum. White paper. – 2020. – P. 4.

[3] Houser K.A., Bagby J.W. Op. cit. – P. 83.

В-третьих, проблема заключается не только в объеме политики конфиденциальности и ее понятности, но и в огромном количестве политик конфиденциальности, с которыми сталкиваются пользователи, и их условиях «take it or leave it», т.е. услуги не предоставляются без соответствующего согласия на обработку персональных данных[1].

Наконец, повсеместный и непрерывный сбор информации в современном мире подрывает способность физических лиц осознанно соглашаться на процесс сбора личной информации и контролировать его самостоятельно. Так, например, получение данных с устройств «умного» дома является циклическим и непрерывным процессом, что ставит под сомнение возможности предоставления конкретного и информированного согласия на их обработку[2].

Последствие 2 – несостоятельность категории «обезличенной информации» в связи с развитием технологий больших данных. Как отмечает А.И. Савельев, при анализе больших данных совокупность важнее отдельных частей, а при перекомпоновке совокупностей нескольких наборов данных получается еще более удачная совокупность[3]. Учитывая множество источников, из которых поступает информация, и невероятную ценность объединения разнородных данных для создания профиля потенциального потребителя, факт существования больших данных и легкость их получения существенно облегчает повторную идентификацию, т.е. деанонимизацию. Поскольку «связанные» данные неизвестны субъекту данных и не существует законодательного требования, позволяющего субъекту данных требовать «разъединения» данных, контроль за использованием подобных цифровых профилей практически отсутствует. Технические и юридические стандарты позволяют операторам манипулировать данными, обмениваться ими и извлекать выгоду из данных, которые создают пользователи.

Более того, с распространением Интернета вещей (Internet of Things) и Интернета поведения (Internet of Behavior) взаимосвязи будут только усиливаться. Так, подчеркивают К.А. Хаузер, Дж.У. Бэгби, смарт-часы или фитнес-браслет в связке со смартфо-

[1] Houser K.A., Bagby J.W. Op. cit. – P. 84.

[2] Burdon M. Op. cit. – P. 291.

[3] Савельев А.И. Указ. соч. – С. 54.

ном могут предоставить очень подробную информацию о жизни, здоровье, передвижениях, интересах, привычках и связях человека[1].

Когда организация создает и хранит большой массив информации на основе собранных данных, а также компановки их общедоступными сведениями или информацией, поступившей от других операторов, указанный массив данных может представлять собой даже более конфиденциальные сведения, чем те, которые запрашиваются организацией напрямую. С помощью традиционных методов анализа данных уже были собраны информационные базы, которые позволили выявлять важные характеристики с достаточно высокой точностью. Например, американская компания Target Corporation, управляющая сетью магазинов розничной торговли, смогла предсказать беременность женщины, основываясь только на покупательских привычках, без непосредственного сбора данных о ее беременности[2].

Некоторые авторы занимают более радикальную позицию: они считают, что концепция «обезличенных» данных, особенно в эпоху больших данных, в значительной степени является своего рода иллюзией, юридической фикцией. Многие категории, называемые судами и политиками «анонимными» данными, легко идентифицируются сами по себе или в сочетании с общедоступными наборами данных[3]. Более того, обезличивание некоторых данных представляется невозможным, что делает заявление об их анонимизации ложными и вводящими в заблуждение. Одним из таких примеров является политика конфиденциальности сервиса по генетическому тестированию 23andMe. Биотехнологическая компания, которая делится данными с «партнерами по исследованиям», утверждает, что генетические данные будут «деидентифицированы» (лишены соответствующих идентификаторов) и «агрегированы» (объединены в набор данных с тысячами данных других людей) перед анализом партнерами[4]. Вместе с тем, идея о

[1] Houser K.A., Bagby J.W. Op. cit. – P. 66.

[2] Ibid. – P. 109.

[3] Stoffel E.C. The myth of anonymity: de-identified data as legal fiction // New Mexico Law Review. – 2024. – Vol. 54, N 1. – P. 133.

[4] Stoffel E.C. The myth of anonymity: de-identified data as legal fiction // New Mexico Law Review. – 2024. – Vol. 54, N 1. – P. 132.

том, что генетические данные, достаточные для того, чтобы сопоставить человека с преступлением, могут быть разумно отделены от его личности, лишена логики[1].

Интерес к защите частной жизни в конфиденциальной информации относительно очевиден: например, осознание того, что положительный ВИЧ-статус конкретного индивида может стать достоянием всего мира, вызывает понятное беспокойство, и требования о возмещении морального вреда указанного субъекта персональных данных кажутся оправданными. Напротив, анонимные, обезличенные и не поддающиеся идентификации данные вызывают больше вопросов – например, нравственные страдания, связанные с потерей информации об устройстве или метаданных не относятся напрямую к личности конкретного человека и не имеют непосредственной связи с его возможными нравственными страданиями[2].

При этом использование фикции обезличивания может привести к отрицательным последствиям для общества. Этот вред, в конечном счете, обусловлен двумя противоречивыми результатами: (1) у тех, кто понимает несостоятельность подобной фикции, снизится доверие к законодателям и судебной системе, в то время как (2) те, кто не так хорошо разбирается в технологических аспектах, скорее всего, будут введены в заблуждение использованием фикции[3].

Отсутствие беспокойства по поводу обезличенных данных также может привести к тому, что потребители и законодатели, которые их представляют, в целом будут меньше беспокоиться о конфиденциальности такой информации. Большинство потребителей в принципе не уделяют время прочтению политики обработки персональных данных, но те, кто это делает, могут не обращать на внимания на указанную проблему из-за ссылок на якобы обезличенные данные. Если же законодатели не выражают явного беспокойства по этому поводу, у компаний мало стимулов предпринимать усилия по сохранению конфиденциальности данных,

[1] Stoffel E.C. The myth of anonymity: de-identified data as legal fiction. – P. 133.

[2] Ibid. – P. 138.

[3] Ibid. – P. 146.

особенно если оно противоречит экономическому росту и широкому использованию технологий в целом.

Аналогия с правовым регулированием медицинской деятельности – новый взгляд на защиту персональных данных

В связи с изложенными выше недостатками современного законодательства о защите персональных данных среди правоведов развернулась дискуссия о том, как должным образом защитить индивидов, не оказывая негативного влияния на инновации.

К.А. Хаузер, Дж.У. Бэгби предлагают изменить современные подходы к защите персональных данных, проводя аналогию операторов данных с медицинскими организациями. Они предлагают десять принципов, на основе которых организации могут моделировать свою собственную стратегию управления данными.

1. *Осуществление надзора*. Советы директоров или иные надзорные корпоративные органы операторов данных должны демонстрировать важность управления данными в рамках своих обязательств по стратегическому планированию и надзору.

2. *Доверие.* Компании должны считать себя фидуциарными управляющими собранных данных, принимать обоснованные решения от имени субъектов данных и учитывать интересы заинтересованных сторон при определении использования данных.

3. *Точность.* Чтобы избежать ущерба, связанного с неточными данными, и гарантировать, что они принесут компании максимальную пользу, наборы данных должны быть сбалансированными и репрезентативными (т.е. давать оптимальное представление обо всех социальных слоях). Кроме того, алгоритмы должны разрабатываться различными командами, а прогнозы – проходить многоуровневую проверку на точность.

4. *Согласие.* Компании должны убедиться, что субъекты данных осведомлены о том, что информация о них собирается и получить согласие на ее обработку. При отсутствии согласия операторы данных должны иметь одно из следующих оснований для использования данных: (1) законный интерес; (2) договорная необходимость; (3) жизненно важный интерес пользователя; (4) юридическое обязательство; (5) общественный интерес.

5. *Выбор.* Фирмы должны предоставлять субъектам данных возможность определять степень охвата и использования их личной информации.

6. *Конфиденциальность.* Компаниям следует периодически проводить оценку конфиденциальности, чтобы определить, для чего собираются данные и как они будут использоваться, каким образом к ним будет осуществляться доступ, в каком виде будут реализованы защита и хранение и др. для выявления рисков и устранения их последствий.

7. *Безопасность.* Данные должны быть защищены от несанкционированного доступа, утечек и иных угроз. Информация должна не только надежно храниться и быть защищена специальными средствами и методами, но и должны быть разработаны политики, предотвращающие непреднамеренный или неправомерный обмен данными.

8. *Управление записями.* Картирование данных – это процесс отслеживания данных, хранящихся у организаций, от их источника до места назначения, который поможет операторам: (1) определить, какие персональные данные они хранят, для чего они хранятся и где они хранятся; (2) оценить любые риски для безопасности или конфиденциальности физических лиц; (3) принять меры по снижению этих рисков; (4) обеспечить легкий поиск и передачу данных.

9. *Совет по данным.* Компании должны создать Совет по данным, в который будут входить специалисты, обладающие глубокими знаниями в области информации и обработки данных, технологий, бихевиористики, юриспруденции и др. Комитету будет поручено разрабатывать политику обработки данных и рассматривать потенциальные варианты использования данных.

10. *«Человек в петле».* Указанный принцип включает в себя несколько аспектов. Во-первых, компаниям следует обеспечить контроль со стороны персонала за любым автоматизированным анализом. Во-вторых, для обеспечения точности и соответствия принципам управления данными необходим контроль со стороны различных общественных наблюдателей, а также периодическое или выборочное тестирование. В-третьих, именно людям следует анализировать предлагаемые нововведения в части обработки информации, чтобы убедиться, что они соответствуют принципам

управления данными. Мониторинг и быстрое реагирование на неточные, несправедливые или незаконные результаты применения инноваций требуют умения быстро выявлять проблемы, разрабатывать решения по их устранению и вносить изменения.

Заключение

Таким образом, стремительный рост использования больших данных и развитие технологий их обработки требуют более широкого обсуждения того, как компании собирают, используют и монетизируют персональные данные, и как закон идет в ногу с технологическими достижениями.

С одной стороны, с развитием новых технологий и бизнес-моделей законодательство о защите персональных данных постоянно дополняется и изменяется. Важность и значительность защиты данных потребителей подтолкнули государственную власть к принятию нормативных актов, направленных на контроль потока данных. Указанное привело к тому, что компании, участвующие в международных транзакциях, связанных с передачей данных, должны учитывать постоянно меняющиеся требования к конфиденциальности в различных странах, иначе они рискуют быть оштрафованными[1].

С другой стороны, хотя возможность собирать и анализировать большие данные привела к ценным открытиям, она также нанесла ущерб тем, кто их предоставляет – субъектам персональных данных.

Для грамотного регулирования защиты персональных данных необходимо понимать последствия обработки данных для людей – от повторения существующей дискриминации до углубления экономического неравенства[2].

Уже сейчас недооценка последствий информатизации данных для человека привела к возникновению проблем с регулированием личной информации: современное законодательство о персональных данных не позволяет обеспечить должный уровень защиты неприкосновенности частной жизни. Принимая во внима-

[1] Houser K.A., Bagby J.W. Op. cit. P. 99.

[2] Wong W.H., Duncan J., Lake D.A. Op. cit. – P. 3.

ние то, что данные в настоящее время имеют существенную ценность и, что более важно, формируют то, как люди реализуют свою свободу воли, опосредуя различные экономические, политические и социальные связи, решение данной проблемы представляется крайней необходимостью.