РИСКИ РАЗВИТИЯ ОБОРОТА ДАННЫХ В ГОСУДАРСТВЕННОМ УПРАВЛЕНИИ[1]

Двинских Д.Ю., Талапина Э.В.[2]

Аннотация

Цифровизация государственного управления, в том числе управления на основе данных, предполагает организацию и урегулирование обмена данными в госуправлении. Для нормативно-правового регулирования обозначенного вопроса необходимо создание среды, снижающей основные риски внедрения обмена данными. Выявление, структурирование, описание и анализ рисков развития оборота данных в государственном управлении стало целью настоящей работы. В статье рассмотрены подходы к классификации рисков обмена данными и практика их регулирования, а также анализ основных рисков обмена данными для России и предложения по их учету в нормативно-правовом регулировании. Делается вывод, что регулирование оборота данных в государственном управлении должно быть комплексным, учитывающим как интересы индивидуумов и коммерческих организаций в части защиты данных, так и государства в части использования данных.

Анализ позволил выявить группу рисков в процессах цифровой трансформации экономики страны, влияющих на эффективность государственного управления в целом. В частности, для индивидуума значим риск нарушения прав и свобод человека при обработке больших данных. Для государства риски обусловлены сложностью и затратностью организации оборота данных, подразумевающего:

- *издержки анализа нестандартизированных данных;*
- *издержки времени на согласование доступа к данным, снижающие оперативность получения информации и ее ценность;*

[1] Статья подготовлена в рамках научно-исследовательской работы по государственному заданию РАНХиГС на 2019 г.

[2] *Двинских Дарья Юрьевна* – кандидат экономических наук, заместитель директора Центра междисциплинарных исследований Института государственного и муниципального управления Национального исследовательского университета «Высшая школа экономики»; ведущий научный сотрудник Центра технологий государственного управления Института прикладных экономических исследований Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации. Адрес: НИУ ВШЭ, 101000, Москва, ул. Мясницкая, д. 9/11. E-mail: ddvinskikh@hse.ru. *Талапина Эльвира Владимировна* – доктор юридических наук, доктор права (Франция); главный научный сотрудник Института государства и права РАН; главный научный сотрудник лаборатории правоприменительной практики в экономике РФ РЭУ им. Г.В.Плеханова; ведущий научный сотрудник Центра технологий государственного управления Института прикладных экономических исследований Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации. Адрес: РАНХиГС, 119571, Москва, пр. Вернадского, д. 82. E-mail: talapina-ev@ranepa.ru.

– *риски потери либо пиратского использования конфиденциальных и секретных данных.*

Нивелирование перечисленных рисков требует масштабных мер со стороны государства в сфере правового регулирования и в области политических решений, а также значительных бюджетных инвестиций.

Новизна изложенных решений заключается в предлагаемой системе связей между рисками развития оборота данных, обусловленного цифровой трансформацией госуправления, основными участниками процесса оборота данных, находящимися в зоне риска при развитии обмена данными, и мерами, которые помогают учесть экономический и юридический интерес участников.

Ключевые слова: цифровая экономика; открытые данные; риски оборота данных; большие данные; государственное управление.

Введение

Цифровая трансформация экономики Российской Федерации, формирование больших массивов информации в цифровой форме во всех сферах социально-экономической деятельности становится вызовом для государственных органов, ставя их перед необходимостью преобразования. Оборот данных в государственном управлении, отвечающий реалиям развития общества и бизнеса, способен воспрепятствовать ускоренному устареванию государства. При этом стоит учитывать, что на текущий момент в процессе внедрения оборота данных имеется и ряд рисков, требующих как организационных, так и правовых корректировок.

Основной проблемой, на изучении которой сконцентрировались авторы настоящей статьи, является необходимость сбалансированного учета рисков оборота данных в государственном управлении при организации нормативно-правового регулирования. Особенность правового регулирования цифровой трансформации в Российской Федерации, и оборота данных в частности, заключается в доминировании программного подхода к разработке и корректировке нормативной правовой базы, регламентирующей процессы информационного обмена, создания инфраструктуры и обеспечивающей легитимность и безопасность использования открытых данных в государственном управлении.

Основным документом стратегического планирования, определяющим направления развития оборота данных в государственном управлении и формирующим цели и задачи его нормативного регулирования в перспективном периоде, является Национальная программа «Цифровая экономика Российской Федерации», паспорт которой был утвержден в 2018 г.[3]. Этой программе предшествовали документы 2017 г. «Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы»[4]

[3] Паспорт Национальной программы «Цифровая экономика Российской Федерации». Утвержден президиумом Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам (протокол от 24 декабря 2018 г. № 16).

[4] Указ Президента Российской Федерации от 09.05.2017 N 203 // URL: http://kremlin.ru/acts/bank/41919 (дата обращения: 05.05.2019).

и программа «Цифровая экономика Российской Федерации», утвержденная распоряжением Правительства РФ от 28.07.2017 N 1632-р[5].

Перечисленные стратегические документы не только определяют направления цифрового развития. Они включают перечень мер государственного регулирования, нацеленных на нивелирование рисков, связанных с ростом числа государственных организаций и коммерческих структур, собирающих первичную информацию о физических и юридических лицах, развитием межведомственного электронного документооборота и формирующимся рынком данных. Стремительность цифровых трансформаций обусловливает острую нехватку исследований по данной проблематике. Необходимо отметить, что многие из поднимаемых в статье вопросов более фундаментально исследованы за рубежом, нежели в России, потому привлечение иностранного опыта крайне полезно.

Несмотря на принятые и запрограммированные изменения в нормативном правовом регулировании основных процессов оборота данных, остаются проблемы, создающие существенные барьеры на пути формирования новых институтов цифровой экономики, развития цифровых технологий и связанных с ними видов экономической деятельности, а также обусловливающие риски функционирования рынка данных и развития их оборота в государственном управлении.

Задачами данного исследования являются: выявление основных рисков развития оборота данных в государственном управлении для ключевых заинтересованных сторон и формирование системы предложений по управлению рисками с целью последующего учета в практической экспертной деятельности.

Данные как основа цифровой экономики

Очевидным трендом в общемировом масштабе стало отношение к данным как к основе современной экономики. К примеру, эксперты компании “Gartner” выделяют пять этапов зрелости цифрового правительства (электронное, открытое, датацентричное, полностью цифровое и «умное»). Согласно этой градации, для датацентричного правительства характерно открытие всех данных в качестве основной технологии, а показателем реализации служит количество услуг, предоставляемых на основе данных[6].

В программе «Цифровая экономика Российской Федерации» (2017 г.) подчеркивалось, что в цифровой экономике именно данные в цифровой форме являются ключевым фактором производства во всех сферах социально-экономической деятельности.

Паспортом национальной программы «Цифровая экономика Российской Федерации» в рамках создания благоприятных правовых условий для сбора,

[5] Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 03.08.2017 (ныне утратила силу).

[6] URL: https://www.gartner.com/smarterwithgartner/5-levels-of-digital-government-maturity/ (дата обращения: 05.05.2019).

хранения и обработки данных предусматривается принятие в июле 2019 г. трех федеральных законов:

1) уточняющего порядок обезличивания персональных данных, условий и порядка их использования,
2) формирующего благоприятные правовые условия для сбора, хранения и обработки данных (определение правил доступа и обработки общедоступной информации),
3) предусматривающего определение состава сведений, составляющих разного рода тайны (банковская, тайна связи, врачебная, коммерческая и пр.).

Ключевое понятие данных необходимо четко определить. Если обратиться к действующему законодательству, то в Федеральном законе от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – Закон об информации) понятия информации и данных используются как равнозначные: информация – это сведения (сообщения, данные), независимо от формы их представления. Интересно, что в Федеральном законе от 20.02.1995 N 24-ФЗ «Об информации, информатизации и защите информации» понятие «данные» относилось лишь к персональным данным (и базам данных). О чем это говорит? Во-первых, развитие технологий и постепенная «оцифровка» повлияли на «выравнивание» значений этих терминов, и понятие «данные» стало распространяться на любую информацию. Во-вторых, отождествление информации и данных произошло в некоем глобальном понимании, вне зависимости от их формы. То есть согласно Закону об информации данные могут быть не только цифровыми.

Такой подход отвечает теории информационного права, но мало стыкуется с пониманием цифровой экономики и программными российскими актами, в которых речь идет только о данных в цифровой форме. Выразим надежду, что это противоречие будет устранено в результате мероприятий, предусмотренных программой «Цифровая экономика».

Но помимо формального понимания есть еще и содержательное. Если вникнуть в суть разграничения данных и информации, то уместно воспроизвести пирамиду семантической иерархии DIKW (data (данные), information (информация), knowledge (знания), wisdom (мудрость)) Рассела Акоффа, предложенную им в 1989 г. (рис. 1).

Рисунок 1

Пирамида Акоффа

Источник: (Филяк, 2017, с. 524).

Из рисунка становится ясно, что данные в большинстве своем не структурированы, а информация, составленная на основе данных, – структурированный ресурс. Категории же знаний и мудрости отражают ценность информации, создавать которую может человеческий разум. В эпоху больших данных предлагается перевернуть эту пирамиду, образовав воронку, где фильтром выступят уже информационно-аналитические и когнитивные системы (Филяк, 2017, с. 526).

Как утверждают специалисты, при определении состава больших данных важную роль играет разграничение терминов раскрытых (опубликованных) и открытых данных, так как эти понятия не являются аналогами и достаточно широко используются в ИТ-среде. В массивы «больших данных» входят как раскрытые, так и «открытые данные», как часть данных, доступных для обработки теми или иными средствами программного обеспечения.

Раскрытые данные – это любые сведения в любой форме о чем-либо, которые может легально и без ограничений получить каждый заинтересованный пользователь. «Открытые данные» (Open Data) – это конкретная ИТ-технология по раскрытию и поддержанию актуальных на текущий момент, машиночитаемых сведений, которые обеспечиваются определенным субъектом. И периодически, по регламенту, «открытые данные» обновляются (актуализируются). Набор показателей в «открытых данных» практически неизменный, поэтому на основе накопленных файлов можно изучить динамику имеющихся показателей. Но главное назначение «открытых данных» заключается в их применении в ИТ-сервисах и системах (Каращук, Майорова, Прохоров, 2018, с. 79). Добавим – в применении с целью создания новых данных.

Таким образом, еще одно важное понятие нуждается в разъяснении – открытые данные. Основные характеристики открытых данных содержит Хартия открытых данных, принятая в 2013 г. странами – участницами «Большой восьмерки»[7], которая сконцентрирована на открытости государственных данных. С учетом принципа открытости данных по умолчанию (openness by default), государства должны публиковать как можно больше данных, причем в машиночитаемой форме. Действующим российским законодательством предусматривается существование информации в особой форме – форме открытых данных. Федеральным законом от 07.06.2013 N 112-ФЗ[8] в Закон об информации внесены дополнения, что «информация, размещаемая ее обладателями в сети «Интернет» в формате, допускающем автоматизированную обработку без предварительных изменений человеком в целях повторного ее использования, является общедоступной информацией, размещаемой в фор-

[7] URL: https://data.gov.ru/hartiya-otkrytyh-dannyh-gruppy-vosmi (дата обращения: 05.05.2019).

[8] Федеральный закон от 07.06.2013 N 112-ФЗ «О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации" и Федеральный закон "Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» // Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 07.06.2013.

ме открытых данных». Подзаконные акты уточняют перечни открытых данных, исходящих от государственных органов (наименования органов власти, план проведения проверок юридических лиц и индивидуальных предпринимателей на очередной год, реестры лицензий на конкретные виды деятельности и пр.).

Собственно, само существование перечней открытых данных государственных органов выглядит странно на фоне принципа открытости по умолчанию («все открыто, за исключением…»). Кроме того, в перечень попали совершенно разрозненные элементы информации, которые часто общеизвестны. При этом не учитывается такой важный элемент открытых данных, как их последующее использование. Еще раз подчеркнем момент, который упускается из виду в нашей стране: открытые данные, создаваемые государством, предоставляются в распоряжение гражданскому обществу, чтобы оно ими пользовалось, обогащало, изменяло, интерпретировало с целью совместного производства публично значимой информации (Grynbaum, Le Goffic, Morlet-Haidara, 2014, p. 720). В реальности же складывается впечатление, что открытые данные – формальный элемент деятельности органов власти, необходимый для их рейтингования и оценки деятельности, а не путь к созданию публично значимой информации негосударственными субъектами.

Остается определить большие данные. В науке нет единства мнений относительно понимания этого термина. Преобладающим является подход трех ключевых характеристик (трех «V») больших данных: большой объем данных (Volume), разнообразие форматов данных (Variety), высокая скорость их генерирования (Velocity). Иногда дополнительно выделяют сложность данных (Complexity). Некоторые ученые также классифицируют по четырем «V» (Value – ценность данных как экономический результат от обработки данных), пяти «V» (Veracity – достоверность данных) и даже шести «V» (Validation – проверка данных) (Bagnoli, 2015).

Важно подчеркнуть, что большие данные существуют уже в цифровой форме и собираются посредством интернета. Это данные из соцсетей, метаданные веб-сайтов, данные интернета вещей, как промышленного, так и частного характера (данные геолокации со смартфонов и фитнес-девайсов). Большие данные могут приобретаться на онлайн-рынках, иметь характер бизнес-данных (о платежах, административные данные), частное или публичное происхождение. Разнообразие больших данных побуждает искать возможности упорядочивающей их классификации.

Попытки классификации данных

Вряд ли возможно создать исчерпывающую классификацию больших данных. Экономистов в такой классификации больше интересуют источники происхождения данных, юристов – возможности обособления правовых режимов. В качестве отправной точки обратимся к представленной в литературе таблице, которая наглядно демонстрирует множественность оснований для классификации (табл. 1).

Таблица 1

Классификация больших данных

По возможности доступа		По субъекту формирования		По возможности идентификации		По источникам поступления			По особенностям информации	
Раскрытые	Закрытые	Государственные	Частные	Определяемые	Неопределяемые	Интернет	Мобильные операторы	Интеллектуальные системы	Больших объемов	Сложного состава

Источник: (Каращук, Майорова, Прохоров, 2018, с. 78).

Специалисты по источникам данных классифицируют их как:

1) правительственные («открытые данные»), т.е. персональные или неперсональные данные, собираемые органами государственного сектора;
2) данные пользователей, потребителей и бизнеса, добровольно оставленные на ИТ-платформах;
3) сгенерированные (с помощью файлов cookie, данных ISP, данных eCall, даже данных пациентов) (Lundqvist, 2018, p. 192).

Также выделяются социальные данные (Social Data) – это часть больших данных, создаваемых людьми в некоммерческих целях: данные из различных социальных сетей, фотобанков, блогов, чатов и т.д. (Денисова, Мухутдинов, 2015, с. 229). С юридической точки зрения важно отметить, что общего правового режима данных не существует (Saint-Aubin, 2015, p. 142), а вместо единой классификации данных можно выделить лишь отдельные их виды (персональные, ноу-хау, тайны). Прежде чем ответить на вопрос о подходящей классификации данных, необходимо обратить внимание на несколько проблем.

Во-первых, собственность на данные. Этот вопрос интересен тем, что в нем сосредоточены разные узловые проблемы права. Прежде всего, следует различать европейский и англосаксонский подходы. Теория информационных вещей берет начало в игнорировании англосаксонским правом разницы между обязательствами, вытекающими из ответственности и из права собственности. В соответствии с экономическим анализом права, экономическая ценность информации позволяет считать ее юридической вещью (например, “propertization” персональных данных). Эта теория оказывает определяющее влияние на утилитаристский подход при выборе решений. Европейские страны длительно сопротивлялись и продолжают сопротивляться такой теории. Вместо информационных вещей (information goods, biens informationnels) во французской юридической литературе предлагается понятие патримониальных (имущественных) прав на данные, на информационное имущество, с тем чтобы уйти от понятия собственности (Saint-Aubin, 2015, p. 148). Согласно этой позиции, у индивидуума не существует

права собственности на свои персональные данные, а только право контроля за их обработкой: это субъективное право, которое осуществляется через третьих лиц (Saint-Aubin, 2015, p. 143).

Тем не менее проблема собственности на данные поднята в европейской Стратегии единого цифрового рынка, и противостояние европейского и американского права еще не закончилось.

Во-вторых, из проблемы собственности на данные возникает дилемма, что собственно есть персональные данные – это объект основных прав человека (публичное право) или вещь, товар (частное право)? Иными словами, речь идет об установлении правового режима (частно-правового или публично-правового), включающего способы защиты права. В советское время, когда о собственности говорить было не принято, широко использовалось понятие владения. Оно даже стало ключевым в создании специфического вещного права (оперативного управления). В ситуации с данными тоже прибегают к этому способу – технически есть своего рода глобальное правило: тот, кто собирает данные, тот «владеет» ими. Поэтому существует потребность в автоматизированной и эффективной процедуре переговоров по сделкам облачных вычислений для определения «владельца» данных и того, будут ли данные «разделены» между поставщиком облака и конечными пользователями, врачами и пациентами и т.п. (Corrales, Fenwick, Forgó, 2017, p. 203).

В-третьих, проблема соотношения публичного и частного права в регулировании данных. На более общем уровне речь идет о разных подходах к информации (и, соответственно, данным) в этих двух главных подсистемах права. Долгое время в публичном праве формировался институт информационной открытости (транспарентности), который в последние годы привел государственное управление некоторых стран к внедрению упомянутого выше принципа открытости по умолчанию. В частном же праве традиционная «закрытость» индивидуумов обусловила формирование института тайн, связанных с их жизнью и деятельностью (коммерческая, банковская и пр. тайны). В то же самое время закрытая информация в виде персональных данных «пронизывает» как частное, так и публичное право. Следствием такой непростой конфигурации стало сосуществование разнообразных правовых режимов информации разных видов и неизбежные конфликты между ними.

На специальном уровне – применительно к персональным данным – режимы их публично-правовой и частно-правовой защиты переплетаются. К примеру, возникает вопрос: как сочетать право на доступ к публичной информации, расширяющееся в свете открытого правительства, и право на защиту частной жизни (Bouhadana, 2015, p. 125).

В-четвертых, проблема международного или глобального регулирования. Тот факт, что интернет наносит удар праву в целом и традиционным методам регулирования в частности, в юридической литературе обсуждается активно. Разумеется, в идеале должны быть общая стандартизация и регулирование классификации данных, признаваемые всеми странами. Только это вряд ли возможно, поскольку существуют политические, фак-

тические и национальные обстоятельства. Есть и страны, не участвующие в международных переговорах. Вероятно, единственно возможного решения для всех нет (Weber & Burri, 2012, p. 126). О невозможности международного правопорядка говорят и в контексте исследования юридической эволюции – такой правопорядок предполагает либо неоспоримое доминирование одной страны, либо бесспорный консенсус между всеми странами; но даже торговые соглашения в рамках ВТО не имеют на сегодня такой степени признания (Halpérin, 2014, p. 189).

Обозначенные проблемы следует учитывать и при выборе варианта урегулирования оборота данных, и при создании классификации данных, которая, вероятно, ограничится нуждами государственного управления и не будет иметь универсального характера. На наш взгляд, наиболее юридически очевидным является подразделение данных на виды в зависимости от их правового режима: персональные данные, общедоступные данные, регулируемые законом тайны.

В то же время четкое разделение правовых режимов не всегда возможно – в реальности данные могут перемешиваться. В частности, большие данные могут содержать персональные данные. Такой «вклад» персональных данных в совокупность публичных данных, используемых и повторно используемых в предоставлении публичной услуги, должен быть оценен (Guglielmi, 2015, p. 84). И, возможно, разработан особый правовой режим. Сбор данных, произведенных прямо или косвенно индивидуумами, нуждается в урегулировании: требуется переоценить технико-юридические способы совместного использования данных (Saint-Aubin, 2015, p. 145). Это – перспективное направление для юридических исследований.

Юридическое значение будет иметь и классификация в зависимости от источника происхождения данных, если при этом четко обозначен правовой статус субъекта – обладателя данных: государственные данные и частные данные (частных юридических лиц и персональные данные). Классификация данных по субъекту формирования наиболее значима для экономического анализа, поскольку различение таких типов данных, как частные (данные индивидуумов и коммерческих организаций) и государственные, позволяет определить «собственника» данных, права и экономические интересы которого могут быть нарушены. Возможность нарушения прав порождает риски оборота данных и формирует необходимость экономического и правового регулирования процесса оборота данных. Таким образом, именно здесь сходятся юридический и экономический анализ.

Риски развития оборота данных в государственном управлении

Выделение частных и государственных данных позволяет систематизировать риски оборота данных в государственном управлении. Риски здесь связаны с нарушением прав частных лиц (индивидуумов и коммерческих организаций) и государства и последующими экономическими потерями от некорректного использования данных. В систематизированном виде риски представлены в Таблице 2. Поясним ее содержание.

Таблица 2

Риски оборота данных

Субъект формирования данных	Тип данных	Риск оборота данных	Управление риском оборота данных
Частные лица (индивидуумы и коммерческие организации)	Индивидуальные (персональные)	Нарушения прав и свобод человека при обработке больших данных	Совершенствование правового режима защиты персональных данных при обработке больших данных в государственном управлении
	Данные коммерческих организаций	Нарушение коммерческой тайны	Нормативное регулирование режимов доступа к сведениям коммерческих организаций
Государство	Государственные	Значительные дополнительные затраты на анализ данных как результат отсутствия стандартизации	Стандартизация представления, обработки и хранения данных в государственном управлении
		Замедление формирования потока данных	Нормативно-правовое регулирование оперативного обновления и использования данных ПФР, ФОМС, ЕСИА и других источников, а также данных, автоматически формируемых интернетом вещей
		Киберугрозы для государственных информационных систем, риски потери либо пиратского использования конфиденциальных и секретных данных	Участие в разработке норм международного права по соблюдению кибербезопасности критической информационной инфраструктуры. Разработка учебных программ по информационной безопасности, обучение сотрудников госучреждений и населения. Организация информационных платформ для обмена актуальными данными о киберугрозах и их источниках всех участников информационных рынков

Источники: Составлена авторами.

Индивидуумы

Главным и самым значимым риском для индивидуума при обороте данных в государственном управлении являются возможные *нарушения основных прав и свобод человека при обработке больших данных.*

Как указывалось выше, в больших данных содержится значительное количество информации персонального значения. Источниками персональных данных, образующих массив первичной информации о физических лицах, служат заполняемые гражданами формы идентификации на сайтах госорганов для получения различного рода государственных услуг, а также для приобретения товаров и услуг в коммерческих структурах. Эти дан-

ные получили определение как большие пользовательские данные. Кроме того, поисковыми системами в интернете собираются персональные данные о личных интересах и предпочтениях граждан, на базе которых формируются специализированные профили физических лиц.

Легитимность сбора, хранения и обработки персональных данных обеспечивается в соответствии с российским законодательством предоставленным пользователем согласием на их обработку. Учитывая, что большинство информационных систем запрашивает персональное согласие на обработку предоставляемых данных, а условия использования этих данных содержат несколько страниц сложного юридического текста, явно не рассчитанного на рядового пользователя, эта персональная информация часто вполне легально становится товаром на рынке данных. В результате автоматизированной обработки формируются характеристики пользователей, которые в дальнейшем используются операторами сетей для собственных целей либо передаются ими другим заинтересованным лицам. Отсутствие правовых норм, регулирующих использование больших пользовательских данных в Российской Федерации, лишает граждан юридической возможности защиты своих прав. Нарушения прав граждан «стимулирует» то, что такая информация представляет прямой коммерческий интерес и может быть использована работодателями при найме на работу потенциальных претендентов, финансовыми аналитиками при оценке финансовой благонадежности клиентов банка, при формировании целевой персональной рекламы коммерческими организациями. Формально нарушение ими Федерального закона «О персональных данных»[9] может быть опротестовано в судебном порядке, однако, как правило, определить источник утечки данных не представляется возможным.

Среди персональных данных, имеющих коммерческую ценность, можно выделить данные:

– медицинских учреждений – о состоянии здоровья, психических, физиологических и физических характеристиках пациентов;
– судебных инстанций – данные по правонарушениям и уголовным делам;
– налоговых служб – о доходах физических лиц;
– банков – о состоянии счетов физических лиц;
– операторов мобильной связи – о местонахождении и содержании телефонных звонков физических лиц;
– кадровых структур работодателей – о карьерных перемещениях работников.

Указанная персональная информация представляет интерес для государственных, коммерческих, научных, аналитических и консалтинговых организаций, однако ее использование возможно только при условии необратимой утраты связи с физическим лицом. Обеспечение такого рода безвозвратной анонимности данных предъявляет особые требования к разработке алгоритмов кодирования данных и нуждается в нормативной правовой поддержке.

[9] Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных» // Собрание законодательства РФ. 2006. № 31 (ч. 1). Ст. 3451.

Все сказанное имеет отношение и к возможным нарушениям прав граждан при обработке данных для целей государственного управления. Традиционное использование статистической информации для формирования отчетных данных органами исполнительной власти характеризовалось отлаженным механизмом деперсонификации личных данных. Распространенная в последние годы тенденция привлечения альтернативных источников для формирования фактических значений целевых показателей государственных программ и других документов федерального и регионального уровня требует разработки правовых норм, регулирующих эти процессы в системе госуправления.

Говоря более предметно, риски вызваны неопределенностями законодательных трактовок в определении порядка обезличивания персональных данных, об условиях и порядке их использования, а также об определении ответственности за ненадлежащую обработку персональных данных. Отсутствует унифицированный порядок получения согласия на использование персональных данных и обеспечения соблюдения прав и интересов граждан. Не уточнена ответственность за ненадлежащую обработку и нарушение безопасности использования персональных данных.

Коммерческие организации

Основным риском является нарушение коммерческой тайны.

Обратной стороной оборота данных для коммерческих организаций становится раскрытие коммерческой тайны и риск потери конкурентного преимущества. Проиллюстрировать эту проблему можно без привязки к цифровому пространству. Представим государственную программу, которая кроме инструмента стратегического планирования считается еще и публичным документом, размещаемым в открытом доступе. Мероприятия, погруженные в программу, становятся объектами публичных обсуждений. Заметим при этом, что реальными исполнителями государственных программ, и в особенности федеральных и региональных проектов как составных элементов программы, являются государственные и частные коммерческие организации. Условиями их участия может быть как субсидирование, так и кооперационные механизмы (например, ГЧП), предполагающие финансовое участие со стороны частного партнера. А теперь смоделируем ситуацию, когда в публично доступном тексте государственной программы фиксируется перечень ее исполнителей, вплоть до деталей финансового участия сторон. В результате коммерческие организации, участвующие в реализации программы, попадают в уязвимую позицию по отношению к конкурентам, получившим подробную информацию о направлениях их стратегического развития и финансовых рисках. А государство испытывает риск от факта, что зарубежным конкурентам становится доступна информация о том, на деятельности каких именно фирм будет держаться успех страны в развитии конкретных направлений.

Раскрытие пообъектных сведений содержит в себе угрозу для всех частных лиц, поэтому развивается деперсонификация сведений и формирование неперсонифицированных баз данных. Так, для индивидуумов эта

процедура обеспечивает значительный прогресс в управлении рисками. При этом для юридических лиц в любом случае остается риск потери сведений, являющихся коммерческой тайной: для многих отраслей, не насыщенных большим количеством игроков, простая фильтрация данных по региону и отрасли позволит идентифицировать конкретного игрока.

В связи с этим необходимо прецедентное формирование режимов пользования информацией, возникающих из конкретных обоснований бизнесом состава сведений, распространение которых таит в себе стратегическую угрозу.

Государство

Как ни странно, государство может столкнуться с еще большими рисками при обороте данных.

1. *Значительные дополнительные затраты на анализ данных как результат отсутствия стандартизации.*

Отсутствие единых стандартов представления, обработки и хранения данных в информационных системах органов власти приведет к созданию технически несопоставимых массивов данных, на анализ которых потребуются дополнительные затраты. С подобной проблемой государство уже сталкивалось на этапе информатизации органов власти, когда информационные системы не коррелировали друг другу.

В настоящее время разработано и эксплуатируется значительное число государственных информационных систем (ГИС), предоставляющих доступ к своим открытым наборам данных. Создаются государственные межведомственные информационные системы, хранящие преимущественно статистическую информацию. Однако даже получение официальной статистической информации часто сопряжено с техническими проблемами и требует участия ИТ-специалистов для извлечения необходимых данных.

Требование интероперабельности данных (заметим, большинство из которых – персональные), обеспечения возможности использования данных, собираемых и хранимых одним оператором, другими участниками информационных рынков, становится одним из наиболее значимых требований применительно к данным в государственных информационных системах. Амбициозной задачей преобразования системы государственного управления является создание государства-платформы, объединяющего в единую систему все ведомственные информационные ресурсы и реализующего госуслуги вне зависимости от ведомственной принадлежности данных. Отсутствие единых стандартов хранения и обмена данными и отсутствие законодательной базы для разработки подобных требований может послужить серьезным препятствием использования информационных ресурсов в госуправлении.

Кроме того, отсутствие единых требований к обороту данных существенно снижает эффективность применения цифровых технологий не только в госуправлении, но и в организациях бюджетной сферы и бизнесе. В частности, препятствует использованию механизмов государственно-частного партнерства для цифровых технологий обмена данными в органах государственной власти. Многообразие форматов данных в коммерческих информационных системах значительно осложняет их использование в го-

сударственном управлении и приводит к дублированию данных информационных систем, увеличивая затраты на реализацию цифровой трансформации управления в стране.

Помимо этого, развитие технологий интернета вещей, в частности промышленного интернета вещей, также замедляется отсутствием стандартов в указанной области. Не разработаны национальные стандарты технологий интернета вещей и промышленного интернета вещей. Отсутствуют национальные стандарты, регламентирующие использование датчиков, средств измерений и измерительных систем, обеспечивающих функционирование автоматизированных устройств и систем, реализующих эти технологии, с учетом соблюдения требований безопасности, совместимости и технологической нейтральности.

2. *Замедление формирования потока данных.*

Фактор, замедляющий процессы своевременного обмена релевантными данными, – это ограниченность возможностей участников экономической деятельности по обновлению сведений об абонентах/клиентах (с их согласия) дистанционно через информационные системы органов государственной власти. В частности, часто нет оперативного обновления сведений, хранимых Пенсионным фондом России, Федеральным фондом обязательного медицинского страхования (ФОМС) и Единой системой идентификации и аутентификации (ЕСИА). К этой проблеме примыкает отсутствие перечня сведений, устанавливаемых операторами связи, которые при необходимости предоставляются заинтересованным лицам и включают в себя данные об устройствах интернета вещей (о конечном оборудовании, функционирующем без участия человека) и использующих его лицах. Таким образом создаются барьеры на пути развития оборота данных, поступающих благодаря интернету вещей, как явлению, способному перестроить экономические и общественные процессы посредством исключения из части действий и операций участие человека. Наконец, в настоящее время отсутствуют четко определенные принципы и порядок раскрытия данных об используемом в рамках интернета вещей оборудовании, своевременном подключении к сети интернет и безопасном функционировании устройств.

3. *Киберугрозы для государственных информационных систем, риски потери либо пиратского использования конфиденциальных и секретных данных.*

Вопросы информационной безопасности требуют комплексных решений: оперативного реагирования на инциденты, создания новых технологий и продуктов кибербезопасности, а также правового регулирования в этой сфере.

«Уровень угроз в информационном пространстве повышается, число рисков увеличивается, а негативные последствия разного рода кибератак носят уже не локальный, а глобальный характер и масштаб», – отмечалось на «Инфофоруме–2018»[10]. В ходе пленарных заседаний форума установлена

[10] URL: https://interaffairs.ru/news/show/19338 (дата обращения: 05.05.2019).

необходимость содействовать выработке международных правовых норм по созданию международной системы информационной безопасности.

Основным объектом киберугроз в России, как и во всем мире, является банковская сфера. По официальной статистике, объем несанкционированных операций со счетов юридических лиц по итогам 2016 г. составил порядка 1,9 млрд руб., в 2015 г. – около 3,8 млрд руб. Объем несанкционированных операций с использованием платежных карт за 2016 г. равен 1 млрд. руб.[11]. Однако жертвами кибернападений становятся также и государственные структуры, и коммерческие организации.

Система управления рисками оборота данных в государственном управлении

Выявленные риски требуют мер по снижению негативных последствий их реализации посредством создания целой системы управления рисками, элементами которой могут стать следующие составные части.

Индивидуумы и коммерческие организации

Для преодоления рисков нарушений основных прав и свобод человека необходимо усовершенствовать правовой режим защиты персональных данных и данных коммерческих организаций при обработке больших данных в государственном управлении. Необходимо конкретизировать формулировки нормативно-правовых актов в части определения:

– порядка обезличивания персональных данных и данных коммерческих организаций;
– условий и порядка использования персональных данных и данных коммерческих организаций;
– ответственности за ненадлежащую обработку таких данных.

Требует унификации порядок получения согласия на использование персональных данных, который должен обеспечить соблюдение прав и интересов граждан. Он должен содержать нормы, определяющие ответственность за ненадлежащую обработку и нарушение безопасности использования персональных данных. Самостоятельной задачей становится нормативное закрепление режимов доступа к сведениям, составляющим коммерческую тайну.

Государство

Преодолеть риски, описанные выше, могут помочь следующие мероприятия.

1. *Стандартизация представления, обработки и хранения данных в государственном управлении.*

Разработка стандартов представления, обработки и хранения данных в системах государственного управления позволит снизить затраты бюджета

[11] URL: https://tass.ru/politika/4406609 (дата обращения: 05.05.2019).

на обработку первичных данных и формирование информационных систем, доступных органам государственной власти и общественным структурам.

Необходимо устранить имеющие место пробелы в системе регулирования, образованной основополагающими национальными стандартами Российской Федерации, а также сопутствующими правилами стандартизации. Опыт развитых стран показывает, что для устойчивого развития нужна выработка рекомендаций в части упрощения процедур разработки документов по стандартизации. К конкретным задачам подобного рода относятся:

– корректировка деятельности технических комитетов по стандартизации, упрощение процедур и сокращение сроков разработки и актуализации документов по стандартизации, ускоренное принятие национальных документов по стандартизации на основе либо с учетом стандартов наиболее авторитетных ассоциаций и организаций;
– обеспечение доступности фонда стандартов, подлежащего переводу в цифровой машиночитаемый формат (на основе принципа открытых данных).

Решением этих проблем могла бы стать разработка комплексного проекта изменений в основополагающие стандарты Российской Федерации, в том числе в ГОСТ Р 1.1-2013 «Стандартизация в Российской Федерации. Технические комитеты по стандартизации. Правила создания и деятельности», ГОСТ Р 1.2-2014 «Стандартизация в Российской Федерации. Стандарты национальные Российской Федерации. Правила разработки, утверждения, обновления и отмены», ГОСТ Р 1.6-2013 «Стандартизация в Российской Федерации. Проекты стандартов. Правила организации и проведения экспертизы», ГОСТ Р 1.7-2014 «Стандартизация в Российской Федерации. Стандарты национальные. Правила оформления и обозначения при разработке на основе применения международных стандартов».

Кроме того, интересам правовой унификации оборота данных в государственном управлении могут послужить:

а) развитие технологий оборота данных и нормативное регулирование цифрового взаимодействия предпринимательского сообщества и государства.

Развитие технологий оборота данных позволит усовершенствовать существующие практики в сфере межорганизационного взаимодействия предпринимательского сообщества и государства в части сбора и предоставления отчетных данных в системе государственного стратегического и оперативного управления. Так, насущной необходимостью являются: нововведения в области инвентаризации форм отчетности, в том числе при сборе статистической информации, разработка новых подходов к формированию отчетности. В частности, рекомендуется создание «карты данных» органов исполнительной власти федерального и регионального уровня, подлежащих предоставлению в качестве отчетности вышестоящим организациям и Росстату, выявление перечня дублирующих и избыточных показателей. На основе всестороннего анализа данных должны быть сформулированы рекомендации по оптимизации запрашиваемой отчетности и исключению избыточного регулирования. Следует расширить круг статистических пока-

зателей, для сбора которых используется выборочное, а не сплошное статистическое наблюдение. Должна быть обеспечена возможность заполнения и представления отчетности непосредственно в местах образования первичных данных, их программная обработка и передача агрегированной информации на порталы федеральных органов исполнительной власти с помощью автоматизированных технологий;

б) стимулирование внедрения электронного документооборота.

Важным этапом процесса формирования сопоставимых данных в системе государственного управления является электронный документооборот. Однако в настоящее время практически отсутствует обязанность организаций и государственных органов принимать документы в электронном виде или в виде электронных дубликатов. Необходимо законодательно изменить ситуацию, когда учреждения требуют параллельно с электронными документами предоставлять оригиналы или их бумажные копии. Сложившаяся практика приводит к потере смысла развития электронного документооборота, который в таком случае не ведет ни к экономии средств, ни к ускорению процессов документооборота и повышению их надежности. В перспективе нужно законодательно полностью исключить повторное предоставление уже выданных ранее государственным органом оригиналов и копий документов, которые необходимы для получения любых видов государственных услуг.

Для повышения эффективности электронного документооборота в системе государственного управления целесообразно подготовить предложения по стимулированию взаимодействия операторов электронного документооборота. В частности, экономически оправдано введение обязательной функциональной обязанности операторов электронного документооборота в виде заключения договоров о взаимодействии с любым другим оператором электронного документооборота (ЭДО) в соответствии с Правилами, утверждаемыми Правительством Российской Федерации. Договоры оператора ЭДО о присоединении к нему системы другого оператора ЭДО должны с необходимостью стать публично открытыми, что не соблюдается в настоящее время. Наконец, должна быть обеспечена возможность определения Постановлением Правительства правил взаимодействия операторов электронного документооборота, а также возможность их подключения к единой системе межведомственного электронного взаимодействия;

в) разработка норм правового регулирования автоматизированных или самоисполняемых сделок.

Устранения пробелов законодательства требуют также автоматизированные или самоисполняемые сделки (смарт-контракты). В частности, это умные контракты и компьютерные алгоритмы для заключения и поддержания коммерческих контрактов посредством технологии блокчейн. В этом аспекте Россия рискует отстать не только от развитых стран, но и от соседей, которые уже ввели смарт-контракты, в частности, от Республики Беларусь. Широкое использование смарт-контрактов повышает доверие в деловой среде и позволяет компаниям сконцентрироваться на поиске новых способов получения прибыли, что приводит к росту национальной экономики;

г) корректировка понятийного аппарата в системе электронного документооборота.

Для избежания правовых коллизий, порожденных расхождениями в трактовке понятия «электронный документ» в различных нормативно-правовых актах, необходимо согласовать определения электронного документа в Гражданском кодексе Российской Федерации и в Законе об информации. Оптимальное решение – унифицировать понятие электронного документа и выработать единую трактовку электронной документации в нормативно-правовых актах, регулирующих данную сферу;

д) введение правовых норм, устанавливающих приоритеты электронной регистрации результатов работ и направленных на ускорение развития оборота данных.

Для стимулирования современных методов оборота данных предлагается установить приоритет электронной регистрации, в том числе с использованием электронных реестров, и придание юридической силы электронной регистрации. При этом необходимо разработать ограничительные нормы использования аналогового документооборота в целях снижения риска «косметической» цифровой трансформации.

2. Нивелирование рисков замедления формирования потока данных.

Это возможно сделать за счет регулирования использования альтернативных источников данных, формирования правового регулирования предоставления таких данных их владельцами либо операторами (сотовыми операторами, клиниками).

Регулирование должно включать и требования по оперативному доступу к актуальным данным.

3. Создание режима кибербезопасности в системах государственного управления.

Характерная особенность киберугроз – удаленность их источников от объектов, на которые эти угрозы направлены. Источники киберугроз могут находиться в другой стране и, как правило, вне правовой юрисдикции их жертв. Это значительно осложняет оценку ущерба от такого рода действий и получение материальных компенсаций нанесенного вреда. Усилий государственных регуляторов недостаточно для решения этой проблемы. Создание режима кибербезопасности требует разработки и принятия норм международного права по соблюдению кибербезопасности критической информационной инфраструктуры. Кроме того, необходима разработка нормативной базы организации межведомственного взаимодействия по вопросам обеспечения информационной безопасности и консолидация усилий государственных структур и коммерческого сектора.

Не менее значимым фактором для разработки экономических и юридических мер противодействия киберугрозам является динамичность информационного пространства, не позволяющая предусмотреть и предвидеть все потенциальные киберугрозы. В этих условиях возможности правового регулирования ограничены, и на первый план выступают экономические меры, направленные на минимизацию рисков реализации киберугроз, такие как:

а) разработка учебных программ по информационной безопасности, обучение сотрудников госучреждений и населения;
б) организация информационных платформ для обмена актуальными данными о киберугрозах и их источниках всеми участниками информационных рынков;
в) координация мероприятий по обеспечению кибербезопасности. Решение соответствующих проблем должен организовать Центр компетенций кибербезопасности, созданный на базе российской государственной компании «Ростелеком»[12]. В числе задач Центра – разработка и внедрение комплексных проектов, таких как организация центров управления информационной безопасностью, корпоративных и ведомственных центров Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак, обеспечение безопасности критической информационной инфраструктуры и автоматизированных систем управления, построение и эксплуатация комплексных систем защиты информации под ключ.

Заключение

Использование цифровых данных стало мотором цифровой экономики в ее частном секторе. Именно бизнес понял выгоды и преимущества платформ и интеллектуального анализа данных. Но этот опыт может применяться и в государственном секторе, в частности в государственном управлении.

Как показывает зарубежная практика и отечественные разработки, большие данные могут успешно использоваться для выработки государственной политики, формирования официальной статистики, администрирования доходов, аудита результативности бюджетных расходов и реализации иных государственных функций (Добролюбова, Южаков, Ефремов, Клочкова, Талапина, Старцев, 2019, с. 106). Промышленный интернет способен помочь в реализации контрольно-надзорной деятельности.

Важно подчеркнуть, что подобная цифровизация государственного управления затрагивает не только органы государственной власти, но и другие субъекты процесса. К примеру, если не обязать субъектов экономической деятельности сохранять информацию в форме открытых данных, мы не получим для свободного повторного использования базы по контрактам в области государственных закупок, государственно-частного партнерства.

Несмотря на столь позитивные ожидания, нельзя не отметить противоречивость позиции России в отношении роли данных и возможностей их сбора и обработки. С одной стороны, подчеркивается польза и потенциал использования открытых данных. С другой стороны, усиливается контроль за сбором и хранением данных (закон Яровой), ужесточаются требования доступа к интернету, принят закон о суверенном интернете. Закрытость данных и обособление русскоязычного интернета от глобальной сети

[12] URL: https://rg.ru/2018/05/22/v-rossii-poiavilsia-centr-kompetencij-kiberbezopasnosti.html (дата обращения: 05.05.2019).

может в перспективе сдержать развитие цифровой экономики в России, создать новые вызовы и привести к технологическому отставанию (ввиду отрыва от передовых практик развитых стран в сфере ИКТ)[13]. Представляется, что многие недостатки правового регулирования являются следствием недостаточной комплексной (экономической и юридической) проработки.

Если говорить о правовом регулировании, то на оборот данных в государственном управлении, открытых и больших, должно откликнуться все законодательство. Помимо изложенных выше моментов, касающихся детальной регламентации специальных вопросов, только комплексное, сбалансированное реформирование законодательства способно обеспечить непротиворечивые правовые режимы. К примеру, предполагается, что антимонопольное законодательство будет играть значительную роль в отношении больших данных, касательно таких злоупотреблений, как маргинальное сжатие (случаи, связанные с PSI), дискриминационный доступ к персональным данным, эксклюзивные соглашения (о разделе), нарушение правил защиты данных при получении персональных данных, злоупотребления при использовании, идеальная монополия ценообразования. Даже чрезмерный сбор данных может нанести антимонопольный ущерб (Lundqvist, 2018, p. 211).

Особое направление – принятие автоматизированных решений на основе интеллектуального анализа данных. Вспомним пирамиду Акоффа, превращающуюся в воронку при помощи технологий больших данных. И здесь, несмотря на привлекательность скорости и возможности финансовой оптимизации, мы вступаем на весьма чувствительную территорию «человеческого». Дело в том, что технократический подход к управлению имеет свои пределы. В частности, алгоритмы и двоичные коды не предназначены для определения политики, так как политика – искусство, которое происходит от этической сферы человеческих существ и принадлежит им исключительно как созданиям, «наделенным разумом и совестью» (ст. 1 Всеобщей декларации прав человека). Программисты склонны слишком подчеркивать эффективность шифрования и кодов как политических инструментов, способных верифицировать и соединять отдельные решения без посредников. Но политика и управление, конечно, намного больше, чем простое соединение голосов, хранение баз данных в синхронизации или предписание сделок через алгоритмы. Возможность видеть мир во всей его сложности контекстно-зависима, и это связано с сильным этическим измерением, с прямым человеческим участием. Все-таки информационная эффективность и автоматизация – не окончательная цель человеческих сообществ (Atzori, 2017).

В статье поднимается проблема рисков развития оборота данных в государственном управлении, актуальность которой значительно укрепили последние государственные инициативы в области внедрения НСУД, развития ФИС СП и локальных информационных систем ФОИВов и РОИВов.

[13] См.: Цифровая экономика и пути ее развития. Цифровая экономика – прорывные технологии и регулирование // Центр международной торговли, Москва (World Trade Center, Moscow). Статья (в 2-х частях) на интернет-портале www.wtcmoscow.ru. 02.10.2018–09.10.2018 (дата обращения: 05.05.2019).

Развитие оборота данных кроме очевидных преимуществ в сфере качества управления и политики открытого государства, связано со значительными рисками, обременяющими владельцев данных. В статье систематизированы основные болезненные для индивидуумов, коммерческих организаций и государства вопросы, которые возникают в связи с информационной открытостью. Это риски использования персональных данных, раскрытия личной информации, потери конкурентного преимущества и иные ситуации, ограничивающие личные свободы и экономические возможности.

Дальнейшее развитие оборота данных требует институционального и правового учета интересов заинтересованных сторон, связанного с развитием нормативно правовой базы и внедрением технологических решений в области управления и защиты информации.

ЛИТЕРАТУРА

1. Денисова О. Ю., Мухутдинов Э. А. Большие данные – это не только размер данных // Вестник технологического университета. – 2015. – Т.18. – № 4. С. 226–230.
2. Добролюбова Е.И., Южаков В.Н., Ефремов А.А., Клочкова Е.Н., Талапина Э.В., Старцев Я.Ю. Цифровое будущее государственного управления по результатам. – М.: Издательский дом «Дело» РАНХиГС, 2019.
3. Каращук О.С., Майорова Е.А., Прохоров Ю.Н. «Большие данные» и перспективы их использования в предпринимательской деятельности // Вестник НГИЭИ. – 2018. – № 10. – С. 77–87.
4. Филяк П.Ю. Сети, большие данные (BIG DATA), интеллектуальный анализ данных (DATA MINING) и обеспечение безопасности // Информация и безопасность. – 2017. – Т. 20. – № 4. – С. 522–527.
5. Atzori M. Blockchain Technology and Decentralized Governance: Is the State Still Necessary? 2017. URL: https://ssrn.com/abstract=2709713 (дата обращения: 05.08.2019).
6. Bagnoli V. Competition for the Effectiveness of Big Data Benefits // Springer. 2015. DOI 10.1007/s40319-015-0382-4.
7. Bouhadana I. Les collectivités territoriales confrontées à la diffusion d'informations identifiantes dans le cadre de la mise en œuvre des services publics en ligne // Droit et gouvernance des données publiques et privées à l'ère du numérique. Sous la dir. de I. Bouhadana, W. Gilles. Paris, Les éditions Imodev. 2015. P. 115–125.
8. Corrales M., Fenwick M., Forgó N. (eds.). New Technology, Big Data and the Law // Springer. 2017. URL: https://www.springer.com/gp/book/9789811050374 (дата обращения: 05.08.2019).
9. Grynbaum L., Le Goffic C., Morlet-Haidara L. Droit des activités numériques. Paris, Dalloz. 2014.

10. Halpérin J.-L. Five Legal Revolutions Since the 17th Century. An Analysis of a Global Legal History // Springer. 2014. URL: https://www.springer.com/gp/book/9783319058870 (дата обращения: 05.08.2019).

11. Guglielmi G. J. Service public et droit des données personnelles // Droit et gouvernance des données publiques et privées à l'ère du numérique. Sous la dir. de I. Bouhadana, W. Gilles. Paris, Les éditions Imodev. 2015. P. 77–84.

12. Lundqvist B. Big Data, Open Data, Privacy Regulations, Intellectual Property and Competition Law in an Internet-of-Things World: The Issue of Accessing Data. Bakhoum M., Conde Gallego B., Mackenrodt M-O., Surblytė-Namavičienė G. (Eds.). Personal Data in Competition, Consumer Protection and Intellectual Property Law. Towards a Holistic Approach? // Springer. 2018. URL: https://www.springer.com/gp/book/9783662576458#aboutBook (дата обращения: 05.08.2019).

13. Saint-Aubin Th. Les droits de l'opérateur de données sur son patrimoine numérique informationnel // Droit et gouvernance des données publiques et privées à l'ère du numérique. Sous la dir. de I. Bouhadana, W. Gilles. Paris, Les éditions Imodev. 2015. P. 141–155.

14. Weber R.H., Burri M. Classification of Services in the Digital Economy // Springer. 2012. URL: https://www.springer.com/la/book/9783642316340 (дата обращения: 05.08.2019).

RISKS OF DATA TURNOVER DEVELOPMENT IN PUBLIC ADMINISTRATION

Daria Yu. Dvinskikh
PhD, Deputy Director at the Center of Public Service Development,
Institute for Public Administration and Governance, HSE.
Leading Researcher of the Center for Public Administration Technologies,
Institute of Applied Economic Research, Russian Academy of National
Economy and Public Administration under the President of the Russian Federation.
Address: 11, Myasnitskaya Str., 101000, Moscow, Russian Federation.
E-mail: ddvinskikh@hse.ru

Elvira V. Talapina
Doctor of Legal Sciences, Doctor of Law (France);
Chief Researcher, Institute of State and Law, Russian Academy of Sciences;
Chief researcher, Plekhanov Russian University of Economics;
Leading Researcher of the Center for Public Administration Technologies,
Institute of Applied Economic Research, Russian Academy of National
Economy and Public Administration under the President of the Russian Federation.
Address: 82, Vernadsky Av., 119571, Moscow, Russian Federation.
E-mail: talapina-ev@ranepa.ru

Abstract

The President's address sets the task of public administration digitalization, including data-based management, for which it is necessary to organize public adminis-

tration data-turnover regulation. Regulation of this issue involves the creation of the environment that reduces the main risks of implementing data turnover.

The purpose of this article is to identify the structure, describe and analyze the risks of data turnover in public administration.

The classification of data-turnover risks and the regulatory practice are discussed in the article, as well as the analysis of the main risks and legal regulation of data-turnover for Russia Federation. It is concluded that the regulation of data turnover in public administration should be comprehensive, taking into account the interests of an individual in terms of personal data protection and the State in terms of data use.

The analysis revealed a group of risks, affecting the main processes of digital transformation of the country's economy and efficiency of public administration as a whole. In particular, the risk of violation of human rights and freedom is very significant for an individual. The analyses of non-standardized data organizing, data-access and data-piracy costs are significant for the government. Expensive legal and policy decisions are necessary to manage data-turnover risks.

Keywords: digital economy; open data; data-turnover risks; big data; public administration.

Citation: Dvinskikh, D.Yu. & Talapina, E.V. (2019). Riski razvitiya oborota dannykh v gosudarstvennom upravlenii [Risks of Data Turnover Development in Public Administration]. *Public Administration Issue*, no 3, pp. 7–30 (in Russian).

REFERENCES

1. Denisova, O.Yu. & Muhutdinov, E.A. (2015). Bol'shie dannye – eto ne tol'ko razmer dannykh [Big Data are Not Only the Data Size]. *Herald of Technological University*, no 4, pp. 226–230.

2. Dobrolyubova, E.I., Yuzhakov, V.N., Efremov, A.A., Klochkova, E.N., Talapina, E.V. & Startsev, Ya.Yu. (2019). *Tsifrovoe budushchee gosudarstvennogo upravleniya po rezul'tatam* [Digital Future of Performance Management in Public Administration]. Moscow: Delo.

3. Karashchuk, O.S., Mayorova, E.A. & Prokhorov, Ju.N. (2018). "Bol'shie dannye" i perspektivy ikh ispol'zovaniya v predprinimatel'skoy deyatel'nosti [Big Data and Prospects for Their Use in Entrepreneurial Activity]. *Bulletin NGIEI*, no 10, pp. 77–87.

4. Filyak, P.Ju. (2017). Seti, bol'shie dannye (BIG DATA), intellektual'nyi analiz dannykh (DATA MINING) i obespechenie bezopasnosti [Networks, BIG DATA, DATA MINING and Security]. *Informatsiya i bezopasnost*, no 4, pp. 522–527.

5. Atzori, M. (2017). *Blockchain Technology and Decentralized Governance: Is the State Still Necessary?* Available at: https://ssrn.com/abstract=2709713 (accessed: 05 August, 2019).

6. Bagnoli, V. (2015). *Competition for the Effectiveness of Big Data Benefits*. Springer. Available at: doi: 10.1007/s40319-015-0382-4 (accessed: 05 August, 2019).

7. Bouhadana, I. (2015). Les Collectivités Territoriales Confrontées à la Diffusion d'Informations Identifiantes dans le Cadre de la Mise en Œuvre des Services Publics en Ligne. In: I. Bouhadana, W. Gilles (eds.) *Droit et Gouvernance des Données Publiques Et Privées a l'Ere du Numérique*. Paris: Les éditions Imodev, pp. 115–125.

8. Corrales, M., Fenwick, M. & Forgó, N. (eds.) (2017). *New Technology, Big Data and the Law*. Springer. Available at: https://www.springer.com/gp/book/9789811050374 (accessed: 05 August, 2019).

9. Grynbaum, L., Le Goffic, C. & Morlet-Haidara, L. (2014). *Droit des Activités Numériques*. Paris: Dalloz.

10. Halpérin, J.-L. (2014). *Five Legal Revolutions Since the 17th Century. An Analysis of a Global Legal History*. Springer. Available at: https://www.springer.com/gp/book/9783319058870 (accessed: 05 August, 2019).

11. Guglielmi, G. J. (2015). Service Public et Droit des Données Personnelles. In : *Droit et Gouvernance des Données Publiques et Privées à l'Ere du Numérique* (eds. I. Bouhadana, W. Gilles). Paris Les éditions Imodev, pp. 77–84.

12. Lundqvist, B. (2018). Big Data, Open Data, Privacy Regulations, Intellectual Property and Competition Law in an Internet-of-Things World: The Issue of Accessing Data. In: M. Bakhoum, B. Conde Gallego, M-O. Mackenrodt, G.Surblytė-Namavičienė (eds.) *Personal Data in Competition, Consumer Protection and Intellectual Property Law. Towards a Holistic Approach?* Springer, Available at: https://www.springer.com/gp/book/9783662576458#aboutBook (accessed: 05 August, 2019).

13. Saint-Aubin, Th. (2015). Les droits de l'opérateur de données sur son patrimoine numérique informationnel. In: I. Bouhadana, W. Gilles. (eds.) *Droit et Gouvernance des Données Publiques et Privées à l'Ere du Numérique.* Paris: Les éditions Imodev, pp. 141–155.

14. Weber, R.H. & Burri, M. (2012). *Classification of Services in the Digital Economy*. Springer. Available at: https://www.springer.com/la/book/9783642316340 (accessed: 05 August, 2019).