ПРЕДЛОЖЕНИЯ ДЛЯ ПРОРАБОТКИ В РАМКАХ ФОРМИРОВАНИЯ КОНЦЕПЦИИ УПРАВЛЕНИЯ ДАННЫХ

1. Использование комплексного межотраслевого подхода к регулированию данных.

Вопросы сбора, обработки и использования данных затрагивают предмет регулирования различных блоков законодательства, при этом риски, связанные с использованием данных, создаваемые законодательством из одного блока, могут устраняться регулированием из другого блока. К ключевым блокам законодательства Российской Федерации, касающегося регулирования данных, относятся в том числе законодательство о персональных данных, гражданское законодательство, законодательство о защите конкуренции.

Таким образом, при выработке регулирования данных необходимо отталкиваться из системного применения законодательства и не ограничиваться точечным внесением изменений лишь в определенный блок законодательства, без учета влияния иных норм законодательства на регулируемые отношения. Новое регулирование данных должно органично встраиваться в систему действующего законодательства, в противном случае возникает риск появления несбалансированного регулирования или регулирования с пробелами.

2. Определение правового режима данных и распределение гражданских прав на них

В отсутствие определенности относительно наличия у лица права на массив данных, а также характера этого права, дальнейшая коммерциализация такого права в правовом поле является невозможной или значительно затрудненной. В этой связи для регулирования вопроса оборота данных одной из первоочередных задач является решение вопроса о распределении прав на данные.

Представляется, что одной из отправных точек для решения этого вопроса является анализ целесообразности разграничения понятий и правовых режимов «данные» и «информация», и их соотнесения, а также оценка необходимости регулирования доступа к данным, с учетом соблюдения законных интересов организаций, осуществивших инвестиции в создание специализированных цифровых платформ, сервисов и иных инструментов, обеспечивающих законный сбор и обработку данных. Это связано с проблематикой существования различных правовых режимов, в зависимости от выбранного подхода. Одним из возможных решений является

разграничение понятий «данные» и «информация». Вторым вариантом является подход к защите законных интересов собственников цифровой платформы, используемой для создания массива данных, через механизм регулирования доступа к данным. Детализация указанных подходов содержится в Приложении №1. Вместе с тем необходимо рассмотреть и иные варианты решения обозначенных проблем.

Еще одним вопросом является особенности доступа к данным иностранных субъектов. Иностранные компании вправе получить доступ к данным, с соблюдением требований, которые применяются к резидентам Российской Федерации, с учетом принципа взаимности. В качестве таких требований возможно установление различных специальных правовых режимов, например, запрета на доступ к данным без образования российского юридического лица. Необходимо избежать ситуации, когда иностранные компании, которые не соблюдают требования законодательства Российской Федерации, устанавливающего ограничения доступа к данным, будут иметь более привилегированное положение, по отношению к российским компаниям, которые данные требования соблюдают.

Безотносительно того, какой вариант изберет законодатель, определение места массивов данных в системе прав, характера и содержания прав, возникающих на них, является одним из ключевых вопросов обеспечения цивилизованного оборота данных и доверия участников возникающих отношений друг к другу, без которых невозможно полноценное внедрение технологий, основанных на обработке больших данных.

3. Учет международных и зарубежных подходов к регулированию данных в силу трансграничного характера оборота данных.

Обеспечение законности обработки персональных данных является одним из ключевых условий защиты прав граждан в цифровой среде и их доверия к интернет-сервисам. Вместе с тем получение согласия на обработку от субъекта в ряде случаев невозможно или сопряжено с несоразмерными затратами, что особенно актуально при обработке больших массивов данных.

В этой связи для обеспечения законности обработки при использовании цифровых технологий необходимо наличие сбалансированных и эмпирически-обоснованных оснований для обработки персональных данных без согласия субъекта. Как следствие, целесообразно комплексно проанализировать существующие в российском законодательстве основания для обработки персональных данных без согласия субъекта и практику их применения (в частности, таких оснований, как обработка в целях заключения и (или) исполнения договоров, для целей осуществления прав и законных интересов оператора или третьих лиц, для достижения общественно-значимых целей и др.) и с учетом существующих зарубежных подходов и международных норм сформулировать предложения о целесообразности

корректировки российского законодательства и правоприменительной практики по данному вопросу.

В частности, целесообразно рассмотреть вопрос о возможности отнесения таргетирования коммерческих предложений при обработке персональных данных для собственных нужд оператора, без передачи третьим лицам, к случаям допустимой обработки персональных данных без согласия субъекта в рамках законного интереса (legitimate interest) оператора, при условии того, что такая обработка не будет ущемлять права субъекта персональных данных.

Кроме того, необходимо предоставить субъекту персональных данных право после предоставления согласия изменить (расширить либо отозвать) предусмотренные таким согласием цели обработки, а также давать согласие с множеством целей и обработчиков, в том числе и дистанционным способом.

Необходимо предусмотреть возможность сбора согласий не только самим оператором персональных данных, но и третьими лицами в пользу оператора, действующими на основании соглашения с оператором.

На практике достаточно часто приходится сталкиваться с ситуацией, когда необходимо получить согласие не напрямую от субъекта, а от третьего лица, которое имеет возможность собрать такое согласие, и с которым есть соглашение. Целесообразно определить порядок установления и перечень требований к компаниям, которые будут осуществлять сбор согласий в интересах третьей стороны.

Кроме того, нужно исключить необходимость получать согласие субъекта для случаев выдачи оператором поручения на обработку персональных данных третьему лицу в определенных случаях. Например, привлеченному в связи с исполнением договора с гражданином (контактные центры, архивы, IT-подрядчики и т.д.). При этом на оператора возлагается обязанность предусмотреть в поручении (соглашении между оператором и обработчиком) требования к защите персональных данных, а также установление ответственности оператора, выдавшего поручение, за действия привлеченных им лиц перед субъектом.

Для прозрачности и информирования субъектов о круге лиц, обрабатывающих персональные данные по поручению оператора, предлагается ввести обязанность размещать актуальный перечень лиц, которым поручена обработка персональных данных, в общедоступных источниках или через личный кабинет, электронную почту и иными способами с возможностью управления этим списком.

Россия является участницей Конвенции Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных» от 28 января 1981 года № 108 (далее – Конвенция № 108), к которой был принят ряд изменений в октябре 2018 года, Российская Федерация подписала 10 октября 2018 года модернизированную версию Конвенции, тем самым подтвердив приверженность принципам и концепциям, заложенным в ней[1].

---

[1] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures

Модернизированная версия Конвенции № 108 представляет собой облегченный вариант вступившего в силу 25 мая 2018 года Регламента ЕС «О защите персональных данных» (EU General Data Protection Regulation), что с очевидностью следует из Пояснительного протокола к ней[2]. Как следствие, это порождает ряд обязательств Российской Федерации по имплементации положений европейского права в российское законодательство. Это касается не только конкретизации ранее существовавших принципов, но и появления новых принципов обработки данных, к которым, помимо уже существующих, добавлены: принцип прозрачности обработки данных, принцип обеспечения приватности по умолчанию (privacy by default) и в архитектуре предоставляемых товаров и услуг (privacy by default), принцип обеспечения подотчетности операторов за соблюдение требований законодательства о персональных данных, принцип обеспечения безопасности обрабатываемых данных.

Имплементация положений модернизированной Конвенции должна способствовать развитию трансграничного оборота данных с европейскими компаниями, что должно способствовать росту российской экономики в условиях, когда основными торговыми партнерами Российской Федерации долгое время были и продолжают выступать страны Европейского союза, главным образом Германия, Нидерланды и Италия[3]. При этом целесообразно имплементировать не все международные практики, а только те, которые соответствуют балансу интересов граждан, бизнеса и государства.

Вместе с тем, использование европейского подхода к регулированию данных в качестве основного не должно исключать возможности рецепции подходов к такому регулированию, выработанных в иных юрисдикциях (США, Сингапур, Япония), в случае, если они позволяют более оптимальным образом отразить баланс интересов граждан, бизнеса и общества и являются эмпирически выверенными и совместимыми с российскими реалиями.

По данным участников рынка в связи с довольно консервативным регулированием данных в Европе компании несут существенные издержки. Например, по оценке Deutsche Telecom, ежедневные потери телеком отрасли в ЕС из-за ограничений в обработке данных составляют 100 млн евро. При этом, по оценке Еврокомиссии, 450 млрд евро - нереализованный потенциал роста цифровой экономики из-за ограничений в сфере обработки данных. Для США, отличающихся мягким подходом к регулированию данных, характерны активные инновации, повышающие как выручку телеком компаний, так и прочих потребительских компаний. В США рынок сервисов, основанных на анализе больших данных, составляет 88 млрд долларов. Рынок цифрового

---

[2] Explanatory Report to the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 10.X.2018. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016808ac91a

[3] См.: Портал внешнеэкономической информации Минэкономразвития России. URL: http://www.ved.gov.ru/monitoring/foreign_trade_statistics/countries_breakdown/ (дата обращения: 24.04.2018).

маркетинга достиг 100 млрд долларов. Большие данные позволяют улучшать опыт потребителей путем создания новых сервисов.

В США существует тенденция, согласно которой права граждан в сфере данных определяются пользовательским соглашением с компанией; чувствительные данные требуют прямого согласия на обработку, при этом направления обработки прочих данных должны быть описаны в пользовательском соглашении; отсутствуют ограничения на объем и срок хранения данных; компании самостоятельно определяют механизм защиты данных, но несут ответственность за сохранность данных.

Доступность данных привела США к лидирующим позициям на мировом рынке больших данных и смежных рынках, например, AI. На мировом рынке аналитики больших данных США занимает более 50% рынка. Из Топ-100 компаний на рынке AI, развитие которой напрямую зависит от доступности данных, ~80% из США.

4. Создание организационно-правовых условий для повторного использования данных.

В условиях, когда одни и те же данные способны создавать новую ценность в зависимости от поставленных задач при их обработке, соединения с иными массивами данных или нового контекста использования, крайне важным является создание условий для того, чтобы одни и те же массивы данных, созданные государством или государственными органами и организациями, могли повторно использоваться заинтересованными лицами. В данном случае речь идет об открытых данных (open data), генерируемых органами публичной власти при выполнении своих функций, которые могут представлять ценность при решении задач, составляющих общественный интерес.

Законодательство должно создать необходимые организационно-правовые условия для обеспечения возможности обработки таких данных заинтересованными лицами. Для этого могут использоваться следующие инструменты:

1) создание банков данных, к которым должен предоставляться недискриминационный доступ на справедливых условиях;

2) закрепление рамочных (стандартных) условий предоставления доступа к таким банкам данных, которые могут использоваться также и в качестве модели для регулирования доступа к иным видам данных;

3) закрепление права создателя массива данных на указание своего имени (наименования) при дальнейшем использовании такого массива другими лицами как важного стимулирующего и репутационного механизма для предоставления доступа к ним.

Есть необходимость синхронизации планов развития государственных информационных систем с запросами предпринимательского сообщества и динамикой развития их подходов к обработке данных.

Должны быть сформированы правила (нормативные, технологические – прежде всего, на основании Open API Specification) для подключения к государственным информационным системам (ГИС), в том числе посредством «Цифрового профиля» и Национальной системы управления данными (НСУД) внешних приложений, созданных независимыми разработчиками, а также для открытия возможности для расширения за счет сторонних сервисов, прошедших сертификацию, услуг, предоставляемых гражданам и бизнесу.

Таким образом, сторонние разработчики будут обладать возможностью предлагать государству («владельцу» ГИС) разработку отдельных ее элементов и (или) связанных приложений (частей программно-аппаратного комплекса ГИС), а также разработку и предоставление целых цифровых сервисов, связанных с ГИС (как в модели подрядчика, так и в модели государственно-частного партнерства в «совместном предприятии», предоставляющем цифровые сервисы гражданам, бизнесу и государству).

Например, какой-либо из наиболее технологичных банков может взяться как за разработку программного обеспечения для оказания сервиса регистрации юридических лиц в качестве подрядчика, так и за оказание этого сервиса «под ключ» в качестве провайдера в партнерстве с государством, сообразно разделяя доходы и расходы.

Кроме того, речь может идти не просто об обмене данными между «государственными» и «коммерческими» сервисами или их интеграции, а, в перспективе, и о масштабном взаимодействии целых государственных и частных (коммерческих) цифровых платформ.

При этом требуют решения такие важнейшие аспекты организации данного доступа как необходимость получения согласий на доступ к данным, проработка механизмов права на неоднократный доступ (подписка), синхронизации с уже имеющимися практиками в сфере доступа к данным (например, ЕГРЮЛ), обеспечения необходимых технических характеристик соответствующих информационных систем, в том числе транспортных. Один из возможных подходов решения данных вопросов сформулирован отдельными участниками рынка и изложен в приложении № 2.

В части экономического механизма функционирования такой модели для внешних поставщиков может быть реализована схема двухуровневого доступа к данным, содержащимся в ГИС. Доступ к части данных может осуществляться по фиксированным тарифам, к другой части данных – по ценам, установленным оператором (операторами) ГИС, либо отдельных ее компонентов. Также возможен вариант, когда оператор взимает с внешних поставщиков конечных сервисов фиксированную плату за транзакции, осуществленные через соответствующие сервисы. При этом необходимо избежать ситуации, когда плата будет вводиться за получение тех сведений,

получение которых является не потребностью, а обязанностью для представителей предпринимательского сообщества (квазиналог).

Представляется целесообразным создать банки данных, доступ к которым предоставляется на недискриминационной и справедливой основе в отношении тех данных, которые созданы с привлечением бюджетных средств (речь идет о данных государственных информационных систем, реестров и иных данных, доступ к которым не является ограниченным в соответствии с законодательством о государственной тайне или иных видах тайн). При этом вполне возможно взыскание разумной платы за предоставление такого доступа, однако, которая не должна создавать барьеры для доступа к ней со стороны заинтересованных лиц.

Следует поощрять создание банков массивов данных на базе некоммерческих организаций, в том числе отраслевых объединений коммерческих организаций, которые на началах самостоятельно установленных правил будут предоставлять недискриминационный доступ к таким данным лицам, отвечающим определенным критериям (data commons).

Уже сейчас существуют такие массивы данных в области геномных данных[4], данных в области химических соединений, представляющих опасность[5], биомедицинских данных[6], и др. Здесь право должно максимально легализовать конструкции создания и распространения информации, схожие с теми, которые реализованы в движении open source (программное обеспечение с открытым исходным кодом).

В настоящее время в Гражданском кодексе Российской Федерации существуют опорные нормы для этого (например, ст. 1286.1 «Открытые лицензии»), однако право должно установить критерии недискриминационного и справедливого доступа, создать стимулы для участия лиц в наполнении таких банков данных. Это может быть реализовано, в частности, посредством разработки модельных (стандартных) условий соответствующих соглашений, а также закреплением права на указание создателя соответствующего массива данных (attribution right).

Модельные (стандартные) договорные условия могут выполнять двоякую роль. В определенных отношениях они будут носить императивный характер, не допускающий отклонений и обеспечивающий недискриминационный и справедливый доступ к определенным категориям данных. Для таких отношений характерно неравенство переговорных возможностей, наличие слабой стороны, которое обуславливает целесообразность императивного метода регулирования отношений (предоставление доступа или регулирование использования банков открытых данных, или данных, представляющих публичный интерес). При этом важно избежать неоправданного фрагментирования таких условий на множество видов, поскольку это будет влечь увеличение транзакционных издержек,

---

[4] The NCI's Genomic Data Commons (GDC) https://gdc.cancer.gov

[5] The Chemical Hazard Data Commons https://commons.healthymaterials.net

[6] https://commonfund.nih.gov/commons

связанных с анализом содержания таких условий и обеспечения совместимости использования различных массивов данных, распространяемых на разных условиях, между собой. Опыт с множеством, порой несовместимых между собой лицензий в сфере open source, свидетельствует о реальности данного риска.

Модельные (стандартные) условия могут использоваться в качестве ориентира для структурирования договорных отношений в отношении использования иных данных. Однако в таком случае стороны, разумеется, будут иметь возможность отступления от их положений. Однако и в таком случае, модельные (стандартные) условия могут использоваться в качестве бенчмарка для оценки справедливости договорных условий, в случае их оспаривания с помощью существующих средств договорного права (например, норм о договоре присоединения – ст. 428 ГК РФ).

Одним из стимулов для включения своих данных в создаваемые банки данных может выступать закрепление права на указание имени (наименования) создателя массива данных при дальнейшем использовании такого массива. Такое указание может иметь важное репутационное значение, а также играть роль в обеспечении защиты прав на такие данные в случае их использования в противоречии с целями, которые были обозначены в правилах использования соответствующего банка данных. Указание имени создателя данных также может иметь важное значение для оценки их возможного качестве и создания атмосферы доверия в рамках сообщества лиц, использующих их.

5. Обеспечение доверия в цифровой среде

Доверие является одним из ключевых условий развития инноваций, основанных на обработке данных[7]. Согласно исследованию Gartner, опасения пользователей относительно сохранности своих данных влекут самоцензурирование и сокращение количества выкладываемых в сеть данных, а также использование альтернативных способов защиты данных (VPN, плагины к браузерам и пр.)[8]. Это, в свою очередь, может повлечь сокращение и ухудшение качества данных, необходимых для адекватной персонализации сервисов. О негативном влиянии отсутствия доверия для развития технологий машинного обучения говорится и в материалах Мирового экономического

---

[7] OECD. Data-driven Innovation for Growth and Well-being. INTERIM SYNTHESIS REPORT. October 2014. P.58. OECD. Meeting the policy challenges of tomorrow's digital economy, 2016. Данный тезис признается и российским правительством. Как отметил в ходе Парламентских слушаний «Большие данные и защита прав пользователей» заместитель председателя правительства РФ Максим Акимов, «если не удастся создать атмосферу взаимного доверия, которое бы обеспечивало динамичное технологическое развитие с одной стороны, но с другой стороны – безусловно защищало бы права, базовые свободы и уверенность граждан в легальном, защищенном использовании их данных, если эту задачу решить не удастся, то обесценятся все иные: инфраструктурные, образовательные, технологические инициативы, которые содержатся в программе «Цифровая экономика».

[8] Gartner/Maverick Research: The Disappearing Customer. Published: 18 September 2017 3

форума[9]. Недавнее исследование ВЦИОМ демонстрирует, что большинство граждан выражают озабоченность непрозрачными механизмами использования их данных в социальных сетях[10]. Доверие к новым технологиям и лицам, их использующим, невозможно без определенного уровня прозрачности при их использовании, особенно в вопросах, которые затрагивают права гражданина. Учитывая, что гражданин представлен в цифровом пространстве в виде данных, регулирование данных о нем напрямую влияет на права, свободы и обязанности такого лица.

С целью обеспечения доверия в цифровой среде предлагается упростить процедуру предоставления согласия граждан на обработку данных в электронной форме. В частности, закрепить в Федеральном законе от 27 июля 2006 № 152-ФЗ «О персональных данных» варианты предоставления согласий дистанционно в электронной форме (смс-сообщения, электронная почта, заполнение формы на сайте и др.), а также нескольким обработчикам на разные цели.

Для целей упрощения процедуры получения согласия гражданина следует:

а) прямо предусмотреть конклюдентную форму предоставления согласия;

б) установить, что обязательные реквизиты распространяются только на бумажные и подписанные усиленной подписью согласия, но не на электронные документы простой электронной формы;

в) использовать понятные для пользователя визуальные средства описания совершаемых действий с персональными данными.

Для эффективного развития больших данных необходимо уточнить понятие «несовместимых целей» обработки, а также добавить дополнительные основания для обработки персональных данных без согласия субъекта. При оценке оператором персональных данных и надзорным органом совместимости последующей обработки персональных данных с целями сбора должны приниматься во внимание следующие персональные критерии: характер и объем обрабатываемых данных; обоснованные ожидания субъекта персональных данных; характер взаимоотношений между субъектом персональных данных и оператором; возможные негативные последствия такой обработки в отношении субъекта персональных данных; предпринятые оператором меры по обезличиванию персональных данных и иные адекватные меры защиты персональных данных.

Многие решения, касающиеся физических лиц, уже сейчас принимаются на основе аналитики данных, в том числе с помощью алгоритмов машинного обучения, в частности, решения о выдаче кредита, о принятии на работу. В Нью-Йорке на основании алгоритмической обработки

---

[9] How to Prevent Discriminatory Outcomes in Machine Learning. WEF Global Future Council on Human Rights 2016-2018. White Paper. March 2018.

[10] Персональные данные в интернете: возможности и риски. Исследование ВЦИОМ. 1 ноября 2018. URL: https://wciom.ru/index.php?id=236&uid=9401&fbclid=IwAR2_IaebzcdZT6348Ojgfbh7vACNPiKOtM4g_caYvc5TsmPs6WLmlwC8x1M

данных принимаются решения о том, в какую школу пойдет ребенок, какие районные отделы полиции укомплектовать большим количеством полицейских, куда следует направить с проверкой органы строительного надзора, какие метрики используются для оценки учителя[11]. Такие решения влияют на реализацию гражданами конституционных прав и нередко касаются социально незащищенных категорий граждан. Использование информационных технологий для принятия такого решений имеет немалый положительный потенциал, сокращая субъективизм, время принятия решений, стоимость конечного продукта для потребителя и пр. Однако, это касается лишь тех систем аналитики данных и машинного обучения, которые используют полные и достоверные входные данные и алгоритмы их обработки, которые не имеют предвзятостей (bias), которые могут повлечь дискриминацию физических лиц по какому-либо критерию (пола, расы, национальности, политических взглядов, проживанию на определенной территории, наличию или отсутствию профиля в сети Интернет и его содержимому и т.п.).

Дискриминационные начала могут появиться в алгоритмах обработки данных в силу различных причин. Во-первых, вследствие наличия определенных предубеждений у разработчиков алгоритма, которые они намеренно или бессознательно привнесли в его архитектуру. Иногда прошлый опыт позитивного или негативного взаимодействия разработчика алгоритма с представителями определенной социальной группы может стать причиной обобщающих выводов, не имеющих под собой достаточной эмпирической основы. Во-вторых, характер входных данных также может повлечь дискриминацию лиц по определенному признаку. Например, когда в качестве обучающих данных для системы рекрутинга используются исторические данные о работниках организации, в которых преобладает определенная социальная группа. Как следствие, такая система начинает отдавать предпочтение кандидатам на работу из такой социальной группы. Или когда вследствие недоступности или малочисленности данных об определенных категориях лиц, такие лица игнорируются или принижаются по сравнению с лицами, в отношении которых существует гораздо больше данных (это, как правило, лица, которые больше пользуются гаджетами и современными информационными сервисами и оставляют гораздо более обширный цифровой след о себе). Такого рода дефекты входных данных по мере принятия все большего количества решений на их основе, которые, в свою очередь, будут являться входными (обучающими) данными для будущих ситуаций, способствуют увековечиванию дискриминационных начал и «диктатуре данных» большинства над меньшинством. Это грубое нарушение принципов равенства граждан перед законом и недопустимости дискриминации, закрепленных в ст. 19 Конституции Российской Федерации и нормах международного права (например, в статьях 2 и 7 Всеобщей Декларации прав человека ООН 1948 года).

---

[11] Jim Dwyer. Showing the Algorithms Behind New York City Services // The New York Times, 24 August 2017.

Ситуация усугубляется еще и тем, что многие алгоритмы и системы машинного обучения работают по принципу «черного ящика», не позволяя отследить порядок принятия решения и тем самым, оценить обоснованность использованных критериев[12]. В некоторых случаях, это непринципиально, например, когда алгоритм строит маршрут для навигатора. Однако, когда некая система, руководствуясь непрозрачной и неподконтрольной логикой, ставит диагноз, назначает лечение, принимает решение об отказе в приеме на работу или в заключении договора страхования жизни, констатирует целесообразность условно-досрочного освобождения лица из мест лишения свободы, такого рода модель принятия решений вступает в противоречие с принципами правового государства.

6. Создание условий для обработки больших данных, обеспечения интероперабельности данных и саморегулирования на уровне индустриальных стандартов.

Существующие в текущем законодательстве понятия и режимы для обезличенных данных не отвечают современному уровню развития технологий. Обезличенные данные не должны рассматриваться как однородная субстанция. Можно условно их разделить на те данные, которые сохраняют связь с физическим лицом и тем самым могут быть деобезличены и данные, которые необратимо утратили связь с физическим лицом и не могут стать предметом деобезличивания. В первом случае, обезличенные данные должны рассматриваться как персональные данные, но в отношении них возможно установление более льготного режима обработки, в частности, за счет расширения круга оснований для их обработки без согласия субъекта. Во втором случае можно говорить о том, что данные перестали быть персональными и могут распространяться без ограничений, установленных законодательством о персональных данных.

В связи с этим целесообразно ввести термин «анонимные данные», под которым следует понимать данные (наборы данных), не позволяющие определить, к какому физическому лицу они относятся, в том числе информация, полученная в результате анонимизации персональных данных.

Данная категория используется в европейском законодательстве и находит свое отражение в идеологии модернизированной Конвенции № 108 и сопроводительных документах к ней. В соответствии с Пояснительным протоколом к Конвенции № 108: «Данные рассматриваются в качестве анонимных только в той мере, в какой невозможно ре-идентифицировать субъекта персональных данных или если такая ре-идентификация потребует неразумное количество времени, усилий или ресурсов, принимая во внимание

[12] Frank Pasquale. The Black Box Society: The Secret Algorithms That Control Money and Information. Harvard University Press. 2015; Marina Krakovsky, "Finally a Peek Inside the 'Black Box' of Machine Learning Systems," https://engineering.stanford.edu/magazine/article/finally-peek-inside- black-box-machine-learning-systems

доступные технологии на момент обработки и развитие технологий. Данные, которые выглядят как анонимные, поскольку не сопровождаются очевидными идентифицирующими субъекта элементами, могут в определенных случаях, тем не менее, допускать идентификацию индивида (не требуя неразумного количества времени, усилий или ресурсов). Это справедливо, например, для случаев, когда оператор или иное лицо имеет возможность определить лицо посредством комбинирования различных типов данных… В таких случаях данные не могут рассматриваться как анонимные и должны охватываться положениями Конвенции».

Основываясь на положениях данного международного договора Российской Федерации, основной критерий анонимных данных – отсутствие связи с физическим лицом, которая либо в принципе не может быть восстановлена в силу технологических соображений, либо теоретически может быть восстановлена, но в силу связанных с этим чрезмерных затрат это практически невозможно.

Критерии анонимных данных, будучи закрепленными в законе, позволяют оператору аргументировать свою позицию посредством ссылок на технические, экономические заключения и исследования и если уполномоченный государственный орган не согласен с ней, то он должен будет привести обоснованные контраргументы об обратном. Кроме того, введение категории анонимных данных позволит отнести к ним:

а) результаты аналитики персональных данных, которые представлены в виде высокоуровневой статистики, в частности, данные, касающиеся коллективных настроений в определенной группе или массовые геолокационные данные;

б) данные, полученные в результате отдельных методов обезличивания, которые не предполагают возможности ре-идентификации (например, метода изменения состава или семантики, который производит замену персональных данных результатами статистической обработки, обобщения или удаления части сведений; метода differential privacy, предполагающий добавление определенного количества «информационного шума» в массив данных, не позволяющий вычленить конкретного индивида из него);

в) зашифрованные данные, к которым у данного лица нет ключа и нет возможности его получить, исходя их критериев анонимных данных (дешифровать с использованием новых и доступных технологий, получить от контрагента или у другого лица на законных основаниях без чрезмерных финансовых или временных затрат).

Обработка данных оператором персональных данных с целью их анонимизации и последующая передача анонимных данных третьим лицам должна быть возможной без получения согласия субъекта персональных данных, если это не нарушает его законные права и интересы. При этом под анонимизацией можно понимать «действия, следствием которых является необратимая технологическая невозможность определить принадлежность данных субъекту персональных данных, при этом при определении такой

необратимости принимается во внимание уровень развития технологий, их доступность на рынке, а также невозможность такого определения в связи чрезмерными временными и финансовыми затратами».

Подходы по обработке анонимных данных могут быть зафиксированы в «кодексе этики» в сфере использования данных, который может быть разработан участниками рынка с привлечением представителей отраслевых ассоциаций, в том числе с участием уже созданных для этих целей предпринимательским сообществом структур, таких как Ассоциация больших данных, Институт развития интернета и других. Причем для обеспечения достижения консенсуса основных субъектов процесса формирования соответствующих норм, в том числе государства и граждан, и их соответствия целям социально-экономического развития при разработке данных подходов целесообразно использовать площадки, предусмотренные функциональной структурой национальной программы «Цифровая экономика Российской Федерации», такие как АНО «Цифровая экономика», соответствующие рабочие группы и центры компетенции.

В целях повышения ликвидности массивов данных и достижения синергетического эффекта от информационного взаимодействия возможна разработка в рамках саморегулирования добровольных стандартов сбора, хранения, обработки и обмена данными, что обеспечит «интероперабельность» (совместимость) данных, созданных и обработанных в рамках различных информационных систем. Такая совместимость будет способствовать формированию единой информационной экосистемы.

Однако в вопросах обеспечения интероперабельности необходима гибкость, вследствие чего она должна осуществляться преимущественно на уровне «мягкого» права (стандартов), нежели чем на уровне жестких законодательных предписаний. Это позволит более оперативно реагировать на нужды изменяющихся технологий и избежать появления неоправданных барьеров.

В зарубежной практике существует немало примеров инициатив по выработке стандартов интероперабельности на уровне саморегулирования. Например, в Сингапуре учрежден консорциум частных компаний для развития «интероперабельной» среды в сфере электронных платежей. Также в Сингапуре учреждено государственно-частное партнерство между частной компанией и государственным органом в сфере электронного здравоохранения по внедрению «интероперабельных» информационных систем здравоохранения.

При поддержке ЕС и Южной Кореи европейские и южнокорейские компании, исследовательские центры и университеты объединились в рабочую группу по развитию всемирной семантической «интероперабельности» Интернета вещей (Worldwide Interoperability for Semantics IoT). Следует наблюдать за тем, какой прогресс они смогут продемонстрировать в обозримом будущем.

7. Стимулирование горизонтальных отношений в сфере использования и защиты данных посредством перехода от методов административного контроля к наделению потребителей новыми эффективными возможностями защиты своих прав при нарушении порядка обработки их данных в цифровой среде.

Одной из проблем существующего правового режима персональных данных является отсутствие эффективных частноправовых механизмов защиты прав субъектов персональных данных.

Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» предусматривает, что субъект имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке (ч. 2 ст. 17). Однако указанные меры недостаточно эффективны. В случае нарушения прав субъектов персональных данных вред не будет иметь явно выраженной имущественной оценки.

Вместе с тем существует механизм контроля со стороны Роскомнадзора, который в сложившейся ситуации фактически стал единственным участником, контролирующим соблюдение прав граждан при обработке данных о них и формирующим соответствующую правоприменительную практику.

При этом Роскомнадзор действует в рамках административных процедур, предъявляя требования к операторам как поднадзорным субъектам. Как следствие, многие операторы следуют требованиям закона лишь формально, не выстраивая действительно эффективную защиту персональных данных.

Имеет смысл рассмотреть варианты, связанные с модернизацией уже существующей системы контроля, посредством приближения ее к субъектам персональных данных, которым необходимо представить соответствующие процессуальные инструменты.

Для преодоления сложившейся ситуации и формирования стимулов для защиты субъектами персональных данных своих прав с участием Роскомнадзора необходимо принять во внимание опыт деятельности Роспотребнадзора как органа исполнительной власти со схожей компетенцией – защитой интересов граждан-потребителей.

Имплементация нового средства защиты права может способствовать выработке более ответственного подхода субъектов к распоряжению своими данными и переносу рассмотрения многих спорных вопросов, связанных с использованием таких данных, с уровня «Роскомнадзор – оператор» на уровень «субъект — оператор». Роскомнадзор при этом может выступать в качестве эксперта как для субъекта, так и для оператора.

При этом в текущий момент указанные меры не должны приводить к росту финансовых санкций, применяемых к операторам.

В качестве преимущества данного предложения появляется сильный аргумент в пользу сбалансированности нового регулирования.

Учитывая, что подобный подход пока не был реализован в международном сообществе (в частности, в США, ЕС, Сингапур, Китай, Япония) есть возможность создать прецедент и привлечь дополнительное внимание зарубежного сообщества к российскому регулированию и программе «Цифровая экономика Российской Федерации» в целом.

Приложение № 1

I. В рамках одного из подходов решения вопросов прав на массивы данных представляется, что отправной точкой является разграничение понятий «данные» и «информация». В настоящее время понятие данные и информация рассматриваются как тождественные в российском законодательстве. Согласно Федеральному закону от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» «информация - сведения (сообщения, данные) независимо от формы их представления». Согласно Федеральному закону от 27 июля 2006 года № 152-ФЗ «О персональных данных», персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Вместе с тем, в сфере информационных технологий понятия «данные» и «информация» имеют разное значение. В соответствии с определением, данным Международной организацией по стандартизации, данные — поддающееся многократной интерпретации представление информации в формализованном виде, пригодном для передачи, связи или обработки. При этом информация – это результат интерпретации (смысл) такого представления.

Данные, выступая товаром, потребление которого одним индивидом, не снижает его объема/ценности для другого индивида (non-rival good), могут быть одновременно использованы для различных целей для создания различных видов товаров/услуг. При этом не существует ограничений в отношении количества целей использования данных. Соответственно, один и тот же массив данных может порождать разную информацию.

О необходимости разграничения понятий «данные» и «информация» при построении экономики, основанной на данных, говорит и ОЭСР, поскольку «информация, которая может быть извлечена из данных, зависит не только от самих данных, но и также от существующих аналитических возможностей по линкованию данных и извлечению из нее нового знания. Эти возможности зависят не только от доступных метаданных, аналитических технологий и методологий, но и от навыков и уже имеющегося знания у лица, обрабатывающего данные».

Существующие проблемы с определением правового режима и распределения прав на данные связаны с противоречивой правоприменительной практикой и различным пониманием понятий «данные» и «информация». Один и тот же массив данных может в зависимости от контекста и специфики оператора повлечь появление различной информации. Иногда эта информация будет относиться к физическому лицу и приобретать статус персональных данных, а иногда – носить исключительно технический характер. Например, геолокационные данные, получаемые с автомобиля, могут в результате их интерпретации посредством линкования с

иными данными и использования специальных технологий характеризовать поведение физического лица – водителя или пассажира. Вместе с тем, те же самые данные могут характеризовать перемещение определенного транспортного средства в пространстве и использоваться для решения сугубо технических задач (поиск оптимального маршрута, сокращение расхода бензина и пр.). Аналогичным образом, данные, получаемые с сенсоров «Умного дома» могут использоваться оператором для совершенствования сервиса, а в иных случаях – для определения предпочтений жильцов такого дома.

В настоящее время из-за отождествления понятий «данные» и «информация» исходный массив данных может быть квалифицирован как персональные данные безотносительно цели и контекста использования. Принимая во внимание, что режим персональных данных тесно связан с конституционным правом человека на неприкосновенность частной жизни (ст. 2 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных») и тем самым является проявлением нематериального блага, которое в соответствии с Гражданским кодексом РФ (далее - ГК РФ) является неотчуждаемыми и непередаваемыми иным способом (п. 1 ст. 150 ГК РФ), признание на такие данные какого-либо исключительного права другого лица будет вступать в противоречие с данными положениями. Это, в свою очередь, затрудняет коммерциализацию данных и создание цивилизованного рынка обмена массивами данных, который необходимо для развития технологий Больших данных, Искусственного интеллекта, Интернета вещей и др. Если провести разграничение между «данными» и «информацией», то можно снять обозначенное противоречие, признав за лицом право на данные, одновременно признавая за субъектом персональных данных права, предусмотренные законодательством о персональных данных. Такая ситуация укладывается в положения, предусмотренные п. 2 ст. 129 ГК РФ: «Законом или в установленном законом порядке могут быть введены ограничения оборотоспособности объектов гражданских прав, в частности могут быть предусмотрены виды объектов гражданских прав, которые могут принадлежать лишь определенным участникам оборота либо совершение сделок, с которыми допускается по специальному разрешению».

В условиях, когда данные приобрели высокую экономическую ценность, вопрос должен быть не столько в том, являются ли они объектом гражданских прав, а в том, кто обладает правом на них. В качестве основного принципа правонаделения можно было бы использовать следующий: право на данные предоставляются лицу, которое понесло затраты на их создание и (или) обработку. Данный подход основан на том, что создание и (или) обработка данных в ряде случаев требует несения финансовых и временных издержек, а также что в условиях современной экономики они являются ценным коммерческим активом. В случае, если исходные данные, подпадали под режим персональных данных, то оператор может приобрести гражданско-правовое право на собранный массив данных или результаты их аналитики в

случае, если были соблюдены требования законодательства о персональных данных, в частности, наличие законного основания для такой обработки. Если данные требования выполнены, то, как вариант, можно применить логику, схожую с той, которая используется в авторском праве: “автор производного или составного произведения осуществляет свои авторские права при условии соблюдения прав авторов произведений, использованных для создания производного или составного произведения” (п. 3 ст. 1260 ГК РФ). Такой подход может создать необходимые стимулы для инвестирования в процессы сбора и обработки данных. Однако необходима дополнительная проработка характера и содержания права, возникающего у создателя данных.

Для решения вопроса о сборе и обработке данных Интернет-площадок предлагается можно установить ряд принципов:

1) Соблюдение баланса между распространением института интеллектуальной собственности на базы данных и правом на доступ к информации. Родовым понятием, через которое база данных в настоящее время определена в статье 1260 ГК РФ, является «совокупность материалов». Это понятие толкуется в настоящее время чрезмерно ограничительно, и предлагается заменить его на более общее - «совокупность данных или сведений», оставляя при этом за ними признак самостоятельности. Такое решение даст использовать предусмотренные частью 4 ГК РФ договоры в отношениях по поводу таких объектов. Этим будет обеспечена судебная защита прав, возникающих в отношениях по поводу данных, в том числе защита их обладателей от злоупотреблений.

2) Данные пользователей, размещенные в различных базах данных, в том числе на UGC-ресурсах в открытом доступе (ресурсы с пользовательским контентом), могут быть использованы исключительно при наличии законных оснований и с соблюдением прав и законных интересов – как субъектов персональных данных, так и владельцев информационных ресурсов, в рамках которых они были размещены. При этом необходимо соблюдение баланса с правом на доступ к информации, в том числе для целей сбора данных для научных и статистических целей.

3) Соблюдение прав площадки, на которой размещаются данные, включая соблюдение технических и юридических правил пользования информационным ресурсом (в том числе ограничений по сбору и использованию данных), которые установлены площадкой, включая разрешение или запрет на использование поисковых роботов.

4) Соблюдение пользователями законодательства при получении доступа к данным, размещенным на площадке, прежде всего, наличие законного основания для обработки персональных данных.

5) Соблюдение владельцами площадок законодательства, недопущение установление дискриминационных условий по доступу к данным.

Права на отдельные объекты пользовательского контента (UGC-элементы) могут принадлежать как самим пользователям, так и иным лицам по различным основаниям. При таком подходе целесообразно сохранить за

площадками право определять правила и случаи разрешенного доступа к такому контенту (объектам авторского права). Такой подход позволит обеспечить интересы владельцев информационных ресурсов и изготовителей баз данных, созданных в результате функционирования информационных ресурсов, а также интересам пользователей, так как дает возможность в любое время осуществлять надлежащий контроль за использованием их контента.

Также предлагается закрепить норму о том, что не является нарушением использование извлеченных на законных основаниях из базы данных сведений, которые относятся к категории общедоступных в форме открытых данных.

Право создателя на данные может быть также структурировано по модели исключительного права на информацию, составляющую секрет производства. В таком случае возможно создание еще одного правового режима, параллельного с ныне существующим правовым режимом «ноу-хау». Это позволило бы избежать необходимости корректировки существующего понятия ноу-хау как сведений «любого характера (производственные, технические, экономические, организационные и другие) о результатах интеллектуальной деятельности в научно-технической сфере и о способах осуществления профессиональной деятельности, имеющие действительную или потенциальную коммерческую ценность вследствие неизвестности их третьим лицам, если к таким сведениям у третьих лиц нет свободного доступа на законном основании и обладатель таких сведений принимает разумные меры для соблюдения их конфиденциальности, в том числе путем введения режима коммерческой тайны» (ст. 1465 ГК РФ). С учетом того, что режим ноу-хау имеет ограниченную степень защиты (исключительное право на ноу-хау прекращается после раскрытия ноу-хау) и ограниченную оборотоспособность, возможна выработка дополнительных правовых режимов охраны данных. При этом следует сделать оговорку, что это только одно из возможных направлений в сфере правовой охраны данных.

Помимо получения сырыми данными «гражданско-правовой прописки», наделение лица, собравшего данные, правом, подобным ноу-хау, могло бы предоставить ему инструментарий защиты не случай недобросовестного завладения такими данными третьими лицами: возможностью предъявления требования о выплате компенсации, требования о запрете дальнейшего использования таких данных; возможно – требования о запрете коммерциализации товаров и услуг, разработанных с использованием таких данных.

Другим вариантом реализации цели по определению места «сырых данных» в системе объектов гражданского законодательства и определении характера прав, возникающих на них, является возврат исходного понятия «ноу-хау», которое существовало до поправок 2014 года. Оно было гораздо шире по своему охвату, и относя сведения о результатах интеллектуальной деятельности в научно-технической сфере или о способах осуществления

профессиональной деятельности лишь к возможным примерам ноу-хау, не исчерпывая ими его содержание, как сейчас.

II. В рамках альтернативного подхода регулирования прав на массивы данных предлагаются иные решения. Так, по мнению его авторов формирование инструментов для защиты данных через институт авторских и смежных прав на данные и распространение института интеллектуальной собственности на базы данных не в полной мере соответствует задаче защиты прав операторов персональных данных и иных цифровых платформ, поскольку охрана интеллектуальной собственности строится на основе т.н. творческого вклада в ее создание. Вместе с тем, формирование баз данных на современных цифровых платформах производится посредством предоставления доступа к специализированному интерфейсу, позволяющему пользователю самостоятельно формировать интересующий его и связанных с ним участников взаимодействия контент без творческого вклада владельцев цифровых платформ.

Права на указанный контент охраняются авторским правом и принадлежат пользователю, в случаях законного размещения такого контента. Более того, часть информации, в особенности, персональные данные, даже будучи консолидированой на той или иной цифровой платформе, не может быть ограничена в обороте владельцем цифровой платформы, либо порождать требования по выплате справедливого вознаграждения такому владельцу, например, если взята из иного источника, включая государственные информационные системы, либо иные общедоступные источники информации.

При этом не подлежит сомнению интеллектуальный вклад разработчиков цифровой платформы, направленный на создание информационной системы, обеспечивающей формирование и поддержку доступа к данным, включая способ организации такого доступа, дизайн и удобное представление данных, дополнительные сервисы, включая интеграцию с иными цифровыми платформами, осуществление торговой и рекламной деятельности и т.д.

Таким образом, в связи с тем, что создание и (или) обработка данных в ряде случаев требует несения финансовых и временных издержек, целесообразно проработать подход к защите законных интересов собственников цифровой платформы через механизм регулирования доступа к данным. Владельцы цифровой платформы либо иного информационного ресурса, на котором размещается пользовательская информация, установить различные (в том числе публичные, либо ограниченные и возмездные) режимы доступа к данным при соблюдении законных интересов пользователей по обеспечению доступности к предоставленной ими информации, а также принципа недискриминационного доступа пользователей к данным. Правила доступа к данным могут также содержать режимы использования данных самой цифровой платформой, включая предоставление доступа к данным третьим лицам для реализации основного

функционала цифровой платформы, либо для иных целей на безвозмездной, либо возмездной основе.

В случае установления публичного доступа к информации (доступного неограниченному кругу лиц без принятия правил, регулирующих доступ к данным, включая традиционные веб-сайты – классические сайты-визитки, общедоступные энциклопедии, новостные и информационные источники, и т.п.), размещаемой в сети Интернет, к законно размещенным данным на таких площадках должны применяться положения статьи 7 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» №149-ФЗ, а также статьи 8 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных». При этом обработка таких данных может осуществляться любыми лицами в любых целях, за исключением действующих законодательных ограничений.

Для сокращения рисков необдуманного размещения чувствительной информации в общем доступе в дополнение к положениям статьи 8 необходимо рассмотреть различные варианты дополнительной защиты прав пользователей при размещении информации в общем доступе без ограничений, включая возможность обязательного дополнительного информирования об особенностях такого размещения.

Приложение № 2

Согласно Концепции цифрового профиля, разработанной Минкомсвязи России и Банком России, а также проектом федерального закона, разработанного Минкомсвязи России в рамках национальной программы «Цифровая экономика Российской Федерации», предлагается создание инфраструктуры цифрового профиля. При этом предусматривается, что порядок получения сведений с использованием инфраструктуры цифрового профиля, а также случаи, когда такие сведения предоставляются за плату или бесплатно, будут определены Правительством Российской Федерации.

В связи с этим возможно:

а) определить случаи, когда доступ к инфраструктуре цифрового профиля не требует согласия физического или юридического лица;

б) предусмотреть возможность доступа коммерческих организаций к инфраструктуре цифрового профиля на постоянной основе (например, по подписке) в целях актуализации клиентских баз данных и минимизации рисков при заключении сделок;

в) разграничить основания для получения сведений с использованием инфраструктуры цифрового профиля на возмездной и безвозмездной основе;

г) определить технические требования к пропускной способности «Цифрового профиля» и существующих элементов инфраструктуры электронного правительства (СМЭВ, отдельные государственные информационные системы). Так, например, операторам связи для исполнения требований законодательства о проверке сведений об абонентах необходима пропускная способность отдельных ГИС (например, ГИС МВД) в объеме не менее, чем 5 запросов в секунду.

В части управления согласиями о предоставлении данных из Цифрового профиля (ЦП) следует зафиксировать, что ЦП управляет исключительно согласиями в отношении сведений, которые:

а) содержатся в государственных информационных системах (ГИС);

б) предоставляются через ЦП;

в) исчерпываются сведениями о юридических лицах, не находящимися в открытом (например, в ЕГРЮЛ) доступе.

Курьер Сервис Экспресс
Москва, тел.: +7 (495) 748-7-748 +7 (495) 995-7-995
www.cse.ru

GLOBAL DISTRIBUTION ALLIANCE
Service Partner

ЗАПОЛНЯЕТСЯ ИСПОЛНИТЕЛЕМ

495-0037622995

1. ОТПРАВКА

ФИО отправителя: **Степанова Виктория Владимировна**
Наим. Орг-ции: **ЦИФРОВАЯ ЭКОНОМИКА**
Код подразделения
Страна: **РОССИЯ** Город: **Москва г**
Область Район
Адрес: **г Москва, пер Конюшковский М., дом 2, офис 1,**
Тел. №: **7 (925) 400-22-76**

2. НАЗНАЧЕНИЕ

ФИО получателя: **Дроздову И.А**
Наим. Орг-ции: **Фонд "Сколково"**
Код подразделения
Страна: **РОССИЯ** Город: **Москва г**
Область Район
Адрес: **г Москва, тер Сколково инновационного центра, ул Луговая, дом 4,**
Тел. №: **84959560033**

3. ОПИСАНИЕ ВЛОЖИМОГО

Общее описание вложимого	Кол-во мест	Вес (кг)	Габариты (см х см х см)
Документы.	1	0.1	0 x 0 x 0
Всего:	1	0.1	Вес V (кг.) = 0

Стоимость для таможни / Валюта

Я подтверждаю, что информация на накладной является полной и точной.
С основными условиями пересылки я ознакомлен.

ФОРМА 2 НАКЛАДНАЯ **Подпись отправителя:**
ЦИФРОВАЯ ЭКОНОМИКА@tk.cse.ru - 18:24 13.03.2019

номер пакета

4. СТРАХОВАНИЕ ОТПРАВЛЕНИЯ
☐ Да / Yes ☒ Нет / No
Страховая сумма: **0 RUR**
Страховой взнос: **0**

5. ОТПРАВЛЕНИЕ С ОБЪЯВЛЕННОЙ ЦЕННОСТЬЮ
☐ Да / Yes ☒ Нет / No
Сумма объявленной ценности: **0 RUR**

номер заказа (документа основания): **495-0037622995**

6. СВЕДЕНИЯ ОБ ОПЛАТЕ
☐ ОТПРАВИТЕЛЕМ ☐ НАЛИЧНЫЕ
☐ ПОЛУЧАТЕЛЕМ ☒ ДОГОВОР
☒ ТРЕТЬИМ ЛИЦОМ ☐ ГАР. ПИСЬМО

код плательщика (номер договора): **6262-Д**

7. СРОЧНОСТЬ: **Сверхсрочная**
8. ИТОГО К ОПЛАТЕ: —

9. ПРИМЕЧАНИЕ
до дверей

10. ПРИЁМ ОТПРАВЛЕНИЯ
Дата: **14.03.2019** Время
Ф.И.О. Сотрудника Курьер-Сервис | Подпись

11. ИНФОРМАЦИЯ О ВРУЧЕНИИ ОТПРАВЛЕНИЯ:
Дата Время
Ф.И.О. получателя
Подпись получателя | Должность
Ф.И.О. Сотрудника Курьер-Сервис

12. ИНФОРМАЦИЯ ЗАКАЗЧИКА:
Ф.И.О. заказчика | Подпись заказчика

Экземпляр исполнителя

стр.1

Курьер Сервис Экспресс
Москва, тел.: +7 (495) 748-7-748 +7 (495) 995-7-995
www.cse.ru

GLOBAL DISTRIBUTION ALLIANCE
Service Partner

ЗАПОЛНЯЕТСЯ ОТПРАВИТЕЛЕМ

495-0037622995

1. ОТПРАВКА

ФИО отправителя: **Степанова Виктория Владимировна**
Наим. Орг-ции: **ЦИФРОВАЯ ЭКОНОМИКА**
Код подразделения
Страна: **РОССИЯ** Город: **Москва г**
Область Район
Адрес: **г Москва, пер Конюшковский М., дом 2, офис 1,**
Тел. №: **7 (925) 400-22-76**

2. НАЗНАЧЕНИЕ

ФИО получателя: **Дроздову И.А**
Наим. Орг-ции: **Фонд "Сколково"**
Код подразделения
Страна: **РОССИЯ** Город: **Москва г**
Область Район
Адрес: **г Москва, тер Сколково инновационного центра, ул Луговая, дом 4,**
Тел. №: **84959560033**

3. ОПИСАНИЕ ВЛОЖИМОГО

Общее описание вложимого	Кол-во мест	Вес (кг)	Габариты (см х см х см)
Документы.	1	0.1	0 x 0 x 0
Всего:	1	0.1	Вес V (кг.) = 0

Стоимость для таможни / Валюта

Я подтверждаю, что информация на накладной является полной и точной.
С основными условиями пересылки я ознакомлен.

ФОРМА 2 НАКЛАДНАЯ **Подпись отправителя:**
ЦИФРОВАЯ ЭКОНОМИКА@tk.cse.ru - 18:24 13.03.2019

номер пакета

4. СТРАХОВАНИЕ ОТПРАВЛЕНИЯ
☐ Да / Yes ☒ Нет / No
Страховая сумма: **0 RUR**
Страховой взнос: **0**

5. ОТПРАВЛЕНИЕ С ОБЪЯВЛЕННОЙ ЦЕННОСТЬЮ
☐ Да / Yes ☒ Нет / No
Сумма объявленной ценности: **0 RUR**

номер заказа (документа основания): **495-0037622995**

6. СВЕДЕНИЯ ОБ ОПЛАТЕ
☐ ОТПРАВИТЕЛЕМ ☐ НАЛИЧНЫЕ
☐ ПОЛУЧАТЕЛЕМ ☒ ДОГОВОР
☒ ТРЕТЬИМ ЛИЦОМ ☐ ГАР. ПИСЬМО

код плательщика (номер договора): **6262-Д**

7. СРОЧНОСТЬ: **Сверхсрочная**
8. ИТОГО К ОПЛАТЕ: —

9. ПРИМЕЧАНИЕ
до дверей

10. ПРИЁМ ОТПРАВЛЕНИЯ
Дата: **14.03.2019** Время
Ф.И.О. Сотрудника Курьер-Сервис | Подпись

11. ИНФОРМАЦИЯ О ВРУЧЕНИИ ОТПРАВЛЕНИЯ:
Дата Время
Ф.И.О. получателя
Подпись получателя | Должность
Ф.И.О. Сотрудника Курьер-Сервис

12. ИНФОРМАЦИЯ ЗАКАЗЧИКА:
Ф.И.О. заказчика | Подпись заказчика

Экземпляр отправителя

стр.2

Курьер Сервис Экспресс
Москва, тел.: +7 (495) 748-7-748 +7 (495) 995-7-995
www.cse.ru

GLOBAL DISTRIBUTION ALLIANCE
Service Partner

ЗАПОЛНЯЕТСЯ ИСПОЛНИТЕЛЕМ

495-0037622995

1. ОТПРАВКА

ФИО отправителя: **Степанова Виктория Владимировна**
Наим. Орг-ции: **ЦИФРОВАЯ ЭКОНОМИКА**
Код подразделения
Страна: **РОССИЯ** Город: **Москва г**
Область Район
Адрес: **г Москва, пер Конюшковский М., дом 2, офис 1,**
Тел. №: **7 (925) 400-22-76**

2. НАЗНАЧЕНИЕ

ФИО получателя: **Дроздову И.А**
Наим. Орг-ции: **Фонд "Сколково"**
Код подразделения
Страна: **РОССИЯ** Город: **Москва г**
Область Район
Адрес: **г Москва, тер Сколково инновационного центра, ул Луговая, дом 4,**
Тел. №: **84959560033**

3. ОПИСАНИЕ ВЛОЖИМОГО

Общее описание вложимого	Кол-во мест	Вес (кг)	Габариты (см x см x см)
Документы.	1	0.1	0 x 0 x 0
Всего:	1	0.1	Вес V (кг.) = 0

Стоимость для таможни / Валюта

Я подтверждаю, что информация на накладной является полной и точной.
С основными условиями пересылки я ознакомлен.

ФОРМА 2 НАКЛАДНАЯ **Подпись отправителя:**
ЦИФРОВАЯ ЭКОНОМИКА@lk.cse.ru - 18:24 13.03.2019

4. СТРАХОВАНИЕ ОТПРАВЛЕНИЯ
☐ Да / Yes ☒ Нет / No
Страховая сумма: **0 RUR**
Страховой взнос: **0**

5. ОТПРАВЛЕНИЕ С ОБЪЯВЛЕННОЙ ЦЕННОСТЬЮ
☐ Да / Yes ☒ Нет / No
Сумма объявленной ценности: **0 RUR**

7. СРОЧНОСТЬ
Сверхсрочная

9. ПРИМЕЧАНИЕ
до дверей

10. ПРИЁМ ОТПРАВЛЕНИЯ
Дата: **14.03.2019** Время
Ф.И.О. Сотрудника Курьер-Сервис Подпись

11. ИНФОРМАЦИЯ О ВРУЧЕНИИ ОТПРАВЛЕНИЯ:
Дата Время
Ф.И.О. получателя
Подпись получателя Должность
Ф.И.О. Сотрудника Курьер-Сервис

12. ИНФОРМАЦИЯ ЗАКАЗЧИКА:
Ф.И.О. заказчика Подпись заказчика

номер пакета
номер заказа (документа основания): **495-0037622995**

6. СВЕДЕНИЯ ОБ ОПЛАТЕ
☐ ОТПРАВИТЕЛЕМ ☐ НАЛИЧНЫЕ
☐ ПОЛУЧАТЕЛЕМ ☒ ДОГОВОР
☒ ТРЕТЬИМ ЛИЦОМ ☐ ГАР. ПИСЬМО
код плательщика (номер договора): **6262-Д**

8. ИТОГО К ОПЛАТЕ
—

Экземпляр исполнителя

стр.3

Курьер Сервис Экспресс
Москва, тел.: +7 (495) 748-7-748 +7 (495) 995-7-995
www.cse.ru

GLOBAL DISTRIBUTION ALLIANCE
Service Partner

ЗАПОЛНЯЕТСЯ ОТПРАВИТЕЛЕМ

495-0037622995

1. ОТПРАВКА

ФИО отправителя: **Степанова Виктория Владимировна**
Наим. Орг-ции: **ЦИФРОВАЯ ЭКОНОМИКА**
Код подразделения
Страна: **РОССИЯ** Город: **Москва г**
Область Район
Адрес: **г Москва, пер Конюшковский М., дом 2, офис 1,**
Тел. №: **7 (925) 400-22-76**

2. НАЗНАЧЕНИЕ

ФИО получателя: **Дроздову И.А**
Наим. Орг-ции: **Фонд "Сколково"**
Код подразделения
Страна: **РОССИЯ** Город: **Москва г**
Область Район
Адрес: **г Москва, тер Сколково инновационного центра, ул Луговая, дом 4,**
Тел. №: **84959560033**

3. ОПИСАНИЕ ВЛОЖИМОГО

Общее описание вложимого	Кол-во мест	Вес (кг)	Габариты (см x см x см)
Документы.	1	0.1	0 x 0 x 0
Всего:	1	0.1	Вес V (кг.) = 0

Стоимость для таможни / Валюта

Я подтверждаю, что информация на накладной является полной и точной.
С основными условиями пересылки я ознакомлен.

ФОРМА 2 НАКЛАДНАЯ **Подпись отправителя:**
ЦИФРОВАЯ ЭКОНОМИКА@lk.cse.ru - 18:24 13.03.2019

4. СТРАХОВАНИЕ ОТПРАВЛЕНИЯ
☐ Да / Yes ☒ Нет / No
Страховая сумма: **0 RUR**
Страховой взнос: **0**

5. ОТПРАВЛЕНИЕ С ОБЪЯВЛЕННОЙ ЦЕННОСТЬЮ
☐ Да / Yes ☒ Нет / No
Сумма объявленной ценности: **0 RUR**

7. СРОЧНОСТЬ
Сверхсрочная

9. ПРИМЕЧАНИЕ
до дверей

10. ПРИЁМ ОТПРАВЛЕНИЯ
Дата: **14.03.2019** Время
Ф.И.О. Сотрудника Курьер-Сервис Подпись

11. ИНФОРМАЦИЯ О ВРУЧЕНИИ ОТПРАВЛЕНИЯ:
Дата Время
Ф.И.О. получателя
Подпись получателя Должность
Ф.И.О. Сотрудника Курьер-Сервис

12. ИНФОРМАЦИЯ ЗАКАЗЧИКА:
Ф.И.О. заказчика Подпись заказчика

номер пакета
номер заказа (документа основания): **495-0037622995**

6. СВЕДЕНИЯ ОБ ОПЛАТЕ
☐ ОТПРАВИТЕЛЕМ ☐ НАЛИЧНЫЕ
☐ ПОЛУЧАТЕЛЕМ ☒ ДОГОВОР
☒ ТРЕТЬИМ ЛИЦОМ ☐ ГАР. ПИСЬМО
код плательщика (номер договора): **6262-Д**

8. ИТОГО К ОПЛАТЕ
—

Экземпляр отправителя

стр.4