ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ
СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»
(РАНХиГС)

Южаков В.Н., Талапина Э.В., Черешнева И.А.

ПРАВОВЫЕ РИСКИ ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИИ РАСПРЕДЕЛЕННОГО РЕЕСТРА В ГОСУДАРСТВЕННОМ УПРАВЛЕНИИ

Москва - 2020

Electronic copy available at: https://ssrn.com/abstract=3888108

Аннотация. В рамках настоящей работы проанализированы фактические отношения, связанные с применением технологии распределенного реестра (ТРР) в государственном управлении, и потенциал их правового регулирования. Были выявлены и систематизированы правовые риски использования ТРР в государственном управлении, предложена классификация правовых рисков при использовании ТРР, прежде всего в форме блокчейна, в государственном управлении. Сформулированы предложения по преодолению правовых рисков при использовании ТРР в государственном управлении.

Южаков В.Н., доктор философских наук, профессор, главный научный сотрудник, директор Центра технологий государственного управления ИПЭИ Российской академии народного хозяйства и государственной службы при Президенте РФ

Талапина Э.В., доктор юридических наук, ведущий научный сотрудник Центра технологий государственного управления ИПЭИ Российской академии народного хозяйства и государственной службы при Президенте РФ

Черешнева И.А., младший научный сотрудник Центра технологий государственного управления ИПЭИ Российской академии народного хозяйства и государственной службы при Президенте РФ

Данный препринт подготовлен на основе материалов научно-исследовательской работы, выполненной в соответствии с Государственным заданием РАНХиГС при Президенте Российской Федерации на 2020 год.

Electronic copy available at: https://ssrn.com/abstract=3888108

СОДЕРЖАНИЕ

Electronic copy available at: https://ssrn.com/abstract=3888108

ВВЕДЕНИЕ

Имеющийся зарубежный и российский экспериментальный опыт демонстрируют несомненные преимущества технологии распределенного реестра и блокчейна, как наиболее распространенного ее вида, для преодоления таких проблем в государственном управлении как коррупция, длительность процедур, субъективный фактор.

Но зачастую выводы о скорейшем внедрении ТРР (блокчейна) базируются на завышенных ожиданиях, не учитывающих риски, в том числе правовые. Проблема оценки таких рисков является актуальной и новой, требующей скорейшего разрешения.

Основной целью настоящего исследования является выявление и систематизация правовых рисков использования ТРР в государственном управлении, формулирование предложений по их преодолению правовыми средствами.

Источником таких рисков во многом является сама природа государственной власти, которая является центростремительной и выстроенной вертикально. Она контрастирует с децентрализованной природой блокчейна, что представляет основную проблему для социальных наук. Совмещение разновекторных феноменов – власти и ТРР – порождает многочисленные риски, в том числе правовые.

Electronic copy available at: https://ssrn.com/abstract=3888108

1 Общие подходы к определению правовых рисков в государственном управлении при применении ТРР

Если в науке государственного управления основным риском от широкого внедрения блокчейна называется снижение значения государства и государственных органов как таковых, то в праве данное опасение выражается в потенциальном снижении значения официального нормативного правового регулирования, так как блокчейн в значительной мере регулируется кодом.

Серьезность риска утраты значения правового регулирования перед лицом блокчейна усиливает необходимость детальных исследований и других правовых рисков. Однако именно юридических исследований в области цифровизации государственного управления в целом, и применения ТРР (блокчейн), особенно не хватает, о чем свидетельствуют зарубежные обзоры в авторитетных научных изданиях [1].

1.1 Правовые риски: понятие и виды

Использование цифровых технологий, эффекты которых недостаточно изучены и просчитаны, ведет к определенным рискам – техническим, организационным, экономическим. Это можно отнести к любой сфере применения, в том числе к государственному управлению. Проблема рисков цифровизации уже привлекла активное исследовательское внимание. Далеко немаловажное значение имеют правовые риски применения цифровых технологий, поскольку государственное управление в правовом государстве осуществляется исключительно на основе права. Но само право недостаточно определилось со своим отношением к технологиям.

Так, «экстремистская» позиция технолибертарианцев и криптоанархистов характеризуется поощрением использования новых ИКТ для освобождения от государства вообще как устаревшего «хранилища» власти. Более сдержанная позиция характеризуется принятием взвешенного решения на основании изучения рисков и преимуществ внедрения цифровых технологий в государственное управление. В этой связи необходимо изучение правовых рисков, дальнейший учет которых предполагается в правоприменительной деятельности.

Можно ли сказать, что правовое регулирование никогда не учитывало риски? Скорее напротив – устоявшееся регулирование как раз и означает учет всех имеющихся рисков (на стадии формулирования норм как правил поведения общего характера). В чем же тогда особенность цифрового этапа? Прежде всего, в скорости – развитие технологий зачастую не позволяет размеренно просчитывать риски, что требует новых правовых техник для создания классических норм. Либо – отхода от общих норм и дробления правил поведения по группам, категориям и пр., что ведет право по пути персонализации;

Electronic copy available at: https://ssrn.com/abstract=3888108

последнее можно назвать революцией для права, поскольку универсальность права остается только в технике, механизме, а принципу равенства как основе правового государства наносится удар. Общие подходы к определению правового риска определены в отечественной литературе и международных документах, но при этом далеко не всегда совпадают.

Ю.А. Тихомиров отмечает, что правовые риски выражаются в:

а) возможности прямого или косвенного нарушения правовых норм;

б) отчуждении граждан от законодательства ввиду низкой правовой культуры и юридической компетентности;

в) ошибках при определении статусов субъектов права, выборе правовых методов регулирования;

г) угрозе увеличения объема юридических коллизий;

д) провоцировании конфликта интересов;

е) возникновении разрыва системно-правовых связей в правовой системе;

ж) нарушении корреляции между способом правового регулирования и мерой отражения экономических, социальных и политических процессов [2].

Существующие в литературе классификации рисков условно можно разделить на две группы:

1) универсальные классификации, применяемые к таким рискам, которые возникают в любой сфере общественных отношений;

2) правовые классификации, которые прямо или косвенно связаны с правом в самом широком его понимании [3].

Анализ суждений различных авторов приводит к выводу, что каждый выделяет признаки рисков, характерные для конкретной области отношений; общего понимания правового риска в проведенном обзоре литературы не встретилось. Тем не менее, изучение литературы весьма полезно для уяснения разнообразных подходов к систематизации правовых рисков, с тем чтобы на базе общих позиций выделить специфику рисков в области государственного управления. Подчеркнем, что внятной теории правовых рисков, которая была бы системно воспринята в правотворческой и правоприменительной практике, в России так и не сложилось. Тем не менее, в целях настоящего исследования определим правовой риск как возможность наступления неблагоприятных последствий правового характера. В целом такие негативные последствия могут выражаться в негативном воздействии на: во-первых, систему правового регулирования в целом, во-вторых, регулирование конкретного объекта отношений, в-третьих, правовую устойчивость системы государственного управления, в-

Electronic copy available at: https://ssrn.com/abstract=3888108

четвертых, реализацию управленческих решений, в-пятых, реализацию прав человека, включая право на судебное обжалование. Такая систематизация правовых рисков в равной мере распространяется на область государственного управления, в том числе при применении цифровых технологий, о чем пойдет речь ниже.

1.2 Классификация правовых рисков при использовании блокчейна в государственном управлении

Одной из задач настоящего исследования является выявление и классификация правовых рисков при использовании блокчейна в государственном управлении. Представляется, что решить ее можно, во-первых, опираясь на изученные выше общие подходы к систематизации правовых рисков, а во-вторых, ориентируясь на конкретный кейс реализации государственной функции. Данный кейс будет сконструирован на основе авторского понимания государственного управления и государственной функции, предложенного в предыдущих научных работах [4]. В своих исследованиях мы показали, что использование блокчейна наиболее перспективно в формализованной, исполнительской деятельности, в частности, при оказании государственных услуг. Согласно предложенному нами проекту ФЗ об обеспечении качества государственного управления [4], государственные услуги оказываются в целях обеспечения и непосредственной реализации прав и законных интересов граждан и организаций. При оказании государственных услуг решается задача качественной и эффективной реализации соответствующих прав и законных интересов граждан и организаций. Поэтому в дальнейшем (во второй части работы) мы сконцентрируемся на детальном изучении правовых рисков, нарушающих права граждан при использовании технологии блокчейн, обращаясь к кейсу оказания государственной услуги на примере государственной регистрации недвижимого имущества. Избранный для иллюстрации пример не случаен, поскольку последний выступил в качестве экспериментальной площадки для внедрения блокчейна в российской управленческой практике.

Несомненно, блокчейн обладает рядом преимуществ распределенного реестра: эффективностью, экономичностью, невозможностью отмены транзакции, прозрачностью, контролируемостью и устойчивостью к цензуре. Тем не менее, предложение децентрализовать государственные услуги через открытый публичный блокчейн может повлечь за собой целый ряд неизвестных, которые могут перевесить преимущества данной технологии для государственного управления.

Одной из ключевых является проблема безопасности и техническая слабость современного блокчейна. В целом преимущества открытых (публичных) блокчейнов для

Electronic copy available at: https://ssrn.com/abstract=3888108

сферы государственного управления вообще и государственных услуг, в частности, могут «перечеркиваться» рядом следующих рисков:

1) риск недобросовестности, проблема масштабируемости технологии, тенденции к централизации и потенциальной зависимости от майнинговых корпораций, которые могут достаточно быстро осуществлять сделки M&A на фондовом рынке, приобретая значительную власть в глобальном масштабе. В настоящее время биткойн преимущественно управляется все более централизованными майнинговыми фермами, которые, например, осуществляют секретные и колоссальные майнинговые операции в Китае или участвуют в торгах на фондовой бирже в Австралии, что ведет к возможным рискам сговора или картелизации [5]. Несмотря на одноранговый характер блокчейна, возможно ли, что в перспективе данная технология будет способствовать созданию все более концентрированных структур (богатство, власть, знания), как это произошло с биткоином? Так, согласно сведениям Bloomberg на декабрь 2017 года около 40 процентов биткоинов принадлежит примерно 1000 пользователям [6]. Исследование компании Diar выявило, что приблизительно $100 млрд. в биткоинах содержатся на менее чем 1% криптовалютных кошельков [7];

2) доминирование рыночной логики над принципиально значимыми государственными услугами и правами граждан, которые должны быть защищены от спекуляций любого рода;

3) возможное отсутствие непрерывности обслуживания и/или сохранения данных в среднесрочной перспективе без разграничения ответственности, обусловленное динамикой рынка и /или серьезными техническими недостатками;

4) на глобальном уровне увеличение влияния технократической элиты с растущими надзорными полномочиями над стратегическими услугами в отсутствии необходимой формальной легитимности.

Таким образом, мы должны сделать вывод, что сфера государственных услуг недостаточно хорошо подходят для использования децентрализованных блокчейнов типа биткоин (или открытого типа блокчейна). Государственные архивы требуют высокой производительности и высокой степени надежности, доступности и предсказуемости, поскольку они не терпят никаких перерывов в обслуживании или сбоев: недостаток в управлении или в реализации сети поставит под угрозу безопасность и права миллионов граждан. Кроме того, при оказании государственных услуг строго необходимо придерживаться формального и транспарентного процесса легитимации для того, чтобы избежать массового проявления частной власти в сфере государственного управления. Еще раз подчеркнем, что большинство описанных рисков проявляет себя по отношению к

Electronic copy available at: https://ssrn.com/abstract=3888108

открытому (публичному) блокчейну, предполагающему наибольшую степень децентрализации. Исследователи отмечают большую вероятность того, что в силу политических и социальных рисков государство не согласится на массовое использование публичного блокчейна в государственно-управленческих целях. Однако закрытый (эксклюзивный) блокчейн тоже влечет риски, для раскрытия которых полезно рассмотреть вопрос о рисках использования информационных систем в государственном управлении, поскольку они имеют много общего с закрытым блокчейном. С. Е. Чаннов выделяет следующие виды угроз, связанных с использованием информационных систем в государственном управлении (государственные информационные системы, далее – ГИС):

Во-первых, поскольку в ГИС содержатся большие объемы персональных данных, а также сведения об организациях (часто квалифицируемые как конфиденциальные), постольку утечки такой информации становятся все более опасными. Одновременно с этим возникает угроза не только использования сведений, содержащихся в ГИС, в противоправных целях, но и непосредственная угроза правам личности на частную жизнь со стороны государства, которое, сосредотачивая персональные данные о гражданах, может получать практически полную информацию о них.

Во-вторых, накопление больших объемов информации в ГИС становится основанием для использования в государственном управлении технологии больших данных (Big Data) [8], а с этим связаны принципиально новые угрозы, особенно в области защиты персональных данных граждан и сведений об организациях. Согласимся с позицией А.И. Савельева, согласно которой «… будущее – за «широким» подходом к определению персональных данных, по крайней мере, пока на смену законодательству о персональных данных не придет принципиально новое регулирование, ориентированное не столько на защиту «анкетных данных» физических лиц, сколько на защиту данных об их поведении в цифровом мире, на основании которых в перспективе будет приниматься множество юридически значимых решений в отношении таких лиц» [9].

В-третьих, уникальность информационных систем, используемых в государственном управлении, в том, что они становятся источником первичных данных, не существующих более нигде. Так, ведение Единого государственного реестра недвижимости, который, фактически, представляет собой государственную информационную систему, осуществляется исключительно в электронном виде (из этого круга могут «выпадать» реестровые дела). Сказанное порождает следующие риски:

1) сложности восстановления информации (если информация, существующая исключительно в электронном виде, была искажена (утрачено), умышленно или случайно, ее может быть нелегко восстановить в первоначальном варианте);

Electronic copy available at: https://ssrn.com/abstract=3888108

2) цифровое неравенство (когда граждане по разным причинам не могут вносить информацию в электронном виде в систему и, соответственно, реализовать свои права) [8].

Специальное исследование правовых рисков блокчейна в государственном управлении нуждается в их более стройной классификации. Изучение подходов к систематизации правовых рисков общего характера, представленных в научной литературе, анализ выявленных учеными рисков в различных сферах позволяет нам классифицировать (предварительно) правовые риски от использования блокчейн в госуправлении следующим образом.

Первую группу рисков образуют те, которые связаны с процессами правоустановления (назовем их - общие правовые риски применительно к блокчейну в госуправлении). Под общими правовыми рисками мы понимаем возможные неясности (неопределенность), противоречия и пробелы законодательства в области государственного управления в отношении технологии блокчейн. Основным источником этих рисков является само право. Это:

1) Риск попадания в «неправовое поле» ввиду общей неурегулированности блокчейна как прорывной технологии. На настоящий момент российское государство не имеет однозначной законодательно выраженной позиции по отношению к данной технологии, она не легализована и одновременно не запрещена. В таких условиях правовые риски очевидны – использование блокчейна трактуется как предпринимательский риск, что, конечно, не может устроить государство в случае его применения в государственном управлении. Учитывая, что в административном праве действует правило «разрешено то, что разрешено», это означает формальную невозможность использования блокчейн в госуправлении в соответствии с действующим законодательством, либо его внеправовое рисковое использование.

2) Риск снижения государственного регулирования блокчейна или даже полного отказа от государственного (нормативного) регулирования. Как следствие – риск утраты значения государственных органов. Всегда считалось, что государство должно активно регулировать общественные отношения, даже в рыночной экономике – устанавливать правила, контролировать. При расчете предпринимательских рисков участие государства (регистрация, обязательные требования) являлось фактором, снижающим их. Но революционность технологии блокчейн с ее децентрализацией может означать (в крайнем ее варианте) отказ от государственного регулирования. Или (в более мягком варианте) – значительное его снижение. Как полагают отечественные эксперты, «возможные риски ослабления регулятивных возможностей государства требуют более тщательной оценки

Electronic copy available at: https://ssrn.com/abstract=3888108

эффектов от использования криптовалют и сопоставления ее результатов с потенциальными масштабами реформирования государственной системы регулирования экономики» [10]. То есть правовое регулирование уступает место техническому, не зависящему от государства. Нужно признать, технические специалисты предлагают любопытные варианты технического регулирования. Для устранения некоторых минусов блокчейна, в том числе эксклюзивного, предлагается перейти к протоколу коллективной подписи, позволяющему распределить ответственность за записи транзакций. При этом ответственность за ошибки (закладки) в программном коде, реализующем работу системы (смарт-контракты) должен нести тот, кто написал программный код. В случае нарушения работы этот субъект должен вмешаться в работу системы и скорректировать её, а также нести ответственность за материальные потери клиентов [11]. Такой подход выражает стремление обойтись собственно техническим регулированием, не прибегая к правовым регуляторам. Это преувеличение технических возможностей в регулировании применения цифровых технологий в ущерб традиционному нормативному представляет собой правовой риск. Причем здесь речь не идет о привычных рисках правовых коллизий внутри самого права [12], это новый риск, рожденный непосредственно использованием технологий.

3) Риск смешения публичного и частного начала в государственном управлении. Данный риск связан с режимом данных, используемых для организации и функционирования блокчейна, данных, поступающих в систему. Очевидно, что функционирование блокчейна будет обеспечивать достаточное количество частных субъектов (начиная с составления алгоритма и заканчивая техническим сопровождением); помимо этого, частные субъекты могут быть привлечены непосредственно к исполнению государственной функции (например, банки). Поэтому должна быть обеспечена сохранность и безопасность данных, а также интероперабельность данных, которыми обладают участники системы распределенного реестра. Совершенно неочевидно, как государство выстроит отношения по поводу доступа к таким данным, и как само будет предоставлять доступ к данным из государственных информационных систем. Подобное смешение публичного и частного способно привести к игнорированию публично-правовой сути государственного управления, коммерциализации отношений государства и частных партнеров, что, в конечном счете, отразится на стоимости услуг и безопасности данных граждан.

4) Риск применения частного права к публично-правовым отношениям. Он связан с опережающим развитием частного права вообще, и в отношении технологии блокчейн в частности. Частное право практически всегда более разработано и актуализировано

Electronic copy available at: https://ssrn.com/abstract=3888108

сообразно технологическому развитию, нежели публичное, что справедливо и в отношении цифровых технологий. Биткоин, к примеру, регулируется в раках частного права, более лояльного к рискам, – ведь хотя биткоин и используется вместо денег, он все-таки не признан денежным средством. Допущение частным правом предпринимательских рисков, свобода договорных отношений создают определенную маневренность правоприменения, гибкость позиций субъектов. Государство со времен нового публичного менеджмента стремится овладеть техниками подобной гибкости. При этом нормы публичного права зачастую остаются более консервативными, традиционными. В этих условиях у государства возникает соблазн применить нормы частного права к государственно-управленческим отношениям. Соблазн, перерастающий в риск, способный нарушить баланс публичного и частного права, нивелировать публично-правовую специфику отношений государственного управления.

Например, одной из многообещающих областей применения блокчейна можно считать использование механизма смарт-контакта в процессе совершения сделок. Смарт-контакт (умный контакт) представляет собой способ совершения операция, которая осуществляется в автоматическом режиме, при наличии определенных условий. Так, одним из перспективных методов использования блокчейна в процессе совершения сделок является «умный» контракт, или смарт-контракт – это автоматический способ совершения операции при наступлении определенных условий. Автоматизация транзакции или отдельных ее элементов позволяет снизить издержки на привлечение третьей стороны для содействия в исполнении сторонами своих обязательств или проверки соответствия исполнения условиям договора. Однако в настоящее время можно говорить о том, что смарт-контракты все-таки являются средством автоматического подтверждения выполнения договоренностей сторон.

Фактически, смарт-контракт можно рассматривать в качестве алгоритма, согласованного сторонами, который «запускается» при наступлении определенного события. Возникает вопрос: является ли такой код договором по смыслу гражданского законодательства? Существует позиция, согласно которой «умный» контракт укладывается в понятие договора как соглашения двух или нескольких лиц об установлении, изменении или прекращении гражданских прав и обязанностей. С гражданско-правовой точки зрения вполне можно говорить о том, что лицо, действуя своей волей и в своих интересах, присоединяется к условиям «умного» контракта посредством совершения определенных действий. После заключения такого контракта стороны пребывают в состоянии связанности результатом своего волеизъявления, сделанного в момент заключения договора, а именно действием программного кода.

Electronic copy available at: https://ssrn.com/abstract=3888108

Тем самым, для признания программного кода самостоятельной формой договора необходимо наличие возможности дешифровки последнего в простой текст для определения прав и обязанностей сторон смарт-контракта и других его условий. Укажем, что вся проблематика смарт-контракта сосредоточена в частном праве, и государству при использовании блокчейна придется принимать ее в расчет.

Кроме того, принятый Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» (вступает в силу с 1 января 2021 года) закрепил понятие цифровой валюты. Под организацией обращения в Российской Федерации цифровой валюты понимается деятельность по оказанию услуг, направленных на обеспечение совершения гражданско-правовых сделок и (или) операций, влекущих за собой переход цифровой валюты от одного обладателя к другому, с использованием объектов российской информационной инфраструктуры. При этом в России запрещено распространение информации о предложении и (или) приеме цифровой валюты в качестве встречного предоставления за передаваемые ими (им) товары, выполняемые ими (им) работы, оказываемые ими (им) услуги или иного способа, позволяющего предполагать оплату цифровой валютой товаров (работ, услуг). Таким образом, запрещено расплачиваться криптовалютой.

Вторую группу рисков образуют те, что связаны с процессами правоприменения (специальные риски, возникающие непосредственно в связи с использованием блокчейна в госуправлении). Под специальными рисками мы понимаем создание и реализацию неоднозначных правовых режимов и правовых статусов в отношении объектов и субъектов государственного управления, а также девиантное поведение. Это:

1) Риск нарушения компетенции государственных органов и полномочий негосударственных субъектов (компетенционный риск). То, что орган власти действует в рамках отведенной ему компетенции – постулат административного права. Это значит, что полномочия органов государственной власти как участников системы блокчейна должны быть сформулированы в общем порядке в тех актах, которые определяют их компетенцию. Если этого не будет сделано – орган власти своими действиями попадает в «серое поле», возможны дефекты компетенции, конфликты компетенций и пр. Отдельные риски возникают и в ситуациях, требующих принятия совместного решения нескольких органов, – все участвующие в системе органы должны быть предварительно введены в качестве участников в систему блокчейна. В данном случае техническим регламентом блокчейна регулировать недостаточно; для того чтобы орган власти был компетентен, необходимо юридическое основание. Кроме того, субъектами государственного

Electronic copy available at: https://ssrn.com/abstract=3888108

управления могут выступать не только органы исполнительной власти. К исполнению государственной функции могут привлекаться разного рода организации, в том числе частные (например, банки). Если нет юридических оснований для такого участия (делегирования полномочий, административного договора), возникает риск нарушения их полномочий.

2) Риск нарушений фундаментальных прав человека. Основное место в ряду таких фундаментальных прав занимает право на защиту персональных данных. Обработка персональных данных в рамках блокчейн должна вестись с соблюдением всех предписанных нормативов. В то же время, могут возникать трудности с определением обработчика данных, на которого законодательство накладывает соответствующую ответственность. Кроме того, в такой обработке могут участвовать частные участники блокчейна при осуществлении государственной функции, на которых эти обязательства распространяются в равной мере. Защита персональных данных предполагает и реализацию права на забвение, которое имеет некоторые особенности в блокчейне.

Кроме того, в любых административных отношениях исключительную важность обретает право на судебное обжалование решений органов власти. В случае реализации государственной функции посредством блокчейна возникают сложности с обнаружением надлежащего ответчика, компетентного суда, что ставит под вопрос саму возможность судебной защиты.

Риск непризнания юридической значимости транзакций (сделок) и документов, сгенерированных в результате действий на базе блокчейна. Прежде всего, существует техническое несоответствие электронного и бумажного документа, поскольку не всегда электронный документ содержит все те реквизиты, что и бумажный. Далее, юридическая значимость электронного документа (и даже его бумажной копии) должна признаваться всеми – и в государственном, и в частном секторе. Обеспечение такой юридической силы возможно посредством тотальной ревизии законодательства, по-прежнему ориентированного на бумажные документы. Более того, на практике – и органы власти, и сами граждане – зачастую предпочитают именно бумажные документы. Если такая ориентация правосознания не будет переломлена, внедрение блокчейна может оказаться просто бессмысленным.

Именно специальные риски являются наиболее показательными с точки зрения основной, конституционной обязанности государства и его органов – обеспечения и соблюдения прав граждан. Они подробно изучены и описаны ниже.

Electronic copy available at: https://ssrn.com/abstract=3888108

2 Результаты анализа прав, обязанностей и ответственности участников блокчейна в государственном управлении

Государственное управление осуществляется на основе и в рамках закона; соответственно, правовой статус субъектов государственного управления нуждается в детальной регламентации. Если в традиционной деятельности иерархия таких правовых актов уже сложилась, то цифровое государственное управление в силу использования новых технологий, влияющих и на порядок осуществления государственных функций, и на компетенцию государственных органов, влечет необходимость, как минимум, уточнения статуса органов государственной власти и порядка их взаимодействия. Применение блокчейна в качестве технологии государственного управления означает, помимо этого, четкую регламентацию прав, обязанностей и ответственности всех участников этого блокчейна, вне зависимости от их принадлежности к государственному или частному сектору.

Экспериментирование с блокчейн-технологиями привело к серии небольших проектов, в рамках которых были объединены усилия государства и бизнеса. Земельные реестры, аутентификация дипломов о высшем образовании, цифровые удостоверения личности и медицинская документация являются наиболее распространенными примерами использования [13]. Так, город Цуг (Швейцария) запустил государственную идентификацию на блокчейне Ethereum, именуемую uPort. Цель проекта – обеспечить надежную и самодостаточную идентификацию на основе блокчейна для аутентификации пользователей в контексте оказания электронных государственных услуг и обмена персональными данными с третьими лицами [14].

Там же, в Швейцарии функционирует проект Cardossier Association, который представляет собой основанную на блокчейне многостороннюю платформу, соединяющую крупных частных и государственных игроков, компаний-разработчиков программного обеспечения и частных автовладельцев в единую автомобильную экосистему. При этом данный консорциум стремится создать рынок данных, обеспечивающий стимулы, прозрачность и справедливый механизм обмена различными видами информационных продуктов. Идея создания проекта «Cardossier» была задумана Цюрихским университетом совместно с AdNovum Informatik AG – компанией по разработке программного обеспечения в целях изучения технического и производственного потенциала технологии блокчейн. Впоследствии к консорциуму присоединились ключевые игроки автомобильной индустрии: AMAG – крупнейший швейцарский автоимпортер и ритейлер, AXA Winterthur – крупнейший швейцарский автостраховщик, Mobility – крупнейший каршеринг в Швейцарии, а также органы,

Electronic copy available at: https://ssrn.com/abstract=3888108

осуществляющие государственную регистрацию транспортных средств, кантона Аргау и Университет прикладных наук в Люцерне, предоставив свой опыт в области защиты данных [15].

Проект «Cardossier» направлен на улучшение швейцарской автомобильной экосистемы посредством хранения данных об использовании автомобилей в системе блокчейн. Существует три основных направления совершенствования [16]:

1) новые предложения продуктов, например, документально подтвержденные автомобильные истории, которые могут потенциально повысить прозрачность рынка подержанных автомобилей и тем самым повысить ценность автомобилей на рынке подержанных автомобилей;

2) оцифровка процессов между участниками экосистемы автомобилей может повысить их производственную эффективность;

3) основанные на данных «Cardossier» в большей степени индивидуализированные продукты и услуги (например, новые страховые продукты или пиринговое автокредитование).

Блокчейн-консорциумы стремятся улучшить совместное образование стоимости на основе совместного использования распределенной платформы. Подобного рода объединения осуществляют свою деятельность в рамках правового поля, при этом государственные органы и учреждения выступают полноправными партнерами-участниками таких отношений, поскольку они играют важную роль в межорганизационных процессах, выступая в качестве поставщика данных, источника доверия, гаранта качества данных, пользователя данных и стимула для создания общественных благ [15]. Рассмотрим блокчейн-консорциум подробнее, уделив особое внимание роли государственных органов в данном взаимодействии.

1) Государственный орган как участник межорганизационных процессов.

В широко распространенных областях с высокой стоимостью и риском, таких как землевладение или использование автомобилей, роль правительств особенно велика. Они не только осуществляют надзор за другими участниками, но и сами принимают участие в наиболее важных сделках, например, в сделках по продаже недвижимости или удостоверению пригодности автомобилей к эксплуатации. В этой роли они в первую очередь заинтересованы в эффективных и действенных (то есть цифровых) процессах. Технология блокчейн облегчает координацию межорганизационных процессов, при этом отсутствует необходимость в наличии сильного центрального частного актора, а государственные органы не выходят за границы своих традиционных зон ответственности.

Electronic copy available at: https://ssrn.com/abstract=3888108

Кроме того, пример Cardossier показывает трансформирующую силу совместно используемых распределенных платформ (поддерживаемых технологиями блокчейн) для государственных органов.

Так, органы, осуществляющие государственную регистрацию транспортных средств, могут перейти от непосредственной проверки автомобилей к цифровой проверке их пригодности для эксплуатации. Поскольку проведение непосредственного осмотра автомобилей государственными органами больше не требуется, постольку данная функция может быть передана частным автосервисам (а также производителям автомобилей для поставки программного обеспечения).

Таким образом, это не просто трансформация государственного органа «извне во внутрь», но и «изнутри во вне», происходящая в тесном сотрудничестве с частными и государственными партнерами, в целях совместного видоизменения экосистемы.

2) Государственный орган как поставщик данных.

Реестры выступают основной сферой применения технологии блокчейн ввиду того, что постоянные и неизменные записи и транзакции лежат в основе любого реестра. Существующие сегодня реестры, например, кадастровые обладают высокой ценностью, поскольку являются сосредоточением достоверной информации. При наличии высококачественного реестра нет никакого смысла в том, чтобы, по сути, дублировать уже затраченные усилия, однако целесообразно «завернуть существующий реестр в обертку блокчейна», предоставив распределенный доступ, и возможность сбора дополнительных данных, как это сделали в Швейцарии в рамках проекта «Cardossier» [15].

3) Государственный орган как источник доверия.

В данном контексте речь идет об институциональном доверии, которое переносится на всю платформу целиком, поскольку если в платформе не участвуют вызывающие доверие институты, то ее трудно будет запустить. Аналогичным образом компании с большей вероятностью присоединятся к платформе, если государственные органы возьмут на себя обязательства по этому поводу. Для частных компаний участие соответствующих государственных учреждений является сигналом их надежности и потенциальной долгосрочности проекта.

4) Государственный орган как гарант качества данных.

Качество данных (пригодность данных для практического использования конкретным приложением) является одной из основных проблем, возникающих в рамках традиционного сотрудничества, в области данных [17]. Несмотря на то, что технология блокчейн гарантирует неизменность данных после момента их ввода в систему, гарантия

Electronic copy available at: https://ssrn.com/abstract=3888108

безупречности первоначального ввода данных отсутствует. В связи с этим необходимо использовать и другие механизмы, например, государственные реестры, которыми предусматриваются специальные правила и процедуры для обеспечения качества данных. Таким образом, во многих развитых странах блокчейн-системы могут либо импортировать свои данные, либо использовать их в качестве внешнего «оракула» [18]. Оракул – это агент, который находит и подтверждает реальные события и передает эти данные в блокчейн для использования смарт-контрактов.

Этот агент может быть программным, аппаратным и человеческим. Оракул в блокчейне – это надежный источник данных, который отправляет информацию в блокчейн для использования другими смарт-контрактами. Augur и Gnosis, платформы на базе Ethereum, уже используют оракулы для получения данных о фондовых рынках. В общем, оракулы являются неотъемлемой частью контрактов с несколькими подписями. Блокчейны Tezos и EOS – примеры использования оракула [19].

В контексте проекта «Cardossie» мы видим, что государственные органы могут использовать принадлежащие им полномочия для того, чтобы принудительно обеспечить качество данных в блокчейне, если они используют данные, полученные на основе блокчейна, для своей внутренней работы. Неизменность записей, внесенных в блокчейн-платформу, усиливает возможность проверки того, были ли данные изменены.

5) Государственные органы как пользователи данных.

Государственный сектор имеет большой опыт в осуществлении сбора информации. При этом он обладает гораздо меньшим опытом обмена цифровыми данными с другими заинтересованными сторонами внутри экосистемы.

В связи с этим и в контексте рассматриваемого проекта можно вести речь о трех способах, при помощи которых государственные органы могут получить пользу от совместного использования блокчейн-платформы.

Во-первых, они могут использовать платформу для интеграции с другими стейкхолдерами и получения большего количества высококачественных данных. Это особенно важно в случае, если они находятся в конце информационной цепочки и вынуждены полагаться на вторичные данные.

Во-вторых, блокчейн-платформу можно рассматривать в качестве распределенной базы данных с тонко детализированным управлением доступом и отслеживанием посещений.

Это позволяет как частным партнерам, так и государственным органам не только иметь гораздо более детальный доступ к данным, но и осуществлять обмен данными на таком уровне, который раньше был невозможен ввиду наличия строгих правил и законов

Electronic copy available at: https://ssrn.com/abstract=3888108

о защите данных. Следуя примеру Эстонии, где многие акторы экосистемы здравоохранения обладают доступом к данным, при этом доступ регистрируется и в случае необходимости может быть оспорен, участники платформы могут перейти к «оптимистичному управлению доступом».

В-третьих, государственные органы могут проводить анализ на основе набора данных, превышающего их собственные ресурсы данных. Суверенная схема передачи данных, интегрированная в платформу «Cardossier», обеспечивает соблюдение нормативов и закона о данных.

6) Государственный орган как стимул для создания общественных благ.

Во многих случаях рассмотренные выше особенности государственных органов выступают мощными стимулами для их включения в блокчейн-консорциумы. Таким образом, неудивительно, что во многих блокчейн-консорциумах государственные органы берут на себя роль организатора платформы. Однако за их участие приходится платить частным агентствам.

Так, согласно ч. 1 ст. 8 Союзной конституции Швейцарской Конфедерации в Швейцарии все люди равны перед законом, тем самым государственные органы и учреждения могут участвовать только в блокчейн-консорциумах, которые открыты для всех швейцарских стейкхолдеров, что наилучшим образом реализуется в рамках некоммерческой ассоциации.

Проект «Cardossier» показывает, что участие государственных учреждений в блокчейн-консорциумах во многих смыслах «социализирует» блокчейн-платформы, т. е. превращает их в общественное благо. С одной стороны, это выступает дополнительным преимуществом «укрощения» методов «дикого запада», характерных для многих рынков цифровых товаров, с другой, это также может устранить стимулы для участия в создании и управлении совместной платформой.

Сочетание этих шести ипостасей позволяет рассматривать государственные органы в качестве ключевых игроков, участвующих в блокчейн-платформе. Таким образом, блокчейн-платформы позволяют новыми способами достичь приемлемого компромисса между разнонаправленными публичными и частными интересами [15].

Особо подчеркнем, что цифровые платформы начинают играть ключевую роль в современной экономике по всему миру, что обусловливается рядом следующих факторов.

Во-первых, действует сетевой эффект.

Во-вторых, платформы способны к извлечению, контролю и анализу данных: чем больше пользователей, тем больше данных. Сказанное позволяет выиграть конкурентную борьбу и обрести статус «лидера».

Electronic copy available at: https://ssrn.com/abstract=3888108

В-третьих, предоставление платформой различного рода услуг, в том числе в комплексе, т.е., по сути, наращивание мощности, увеличивает издержки пользователей, которые они понесут, в случае принятия решения о переходе к другой платформе или провайдеру услуг [20].

В литературе на современном этапе широкое распространение получил подход, согласно которому государство рассматривается в качестве платформы - «государство как платформа (далее – ГКП)». Последний представляет собой экосистему, состоящую из трех групп, как правило, рассматриваемых в качестве субъектов, взаимодействующих друг с другом в рамках социально-экономического развития государства (таблица 2.1). Для каждой группы характерен определенный набор интересов, которые могут получить свою реализацию в процессе цифровой трансформации.

К первой группе относится государство, которое заинтересовано в повышении качества государственного управления, потенциальной готовности к технологических вызовам и перманентным усложнениям и изменениям существующих экономических отношений, обеспечении поддержки в развитии человеческого капитала и его сохранении внутри страны, а также повышении уровня конкурентоспособности государства на мировой арене.

Ко второй – граждане, которые рассматриваются в качестве потребителей услуг государства. Интерес граждан, прежде всего, связан с увеличением спектра предоставления государственных услуг, а также повышением их качества, снижением различного рода издержек (например, временных), субъективного фактора, а также повышения уровня безопасности и стабильности правовой среды в целом.

К третьей группе соответственно относится бизнес, интересы которого сопряжены с созданием инфраструктуры для запуска цифровых платформ за счет бюджетного финансирования, «проведении исследований и разработок, которые мог бы использовать в своих бизнес-целях, в создании законодательства, благоприятного для формирования и развития бизнеса, в преференциях со стороны государства и поддержке в работе на зарубежных рынках» [21].

Таблица 2.1 – Экосистема субъектов ГКП и их интересов

Государство как платформа		
Государство	Граждане	Бизнес
Повышение удовлетворенности государственными сервисами для граждан и бизнеса	Снижение субъективизма при получении государственных услуг	Поддержка в работе на зарубежных рынках
Сохранение человеческого и технологического капитала внутри страны	Повышение безопасности и стабильности среды для жизни и бизнеса	Технологическая инфраструктура платформы

Electronic copy available at: https://ssrn.com/abstract=3888108

Продолжение таблицы 2.1

Государство как платформа		
Государство	Граждане	Бизнес
Повышение скорости и качества государственного управления, стратегических решений	Расширение спектра и качества услуг	Поставщик данных для ГКП
Повышение конкурентоспособности страны на внешних рынках	Снижение стоимости государственных услуг	Потребитель сервисов ГКП
Адаптивность к вызовам нового технологического уклада		Исследования и разработки в ГКП для использования в бизнес-процессах
		Законодательство, благоприятное для создания и развития бизнеса

Примечание – Источник [21].

В этой связи можно прогнозировать появление следующей модели государственного участия:

- сервисное государство, «заточенное» на граждан-пользователей и субъектов предпринимательской деятельности;

- государство возьмет на себя управленческую роль координатора всех участников платформы;

- необходимость механизма обратной связи между гражданами и государством [21].

Так, в октябре 2019 года председатель КНР Си Цзиньпин заявил, что необходимо увеличить инвестиции в развитие блокчейна, чтобы занять лидирующие позиции на волне индустриальной и технологической трансформации. В апреле текущего года для массового внедрения этой технологии КНР сформировала национальный комитет по блокчейну и стандартизации, в работе которого примут участие крупнейшие технологические компании Ant Financial, Huawei, Tencent, Baidu. Еще одна масштабная инициатива Китая – создание надежной, недорогой и широкодоступной платформы для блокчейн-сервисов с разветвленным облачным хранилищем данных (Blockchain Service Network, BSN). Она готовится в сотрудничестве с UnionPay (оператор национальной платежной системы Китая) и China Mobile (крупнейший в мире мобильный оператор) [22]. В России потенциальная возможность применения технологии распределенных реестров в рамках предоставления государственных услуг, связанных с оформлением и выдачей документов, а также совершению различного рода регистрационных действий допускается Правительством. Например, Поручение Председателя Правительства Дмитрия Медведева от 06 марта 2017 года по вопросу о возможности применения

Electronic copy available at: https://ssrn.com/abstract=3888108

технологии блокчейн в системе государственного управления и экономике Российской Федерации [23].

Использование блокчейна допустимо там, где существует «пошаговые правила поведения: внесение записей о переходе права собственности или обременениях на недвижимое имущество, акции или доли хозяйственных обществ, удостоверение документов и сделок, проведение финансовых операций, предоставление сведений из публичных реестров и др. [24].

Тем самым, данная технология «может использоваться для автоматизации подобных процессов в любой организации, однако речь не идет об автоматизации права как явления, скорее о возможности оптимизации и дигитализации процессов в областях, где нет необходимости привлекать специалистов для решения задач, с которыми может справиться компьютер» [24].

Технологически важно, что блоки записываются в линейном последовательно-хронологическом порядке.

Реестр записей децентрализованных транзакций можно использовать «для регистрации права собственности, подтверждения и отзыва контрактов, нотариальных записей, состояния здоровья и др., т.е. в областях, где требуется наличие подтверждающего документа, в роли которого выступит блок с определенной записью» [22]. Выделяются следующие варианты применения данной технологии:

«1) страхование;

2) кредитование через Интернет;

3) оформление прав наследования, завещания;

4) нотариальные действия и документы, требующие анонимности и возможности использования вне страны (региона) получения/ оформления;

5) карты здоровья, 6) сохранение культурного наследия;

7) право интеллектуальной собственности» [25].

Другие источники указывают на следующие использования блокчейна в госсекторе:

1) для реорганизации интерактивной системы традиционных услуг гражданам (улучшение идентификации личности отдельных граждан и записей в финансовых операциях, голосовании, налоговых сборах, регистрациях, лицензировании и других обычных действиях правительства, требующих проверки подлинности удостоверения,

2) для облегчения обеспечения безопасности аудиторских проверок для обеспечения соответствия нормативным требованиям в целях сокращения объема расходов по контрактам и совершенствование правоприменительной деятельности,

Electronic copy available at: https://ssrn.com/abstract=3888108

3) для обеспечения безопасного и надежного управления идентификационными данными, особенно для иммигрантов и иностранцев,

4) технология блокчейн может улучшить процессы управления контрактами правительств путем проверки завершения этапа или соблюдения крайнего срока, тем самым улучшая кредитоспособность подрядчика [26].

За счет того, что хранение юридических документов (справок, актов, отчетов и др.) осуществляется в распределенном реестре, можно минимизировать бумажный документооборот, сэкономить время на совершении формальных, однако обязательных в соответствии с законодательством операций, одновременно верифицируя их в кратчайшие сроки [27]. Данная технология может быть использована для создания так называемых репутационных списков в отношении государственных служащих. Также эта технология позволяет создавать репутационные списки для государственных служащих, в рамках которых будет существовать потенциальная возможность внесения записи, содержащей информацию о совершенной государственным служащим манипуляции с бюджетными средствами различных уровней бюджетной системы РФ.

Предполагается, что блокчейн перспективно использовать в регистрационной деятельности, госзакупках. Но в действительности в регистрационной деятельности занято множество органов. Только непосредственно в акте регистрации могут участвовать банки, нотариусы, строительные компании. Если принять во внимание все сопутствующие действия (а это как минимум регистрация по месту жительства, постановка на налоговый учет), то диапазон задействованных субъектов расширяется. Отсюда очевидны проблемы: взаимоотношения органов публичной власти (федеральные и региональные, местное самоуправление), межведомственные (Росреестр и МВД по поводу регистрации по месту жительства), государственные и «окологосударственные субъекты (БТИ, МФЦ), государственные – негосударственные субъекты (Росреестр – банки, нотариус) и пр.

В целом исследование прав и обязанностей участников блокчейна, используемого в государственном управлении, позволяет сделать следующие обобщения.

1) Целям государственного управления более всего отвечает закрытый (эксклюзивный) блокчейн. При этом субъекты государственного управления наделяются функциями валидатора, осуществляющего проверку транзакций.

2) Субъектами государственного управления, наряду с органами государственной власти или наделенными отдельными государственными полномочиями органами местного самоуправления, могут выступать иные лица (наделенные полномочиями по государственному управлению в установленном федеральными законами порядке органы

Electronic copy available at: https://ssrn.com/abstract=3888108

и организации), и даже частные лица (банки, например), которые привлекаются к осуществлению транзакций.

3) Взаимодействие субъектов государственного управления в рамках блокчейна требует тщательной проработки в нормативном плане режима доступа к информации, содержащейся в реестре. Необходима дифференциация по формам и объемам такого доступа. При этом следует иметь в виду:

а) объемы компетенций органов исполнительной власти, которыми они наделены непосредственно в силу закона или иных НПА;

б) полномочия, полученные в силу иных механизмов делегирования;

в) объем функций по государственному управлению, осуществляемый частными лицами в рамках блокчейна.

4) Полномочия органов власти как участников системы распределенного реестра должны быть сформулированы в общем порядке в тех актах, которые определяют их компетенцию (т.е. нормативно). Нормативные изменения компетенции государственных органов предполагают:

а) общие изменения компетенции (это означает введение нормы общего характера о цифровой компетенции – реализации полномочий посредством использования цифровых технологий – для всех органов власти;

б) предметные изменения компетенции (нормы, устанавливающие порядок осуществления государственного управления в конкретной сфере);

в) субъектные изменения компетенции (нормы о компетенции конкретных органов власти и должностные инструкции государственных служащих).

5) Отдельной проработки заслуживает механизм консенсуса в принятии решения несколькими субъектами государственного управления – например, в случае перевода на блокчейн разрешительной функции, когда для окончательного решения по выдаче разрешения требуется согласие нескольких субъектов.

6) Отдельная проблема – интероперабельность данных, которыми обладают участники системы распределенного реестра, которая должна быть обеспечена за пределами блокчейна и даже до его создания.

7) Статус валидатора в системе блокчейн автоматически влечет статус обработчика персональных данных, с полным объемом обязанностей и ответственности такого обработчика в соответствии с законодательством о защите персональных данных.

8) Функционирование блокчейна как распределенной системы не может предполагаться абсолютно беспроблемным и бесконфликтным, особенно на первых порах. Потенциальные конфликты должны быть учтены:

Electronic copy available at: https://ssrn.com/abstract=3888108

а) при формулировании компетенции органов власти;

б) при наделении полномочиями по государственному управлению негосударственных субъектов;

в) при коррекции законодательства о порядке осуществления государственной функции (регистрация недвижимости, выдача разрешений и пр.);

г) при разработке алгоритма, на котором основывается конкретная система распределенного реестра;

е) путем создания независимого органа по защите персональных данных.

Сказанное позволяет сделать вывод о необходимости адаптации к применению блокчейна (а в перспективе возможно других видов ТРР) в деятельности органов государственного управления текущих актов, устанавливающих их компетенцию, разработке типовых соглашений органов об участии в ТРР, что позволит минимизировать правовые риски компетенционного характера. Кроме того, нуждаются в нормативном оформлении вопросы, кто и по каким правилам разрабатывает алгоритм, осуществляет техническую поддержку блокчейна и является держателем данных. В случае привлечения частных субъектов необходимо нивелировать как общие, так и специфические риски.

Electronic copy available at: https://ssrn.com/abstract=3888108

3 Результаты анализа возможности соблюдения основных прав человека при использовании блокчейна в государственном управлении

3.1 Право на защиту персональных данных

Персональные данные и их использование выступают основополагающим структурным элементом цифровой экономики. Все большее число бизнес-моделей полагаются на персональные данные в качестве ключевого ресурса. В обмен на свои данные пользователи получают персонализированные и инновационные услуги. В то же время сбор, обработка и использование компаниями персональных данных ставят под сомнение неприкосновенность частной жизни и основные права человека. Кроме того, учитывая большую коммерческую и стратегическую ценность персональных данных, их накопление, контроль и использование могут породить проблемы, связанные с конкуренцией, и негативно повлиять на потребителей. Таким образом, разработка нормативно-правовой базы, обеспечивающей надлежащий уровень защиты персональных данных, и в то же время предоставляющей предприятиям открытые и равные условия для развития основанных на данных инновационных услуг, выступает сложной задачей. Для ее решения может быть использован комплексный подход, позволяющий рассмотреть проблему защиты персональных данных через призму различных отраслей права, как частного, так и публичного.

С юридической точки зрения, из права на защиту частной жизни «выводится» право на защиту персональных данных [28]. Право на частную жизнь – одна из азбучных истин континентального права [29]; к примеру, французская доктрина различает две составные частной жизни – личная частная (персонально-интимная) жизнь и социальная частная жизнь. Именно в логику социальной частной жизни отлично вписываются социальные сети, в то время как с личной частной жизнью они скорее находятся в антагонистических отношениях [29]. ЕСПЧ подтвердил право любого индивида строить отношения с другими людьми [30], охватив впоследствии этим правом и электронную переписку [31]. Директива Европейского парламента и Совета Европейского союза от 15 декабря 1997 г. № 97/66/ЕС [32] обязывает соответствующие государства на уровне национального законодательства «обеспечивать конфиденциальность коммуникаций, осуществляемых посредством общедоступной телекоммуникационной сети и общедоступных телекоммуникационных услуг». Все это – право на частную жизнь.

Российское законодательство в рассматриваемой сфере является проевропейским по своим истокам. Собственно, европейский путь России в этой области начался с ратификации Конвенции о защите физических лиц [33]. Далее, Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» [34] определил персональные данные в

Electronic copy available at: https://ssrn.com/abstract=3888108

широком ключе (любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу), что полностью соответствует европейскому подходу. Наконец, Федеральным законом от 02.07.2013 № 142-ФЗ [35] в Гражданский кодекс была введена статья 152.2 «Охрана частной жизни гражданина» (Если иное прямо не предусмотрено законом, не допускаются без согласия гражданина сбор, хранение, распространение и использование любой информации о его частной жизни, в частности сведений о его происхождении, о месте его пребывания или жительства, о личной и семейной жизни).

Однако правоприменение нуждается в более точной формулировке, что такое персональные данные. И если в Европе подобного рода широкие определения получают судебную интерпретацию, то в России больше ориентируются на разъяснения уполномоченного органа в данной области. Так, в Методических рекомендациях Роскомнадзора по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения (п.п. 2.5-2.7) [36] выделено три категории персональных данных, подлежащих обработке оператором:

- персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (фамилия, имя, отчество, год, месяц, дата рождения, место рождения, адрес, семейное положение, социальное положение, имущественное положение, образование, профессия, доходы, другая информация, относящаяся к субъекту персональных данных);

- специальные категории персональных данных (расовая, национальная принадлежность, политические взгляды, религиозные или философские убеждения, состояние здоровья, интимная жизнь);

- биометрические персональные данные (сведения, которые характеризуют физиологические и биологические особенности человека, на основе которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных).

Логичен вывод о том, что российское законодательство в области защиты частной жизни вполне соответствует европейским стандартам. Однако в Европе уже признано, что их необходимо пересматривать в свете цифровизации общества, поскольку налицо явный конфликт требований о защите персональных данных и фактической невозможностью их соблюсти в связи с попаданием таких сведений в интернет. Как отмечают исследователи, в новых технологических реалиях обезличивание данных уже не может выполнять

Electronic copy available at: https://ssrn.com/abstract=3888108

функцию эффективного средства защиты персональных данных и в более глобальном смысле – частной жизни граждан [37].

Таким образом, именно персональные данные являются одним из основных вопросов цифровой революции, с увеличением количества цифровых устройств они пропитали все сферы частной и публичной жизни. Цифровые персональные данные представляют особый интерес. С точки зрения правового регулирования, если изначально персональные данные регулировались только публичным правом (как и в целом, право на информацию и информационное право возникли в публично-правовой сфере), то теперь персональными данными все больше занимается частное право, а также уголовное, международное. Это ведет к комплексности регулирования. Обостряется конфликт публичного и частного, одновременно усредняются их подходы, благодаря такого рода комплексным институтам взаимодействие между подсистемами и отраслями права усиливается.

3.2 Право на забвение

В Европе право на забвение получило значительное внимание в свете принятого в 2014 году решения Европейского суда справедливости и законодательных дискуссий в Европейском парламенте в связи с разработкой Общего регламента по защите данных (далее – GDPR), принятого в 2016 году. Однако до того, как эра интернета достигла своего полного расцвета, более привычная форма такого права, возможно, заключалась в возможности бывших преступников скрыть информацию, которая имеет непосредственное отношение к их криминальной истории.

Так, в Швейцарии это право было признано Федеральным судом Швейцарии в деле BGE 122 III 449, где он постановил, что публичный интерес населения к информации, касающейся правонарушителей, не бесконечен. Поэтому широкая общественность не должна иметь неограниченный доступ к персональным данным, относящимся к преступлениям. Соответственно, преступник имеет право на забвение, как только он больше не представляет интереса для широкой общественности и отбыл свое наказание. В широком смысле слова, Федеральный суд Швейцарии признает право на забвение в качестве дальнейшей разработки положений об удалении, в соответствии с которыми информация не обязательно должна быть удалена, но больше не может распространяться. Таким образом, процесс удаления осуществляется скорее в смысле акта забвения по отношению к коллективной памяти швейцарского общества [38].

В Европейском союзе право на забвение получило свою реализацию в рамках GDPR (ст. 17 Право на удаление (право на забвение)). Однако до принятия GDPR ядро данного права уже существовало в законодательстве о защите данных в том смысле, что

Electronic copy available at: https://ssrn.com/abstract=3888108

лицу было предоставлено право требовать от обработчиков данных удаления относящихся к нему персональных данных [38]. Его корни – в ст. 12 директивы 95/46/CE, где признано в общем плане право на исправление данных, чья обработка не соответствует директиве, по причине неполноты или неточности данных. То, что данное право фактически представляет собой право на забвение, было подтверждено Европейским судом в его знаковом судебном решении.

В деле Google Spain 2014 года физическое лицо в конце 1990-х годов было вовлечено в процедуру ареста имущества, направленную на погашение долгов этого лица по социальному обеспечению. При вводе имени данного физического лица в поисковой машине Google последняя выдавала результаты публикаций в газете, которая содержала сведения о данном разбирательстве. В связи с этим данное физическое лицо обратилось с жалобой к испанскому должностному лицу по защите данных, требуя удаления публикаций с веб-сайта издателя, а также из результатов поиска Google, со ссылкой на закон о защите данных. Европейским судом проанализированы дела в соответствии с действующей Директивой 95/46/ЕС Европейского парламента и Совета Европейского Союза от 24 октября 1995 года о защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных (директивой по защите данных). В отношении издателя жалоба была отклонена, поскольку испанское должностное лицо по защите данных пришло к выводу, что публикация такой информации отвечает публичным интересам. Однако в отношении Google жалоба была удовлетворена. В конечном итоге, Европейский суд, по-видимому, подтвердил толкование закона испанским должностным лицом по защите данных: операторы поисковых систем могут быть обязаны удалять ссылки на персональные данные, когда обработка этих данных представляет собой нарушение принципов, касающихся качества данных, из-за того, что данные больше не являются релевантными или необходимыми для целей, для которых они были первоначально собраны или обработаны. В тех случаях, когда данные не обрабатываются в соответствии с Директивой 95/46/ЕС, субъект данных имеет право потребовать стирания таких данных в соответствии со статьей 12 (b) данной Директивы. Кроме того, Статья 14 (a) директивы предоставляет физическим лицам в любое время высказывать на законном основании возражение против обработки касающихся их данных, кроме случаев, когда национальным законодательством определено иное. Если возражение является обоснованным, контролер обязан прекратить обработку этих данных. Таким образом, Европейский суд постановил, что физическое лицо имеет право требовать удаления своих персональных данных на основании статей 12 (b) и 14 (a), что означает,

Electronic copy available at: https://ssrn.com/abstract=3888108

что субъект данных имеет право на забвение или, по крайней мере, право быть исключенным из списка (right to be delisted) [38].

С другой стороны, право на забвение, предусмотренное в статье 17 GDPR, исключительно представляет собой право требовать удаления своих персональных данных, причем по лимитированным мотивам. Статья 17 (1) GDPR устанавливает ряд оснований, на основании которых может быть сделан запрос на удаление или «стирание»:

а) персональные данные больше не требуются для целей, для которых они были получены или обрабатывались в иных случаях;

б) субъект данных отзывает свое согласие, на основании которого согласно пункту (a) Статьи 6 (1) или пункту (a) Статьи 9 (2) проводилась обработка, и если отсутствует иное юридическое основание для обработки;

в) субъект данных возражает против обработки согласно Статье 21 (1), и отсутствуют имеющую преимущественную юридическую силу законные основания для обработки, или субъект данных возражает против обработки согласно Статье 21 (2);

г) персональные данные обрабатывались незаконно;

д) персональные данные должны быть уничтожены в целях соблюдения юридической обязанности согласно законодательству Союза или государства-члена ЕС, под действие которого подпадает контролер;

е) персональные данные собирались в отношении предоставления услуг информационного общества согласно Статье 8 (1) [39].

Однако GDPR вводит критерий сбалансированности интересов ввиду того, что решение Google Spain было подвергнуто критике, поскольку оно в достаточной степени не учитывало такие существенные интересы, как право на свободу слова и информацию. Соответственно, запрос на удаление должен быть сбалансирован с публичными и частными интересами сохранения неизменности данных. В статье 17 (3) GDPR перечислены случаи, при которых право на забвение может «уравновешено»:

а) для осуществления права на свободу выражения мнения и распространения информации;

б) в целях соблюдения юридической обязанности, которая требует проведение обработки согласно законодательству Союза или государства-члена ЕС, под действие которого подпадает контролер, или для выполнения задачи, осуществляемой в интересах общества, или при осуществлении официальных полномочий, возложенных на контролера;

в) по причинам государственного интереса в области общественного здравоохранения в соответствии с пунктами (h) и (i) Статьи 9 (2), а также Статьи 9 (3);

Electronic copy available at: https://ssrn.com/abstract=3888108

г) в целях архивирования в интересах общества, в целях научных или исторических исследований или в статистических целях, указанных в Статье 89 (1), постольку, поскольку право, указанное в параграфе 1, может сделать невозможным или негативно отразиться на достижении целей указанной обработки; или

д) для обоснования, исполнения или ведения защиты по судебным искам [39].

Статья 17 (2) GDPR касается проблемы распространения информации в онлайн-среде – аспекта, который, возможно, не был должным образом рассмотрен в Директиве 95/46/ЕС и не был принят во внимание в предыдущем прецеденте в отношении права на забвение. Примечательно, что подход, который следует принять в этой связи, горячо обсуждался на протяжении всего законодательного процесса. В частности, Европейский парламент предложил возложить на процессора данных обязательство по стиранию данных и принятию разумных мер для обеспечения того, чтобы данные, обрабатываемые третьими лицами, были стерты. Статья 17 (2) GDPR предусматривает, что если контролер обнародовал персональные данные и он обязан их удалить, то с учетом имеющихся технологических возможностей и расходов на имплементацию он должен принять необходимые меры, в том числе технические меры, чтобы проинформировать контролеров, которые обрабатывают персональные данные, о том, что субъект данных затребовал от них удаление любых ссылок, копий или точных повторений указанных персональных данных [39].

В России право на забвение введено Федеральным законом от 13.07.2015 № 264-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и статьи 29 и 402 Гражданского процессуального кодекса Российской Федерации», который предписал операторам поисковых систем исключать из результатов поисковой выдачи ссылки, позволяющие получить доступ к информации о заявителе, распространяемой с нарушением законодательства Российской Федерации, являющейся недостоверной или неактуальной.

Основанием удаления является недостоверность или неактуальность сведений, утративших значение для заявителя в силу определенных обстоятельств или действий самого заявителя. По мнению исследователей, именно в данном аспекте и проявляется несовершенство положений GDPR и ст. 10.3 Закона № 149-ФЗ: не определен критерий общественной значимости, который устанавливал бы баланс между интересами общества (право на информацию) и неприкосновенностью частной жизни.

Еще одним проблемным аспектом «права на забвение» является то, что по запросу заявителя удаляются именно ссылки в поисковой системе, но не сама информация.

Electronic copy available at: https://ssrn.com/abstract=3888108

В связи с этим в литературе предлагается скорректировать положения ст. 10.3 Закона № 149-ФЗ и доработать механизм реализации «права на забвение», а именно: ввести критерий общественной значимости, определяющий основание удаления из Сети тех или иных сведений; исключить возможность требовать от оператора поисковой системы удаления из результата поиска ссылок не иначе как по решению суда; предоставить оператору поисковой системы самостоятельно определить форму обращения к ним; рассмотреть возможность удаления всей информации о заявителе, указанной в его обращении, а не конкретных ссылок на нее [40].

3.3 Право на судебное обжалование решений органов власти

Право на судебную защиту прав и свобод гарантировано каждому в силу ст. 46 Конституции РФ. Будут ли им охвачены так называемые технические действия при регистрации на блокчейне? Попытаемся ответить на этот вопрос.

Необходимо отметить, что конституционное право на обжалование в суд решений и действий (бездействия) органов государственной власти трактуется широко. Конституционный Суд РФ, выявляя смысл конституционных положений ст. 46 Конституции РФ, неоднократно подчеркивал, что «возможность лица обжаловать принятые органами государственной власти и местного самоуправления и их должностными лицами решения, включая нормативные правовые акты, воплощающая в себе как индивидуальный (частный) интерес, связанный с восстановлением нарушенных прав, так и публичный интерес, направленный на поддержание законности и конституционного правопорядка, является неотъемлемой характеристикой нормативного содержания права каждого на судебную защиту, одной из необходимых и важнейших его составляющих» [41]. В данном случае категорией "решения" охватываются как нормативные, так и индивидуальные акты.

По большому счету, каким бы образом ни были затронуты права человека при обработке его данных в блокчейне, это составляет предмет отдельного судебного иска. К слову, судебная практика в области защиты персональных данных в России находится в стадии формирования.

Анализ судебной практики по защите персональных данных в суде специалистами СПС Консультант плюс позволил систематизировать исковые требования, обычно предъявляемые в таких случаях, следующим образом:

1) основные исковые требования:

- о защите персональных данных;

Electronic copy available at: https://ssrn.com/abstract=3888108

- о признании незаконными действий ответчика по получению/обработке/хранению/использованию/распространению/предоставлению (передаче) персональных данных истца третьему лицу;

- о признании незаконным бездействия ответчика, выразившегося в не прекращении обработки персональных данных истца и их не уничтожении после получения ответчиком заявления истца об отзыве согласия на обработку его персональных данных и их уничтожении;

- о признании информации, распространяемой на сайте в сети Интернет в отношении истца, информацией, обрабатываемой с нарушением законодательства РФ в области персональных данных;

- об обязании ответчика отозвать/изъять/исключить/уничтожить (заблокировать и уничтожить) персональные данные истца из информационных баз данных/из электронной базы (базы, системы) ответчика/из документов;

- об обязании ответчика прекратить хранение/обработку/передачу третьим лицам персональных данных истца.

2) дополнительные исковые требования:

- о признании договора незаключенным;

- о расторжении кредитного договора/договора об оказании платных медицинских услуг/другого договора;

- о признании заключенного между истцом и ответчиком договора займа недействительным, о применении последствий недействительности договора;

- о признании недействительным договора об обязательном пенсионном страховании;

- о признании незаконной передачи персональных данных в порядке применения последствий ничтожной сделки;

- об обязании ответчика исключить персональные данные истца из бюро кредитной истории/внести исправления в кредитную историю истца в бюро кредитных историй/произвести обновление кредитной истории в центральном каталоге кредитных историй;

- об обязании ответчика направить уведомление об уничтожении персональных данных истца в Роскомнадзор;

- об обязании ответчика дать опровержение размещенной информации об истце;

- об обязании ответчика уничтожить сведения об истце, порочащие его честь, достоинство и деловую репутацию;

Electronic copy available at: https://ssrn.com/abstract=3888108

- о признании деятельности сайта в отношении истца нарушающей его права на неприкосновенность частной жизни, личную и семейную тайну;

- о включении электронного ресурса, на котором размещены персональные данные истца, в Реестр нарушителей прав субъектов персональных данных;

- о компенсации морального вреда;

- о взыскании судебных расходов.

Заметим, что данная систематизация проведена в рамках существующего российского законодательства. Одновременно, с точки зрения предмета иска в литературе сформулировано предложение предусмотреть в законодательстве новое притязание: требование о возврате доступа к цифровому коду - для случаев неправомерной цифровой транзакции, совершенной помимо воли собственника вещи [42]. Это имеет прямое отношение к организации государственного блокчейна, в особенности при регистрации сделок с недвижимостью. При двойной регистрации цифрового права на недвижимость за разными лицами и при сохранении владения вещью действительный обладатель права мог бы по аналогии с оспариванием зарегистрированного права в ЕГРП (ЕГРН) (п.п. 52-59 Постановления Пленумов ВАС РФ и ВС РФ от 29.04.2010 № 10/22) требовать признания цифрового права отсутствующим, и тогда ответчиком было бы лицо, неправомерно указанное в реестре блокчейна в качестве правообладателя, а администраторы блокчейна будут выступать третьими лицами без самостоятельных требований. Таким образом, при совершении неправомерных цифровых транзакций для защиты обладателей цифровых прав должен существовать самостоятельный способ защиты: требование о возврате доступа к цифровому коду, механизм реализации которого может сочетать в себе принципы традиционных правовых притязаний и технические особенности киберпространства.

К слову, использование блокчейна в частно-правовых интересах способно создать даже большие спорные ситуации. Частично они могут разрешаться традиционными гражданско-правовыми способами. Так, при добросовестном приобретении токена должны применяться принципы, которые существуют как в правовом институте ограничения виндикации (ст. 302 ГК РФ), так и в нормах о защите обладателей бездокументарных ценных бумаг (ст. 149.3 ГК РФ). Недобросовестные лица, причастные к неправомерной цифровой транзакции, должны нести ответственность за причиненные убытки.

Однако если транзакции на платформе блокчейн совершаются анонимно, то применение указанных способов защиты имущественных прав будет осложнено тем, что

Electronic copy available at: https://ssrn.com/abstract=3888108

без осведомленности личности ответчика потерпевший не сможет оформить исковое заявление и определить начало исчисления исковой давности.

В последнее время юристы все чаще признают, что возможно и создание гибридных способов правового регулирования, включающих как сугубо юридические, так и цифровые инструменты, что требует совместной работы представителей юридической науки и программистов.

Продолжение дискуссии в частном праве строится вокруг цифровых прав. Токен (цифровое право), по существу, является юридическим символом, удостоверяющим посредством записи в децентрализованной информационной системе права на объекты гражданских прав. Токен должен оставаться технологией, конструирование из него юридической фикции посредством наделения его качеством оборотоспособности и выделения в ст. 128 ГК РФ нового вида имущества, по крайней мере в вещном праве, является неоправданным.

Цифровые права в качестве фикций допустимо задействовать в обязательственных, интеллектуальных и корпоративных правоотношениях, так как здесь имущественное право само по себе выполняет роль и субъективного права, и объекта [42].

Возвращаясь к предмету нашего исследования, отметим, что даже в цивилистической литературе для обеспечения охраны прав участников рынка недвижимости рекомендуется использовать консорциумный блокчейн, администраторами которого должны выступать специалисты в сфере недвижимости. Получается, только отойдя от изначальных «чистых» принципов блокчейна (оставляя неизменность данных и защиту, но сохраняя «власть» над ними), можно получить технологию более управляемую и совместимую с законодательством.

Electronic copy available at: https://ssrn.com/abstract=3888108

4 Результаты исследования юридической значимости документов, созданных в результате блокчейна

С правовой точки зрения использование технологии распределенного реестра уместно, если это позволяет достичь юридически значимых результатов. В избранном нами для целей настоящего исследования кейсе - государственной регистрации недвижимости - таким результатом будет передача имущества (права), что традиционно удостоверяется документом.

В теории права выделяются признаки юридически значимого документа. Это документ, который: содержит информацию, имеющую правовое значение (1), порождает юридические последствия (2), регулирует общественные отношения, придает им стабильность и устойчивость (3), оформляется в процессе юридической деятельности (4). Для оформления документов необходим волевой акт – законодателя, гражданина, объединения, госоргана, юридического лица и т.д. – в пределах компетенции (если речь идет о госорганах и (или) должностных лицах) или правоспособности (актуально для граждан и их объединений).

Согласно п.п. 14 п. 3.1 ГОСТ Р 7.0.8-2013 «Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения», утв. Приказом Росстандарта от 17.10.2013 N 1185-ст (далее – ГОСТ Р 7.0.8-2013, юридически значимый документ – это документ, который может выступать в качестве подтверждения деловой деятельности либо событий личного характера. При этом понятия «юридическая значимость» и «юридическая сила документа» не равнозначны (юридическая сила документа - свойство официального документа вызывать правовые последствия, п.п. 15 п. 3.1 ГОСТ Р 7.0.8-2013). Таким образом, юридическая сила по смыслу уже, нежели юридическая значимость. В литературе отмечается, что юридическая значимость документа согласно ГОСТу 2013 является свойством любого документа, а не только свойством официального документа [43]. Встречается также мнение, что юридическое значение является одним из факторов для отнесения документов к официальным [44].

По информации Минкомсвязи России «Электронная трудовая доступна теперь на Едином портале госуслуг» к юридически значимым документам относится информация из электронной трудовой книжки, загруженная в личный кабинет на портале госуслуги, выгруженная в виде скана бумажной выписки. ФТС России отмечает, что отсутствие надлежащего удостоверения документа лишает его юридической значимости [45]. Согласно Приложению 4 к Временным единым требованиям к техническим параметрам сегментов аппаратно-программного комплекса «Безопасный город» (утв. МЧС России

Electronic copy available at: https://ssrn.com/abstract=3888108

29.12.2014 № 14-7-5552) юридическая значимость документов обеспечивается использованием сертифицированных средств криптографической защиты информации – электронной подписи.

Как видим, у органов и организаций достаточно широкий диапазон подходов к оценке значимости собственных юридических документов.

В рамках частного права чаще всего оценивается значимость ценных бумаг. В отношении документарных ценных бумаг обязательные реквизиты, требования к форме документарной ценной бумаги и другие требования к документарной ценной бумаге определяются законом или в установленном им порядке. При отсутствии в документе обязательных реквизитов документарной ценной бумаги, несоответствии его установленной форме и другим требованиям документ не является ценной бумагой, но сохраняет значение письменного доказательства (ст. 143.1 ГК РФ).

В разъяснениях, данных СПС Консультант плюс, юридически значимый документ определяется как документ, отвечающий определенным требованиям, которые установлены нормативно-правовым актом или участниками правоотношений, и подтверждающий конкретные факты.

Использование электронной формы документа дополняет перечень его признаков в условиях цифровой экономики. В ходе расширения практики электронной переписки, суд признает, что получение или отправка сообщения с использованием электронного адреса электронной почты, известного как почта самого лица или служебная почта его компетентного сотрудника, свидетельствует о совершении этих действий самим лицом, пока им не доказано обратное [46]. Но это в гражданском обороте, где все разрешено, что не запрещено. Государственное управление и действия госорганов регулируются в нормативном порядке, поэтому и в отношении электронных документов, и тем более в отношении документов, сформированных посредством блокчейн, придется принимать норму общего действия, легитимизирующую такие документы.

Аналогичным образом электронный документооборот был признан в сфере государственных закупок. Передача документов и информации посредством электронной почты не будет считаться надлежащим способом исполнения обязательств в случаях, когда законом прямо предусмотрена необходимость использования иных средств взаимодействия участников гражданского оборота при исполнении заключенной сделки. К примеру, Федеральным законом от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» не предусмотрена возможность направления победителем торгов банковской гарантии заказчику посредством электронной почты, факса либо нарочным путем. Обмен

Electronic copy available at: https://ssrn.com/abstract=3888108

информацией между участником электронного аукциона и заказчиком должен осуществляться только через электронную площадку в форме электронных документов, подписанных усиленной электронной подписью лица, имеющего право действовать от имени участника такого аукциона [47].

Юридическая сила документа служит «инструментом» определения пределов осуществления конкретных действий субъекта и значимости создаваемого им документа во времени, пространстве и по кругу субъектов. Отметим обязательные требования юридической силы документа:

- соблюдение установленной формы;

- соответствие нормативно установленным, а в некоторых случаях - также установленным обычаями, порядку и процедурам создания документа и его использования;

- обеспечение достоверности документированной информации (содержания), подписи и прочих реквизитов, возможность их проверки;

- обеспечение необходимой степени защищенности записи документированной информации с реквизитами (содержания) от подделки и несанкционированных изменений и защиты документа в целом (от уничтожения);

- изложение и удостоверение документированной информации должностным лицом (органа власти или юридического лица) или физическим лицом собственноручной подписью, от которого документ исходит в пределах его полномочий и компетенции;

- установление и соблюдение порядка ведения и приобщения документа к делу [48].

При этом основным условием, обеспечивающим юридическую силу документу, является тот факт, что фиксируемая в документе выделенная информация о событиях, состояниях, фактах, действиях и обстоятельствах должна быть связана с определенными правоотношениями и (или) юридическими последствиями. В связи с этим содержание выделенной информации документа (как воплощение письменной формы) всегда увязано с определенными реквизитами, как правило, характеризующими субъектов, которые и составили документ, и позволяющих по таким реквизитам их идентифицировать. Последние, в свою очередь, увязаны с формой представления документа [48]. Так, требования к электронной подписи установлены в Федеральном законе от 06 апреля 2011 года «Об электронной подписи».

Важное значение обретает правовой статус субъектов, ведущих и контролирующих базы данных – он также должен определяться специальными законами или отдельными нормативно-правовыми актами. Все это непосредственно влияет на установление

Electronic copy available at: https://ssrn.com/abstract=3888108

юридической силы электронного (цифрового) документа, который может быть выражен и в виде записи в базе данных. Кроме того, имеют значение юридическая сила взаимосвязанных с ним первичных электронных документов, соблюдение иерархии форм его представления, а также наличие юридической связи с создавшим их субъектом, его правовым статусом, полномочиями, ответственностью и его обязательными правоотношениями с другими субъектами. Добавим к этому особый режим хранения и защиты как самих документов, так и программно-аппаратных средств, включающих материальные носители, а также организацию защиты этих средств [48]. Получается, что юридическую силу электронного документа обеспечивает целый комплекс средств.

Нужно учитывать, что новая система регистрации на блокчейне возникает не только в отношении новых объектов и субъектов без истории. Более того, истории этих субъектов и объектов – по большей части бумажные. Их достоверность можно проверить только традиционным способом. То есть фиксация сделки через блокчейн не должна легализовать предыдущую незаконную сделку.

В литературе отмечается, что преимущества распределенных реестров на основе блокчейн-технологий по сравнению с централизованными, ведущимися одним субъектом, позволяют выделить критерии, которыми можно руководствоваться при принятии решений по вопросам создания государственных блокчейн-реестров [49], а именно:

1) Государственный реестр используется для реализации прав и обязанностей значительного количества субъектов, не входящих в систему государственного управления (граждан и организаций). Это позволяет в полной мере реализовать такое преимущество блокчейна, как общедоступность. Так, реестр объектов недвижимого имущества и прав на него, построенный на основе технологии блокчейн, даст возможность внесения записей в него значительному количеству физических и юридических лиц - обладателей прав на эти объекты. При этом большинство из указанных лиц будет крайне заинтересовано в сохранности и неизменности этих записей, что приведет к копированию реестра на большое количество носителей.

2) Отношения по поводу объектов, вносимых в реестр, носят преимущественно гражданско-правовой, а не административно-правовой характер. Предполагается, что преимущества блокчейна позволяют реализовать возможность заключения различных сделок в отношении указанных объектов с помощью смарт-контрактов. Поэтому отношения, не предполагающие смарт-контрактов, целесообразно фиксировать с помощью обычных электронных реестров, а не блокчейна.

Electronic copy available at: https://ssrn.com/abstract=3888108

3) Блокчейн, обеспечивая неизменность записей в реестре, помогает нивелировать коррупционные риски в таких областях, как государственные закупки, управление государственным имуществом.

Следует заметить, что данное перечисление скорее поясняет ожидания от использования блокчейна в государственном управлении, хотя несомненно будет полезным при формулировании нами критериев обоснованности применения ТРР в завершающей части работы. Возвращаясь к вопросу о юридическом значении документа, нужно подчеркнуть, что значение определяется тем, как документ реализуется в конкретных правоотношениях, порождая, изменяя и прекращая их.

Основным требованием к документу является его качество, под которым понимается соответствие предъявляемым к нему нормативным требованиям. К ним относятся законность (содержание, форма), обоснованность, достоверность (под достоверностью следует понимать соответствие содержания юридического документа действительности), юридическая и лингвистическая грамотность (кстати, ее в электронном формате проще всего контролировать – путем введения обязательных шаблонов документов).

Документ, который не соответствует предъявляемым к нему требованиям, содержит дефекты. Согласно доктрине, дефект юридического документа - это изъян, состоящий в несоответствии формы и (или) содержания юридического документа нормам законодательства, а также потребностям правового регулирования общественных отношений. Дефект возникает в результате умышленной или ошибочной деятельности лиц, создающих, принимающих, перерабатывающих юридические документы, и влекущий за собой ухудшение качества юридического документа [50].

Дефекты формы юридического документа могут быть подразделены на:

- дефекты носителя юридического документа;
- дефекты реквизитов юридического документа;
- дефекты структуры юридического документа [50].

Под содержанием юридического документа следует понимать единство его элементов, свойств, раскрывающих сущность и назначение юридического документа. К содержательным относят лингвистические дефекты, логические дефекты, дефекты фактов, фактические дефекты.

В результате дефектов юридический документ может стать непоследовательным и неполным по содержанию. Можно выделить следующие виды дефектов внешней формы выражения юридических фактов:

Electronic copy available at: https://ssrn.com/abstract=3888108

- неполнота информации (когда документ содержит не всю необходимую для наступления юридических последствий информацию);

- ошибки в содержании юридического документа, удостоверяющего юридический факт (или ошибки невнимательности – неправильно указана фамилия, наименование учреждение и пр.);

- фальсификация доказательств о несуществующих юридических фактах (это умышленное искажение, влекущее ответственность вплоть до уголовной);

- отсутствие юридического документа, подтверждающего юридический факт (его утеря, кража и пр.). Часто восстановление документов проходит специальную процедуру (как при восстановлении паспорта либо установлении юридических фактов в суде) [50].

Под фактической ошибкой понимается неумышленный изъян в содержании юридического документа. Это может быть неточное приведение реквизитов нормативных правовых актов, к которым отсылает юридический документ, отсылка к нормативным правовым актам, утратившим юридическую силу, «пустые» отсылки (к статьям нормативного правового акта, не содержащим необходимой информации), отсылка к нормативным правовым актам, которые еще не приняты.

Практически все перечисленные виды дефектов могут быть свойственны и цифровым документам. Если для бумажных документов устоялась система обнаружения и исправления ошибок, то для блокчейн-ошибок это еще предстоит сделать. Так, в европейском административном праве (в частности, французском) имеется право на ошибку (например, после официальной подачи налоговой декларации дается период для исправления ошибок). Иногда ошибка может даже трактоваться в пользу потребителя - статья 3 Конвенции для унификации некоторых правил, касающихся международных воздушных перевозок, прописывает, что неправильность проездного билета не влияет ни на существование, ни на действительность договора о перевозке (право на ошибку в авиабилете). Так называемые технические ошибки могут исправляться в судебных решениях, чему посвящены отдельные процессуальные нормы. Материальное законодательство также содержит определение технической ошибки - это описка, опечатка, грамматическая или арифметическая ошибка либо подобная ошибка, допущенная при оформлении или переоформлении юридически значимого документа (ч. 1 ст. 61 Федерального закона от 13.07.2015 № 218-ФЗ «О государственной регистрации недвижимости»; ст. 7.1 Закона РФ от 21.02.1992 № 2395-1 «О недрах»; ч. 12 ст. 5.1 Федерального закона от 18.07.2011 № 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц»; п.п. 1, 2 ч. 2 ст. 21 Федерального закона от 03.07.2016 № 237-ФЗ «О государственной кадастровой оценке»). Техническая ошибка

Electronic copy available at: https://ssrn.com/abstract=3888108

исправляется самим уполномоченным органом в течение установленного законом срока после обнаружения этой ошибки по собственной инициативе либо по заявлению любого заинтересованного лица.

Необходимо продумать способы устранения ошибок в документах, используемые системой распределенного реестра. Кстати, многие из них могут устраняться превентивно, до внесения в систему – в случае разработки соответствующих шаблонов, загружаемых в систему.

Еще одна проблема юридической значимости документов на блокчейне – возможное их непризнание сторонами. Как отмечается в цивилистической литературе, само по себе использование технологии смарт-контракта на практике может привести к новому виду недобросовестного поведения: непризнание стороной ответственности лишь на том основании, что договор был заключен и исполнен с использованием смарт-технологий [51]. Данное предположение справедливо и в отношении документов, созданных посредством блокчейн. Однако решение проблемы во многом за пределами техники и права, скорее это задача цифрового воспитания населения. Право же располагает механизмом «постепенной» модификации правового сознания, например, путем введения типового условия сделки о признании как транзакции, так и связанных с ней документов, сформированных посредством ТРР. В крайнем настойчивом варианте возможно введение такого правила на нормативном уровне (что, впрочем, нежелательно с точки зрения общественного мнения).

Electronic copy available at: https://ssrn.com/abstract=3888108

5 Предложения по основным способам преодоления правовых рисков использования блокчейна в государственном управлении

Проведенное исследование позволяет не только систематизировать правовые риски от использования блокчейн-технологий в государственном управлении, но и предложить способы их преодоления.

Прежде всего, это касается рисков несоблюдения прав человека. Их признание и соблюдение является основной обязанностью государства и его органов, согласно российской Конституции. В этом смысле отправной точкой освоения ТРР, в том числе в форме блокчейна, является аксиома – права человека стоят выше применения цифровых технологий (использования ТРР (блокчейна)). Конституционный Суд Российской Федерации неоднократно выражал правовую позицию о том, что задачи одной только рациональной организации деятельности органов власти не могут служить основанием для ограничения прав и свобод [52, 53].

Мы исходим из того, что преодоление правовых рисков использования ТРР в государственном управлении может осуществляться не только правовыми средствами. Представляется, что помимо чисто нормативного регулирования, на минимизацию или нейтрализацию рисков могут работать меры технического регулирования (протоколы), а также правильное сочетание (возможно, каскадное) правовых и технических мер.

Для последнего очень важно ясно сформулировать цели и скоординировать механизм действия, что представляет собой комплексную междисциплинарную задачу. Это нужно, чтобы не получилось противоречия правовых и технических актов, обилия разнонаправленных регулирующих актов, что составит отдельный риск.

К слову, в литературе к рискам цифровизации относят и несовершенство правовой базы - отсутствие необходимой правовой базы для цифрового госуправления и цифровой экономики, и недостаточный уровень подготовки госслужащих [54], а также недостаточную степень взаимодействия между имеющимися структурными составляющими системы электронного правительства, на различных уровнях власти, - проблему, констатированную еще на этапе электронного правительства.

Данные, и в частности персональные данные, составляют основу функционирования цифровых технологий, в том числе технологии распределенного реестра. Соответственно, большинство правовых рисков связано с основаниями и процедурами их обработки посредством ТРР. Действующее законодательство о персональных данных не вполне «приспособлено» к подобным технологиям, хотя и содержит разумные базовые позиции.

Electronic copy available at: https://ssrn.com/abstract=3888108

Нам представляется, что необходимо в первую очередь систематизировать и урегулировать принципы защиты персональных данных применительно к ТРР, исходя из того, что они распространяются на любого (человека, независимо от гражданства), без какой бы то ни было дискриминации.

Они реализуются прежде всего самим обладателем персональных данных, но при этом необходим контроль независимого органа за защитой персональных данных. При использовании ТРР, в том числе в государственном управлении, в полной мере должны реализовываться критерии законной обработки данных (лояльная обработка, целевая обработка, минимизация данных, качество данных, безопасность данных).

При этом для минимизации рисков для прав человека при использовании блокчейна в государственном управлении необходимо выработать условия использования блокчейна.

Ответственный за обработку данных должен осуществлять контроль за локализацией майнеров. Напомним, любая операция по блочной цепочке предполагает отправку всем миноритариям блокчейна запроса о проверке транзакции (а значит, потенциально и персональных данных) и обновление блокчейна путем добавления нового блока в блочную цепочку у всех участников.

В целях государственного управления круг участников блокчейна должен быть ограничен страной.

Освоение блокчейна в государственном управлении нуждается также в выборе формата для регистрации данных. Принцип минимизации данных требует, чтобы собранные данные были актуальны и ограничивались тем, что необходимо для целей, для которых они обрабатываются. Кроме того, персональные данные не могут храниться в течение неопределенного времени, поэтому срок хранения должен быть определен в соответствии с целью обработки данных. Очевидно, что блокчейн не позволяет реализовать данный общий принцип работы с данными в полной мере. Одна из особенностей блокчейна заключается в том, что зарегистрированные в нем данные не могут быть удалены. После того, как блок, в который интегрирована сделка, был принят участниками, сделка уже не может быть изменена на практике.

Следует напомнить, что блокчейн может содержать две большие категории данных персонального характера:

а) данные, относящиеся к личности участников и майнеров. Каждый участник имеет идентификатор, состоящий из набора буквенно-цифровых символов, которые выглядят случайными и являются открытым ключом к учетной записи участника. Сама

Electronic copy available at: https://ssrn.com/abstract=3888108

архитектура блокчейна делает идентификаторы видимыми всегда, это необходимо для эффективного функционирования.

При освоении ТРР в госуправлении надо учитывать, что по сути, такие данные невозможно минимизировать в соответствии с законодательством о защите персональных данных, а срок их хранения (обработки) будет совпадать со сроком службы самого блокчейна;

б) дополнительные персональные данные. Помимо идентификатора участников, дополнительные данные, хранящиеся на блокчейне, могут содержать данные персонального характера, а также данные, потенциально относящиеся не к участникам и майнерам.

В отношении таких персональных данных при освоении ТРР в госуправлении следует выбрать способ защиты их конфиденциальности. Здесь возможно несколько вариантов – записывать подобные данные в блокчейн в виде криптографического обязательства, хэш-отпечатка или в зашифрованном (до их введения) виде.

Предпочтительным общим принципом первых двух решений является то, что сами персональные данные хранятся в другом месте, а не в блокчейне как таковом (например, в информационной системе обработчика), а в блокчейне хранится только информация, доказывающая существование данных (криптографическое обязательство, хэш-отпечаток). В принципе, и за пределами блокчейна персональные данные предпочтительнее хранить в зашифрованном виде.

Представленные иллюстрации доказывают, что защита данных в системе распределенного реестра, в том числе в рамках госуправления, требует не только правовых, но и технических мер, а также сочетания технических и правовых средств.

Однако далеко не все риски возможно преодолеть чисто техническими средствами. Здесь нужны и другие решения.

Это утверждение касается, прежде всего, проблемы добросовестности участников сделки (транзакции). Для пояснения обратимся вновь к уже представленному нами кейсу государственной регистрации недвижимости.

Одним из главных рисков участников гражданского оборота является риск приобретения объекта у неуправомоченного отчуждателя. Его можно минимизировать, в том числе, за счет правовой конструкции добросовестного приобретателя - лица, сделавшего все от него зависящее, чтобы убедиться в наличии у отчуждателя права на распоряжение объектом [55].

Стоит упомянуть, что реестр прав на недвижимое имущество изначально формировался для фиксации и передачи прав, а не самих объектов права, так как

Electronic copy available at: https://ssrn.com/abstract=3888108

существование недвижимого имущества и его правообъектность представляют собой объективно существующее явление, а учет и правовая охрана недвижимости связаны исключительно с фактом наличия последней [56]. Добросовестность участников устанавливается через проверку достоверности имеющихся сведений (данных). В юридической литературе отмечена проблема, связанная с достоверностью данных реестра, - это выбор между принципами внесения и противопоставления, различие между которыми заключается в необходимости участникам отношений выяснять сведения о юридических фактах, лежащих за пределами реестра.

Регистрационная система, основанная на принципе внесения, направлена на оптимизацию дополнительных издержек потенциального приобретателя, так как в реестре содержатся все сведения, необходимые для обеспечения действительности перехода права на объект и возможности по заключению сделки. Система противопоставления, в свою очередь, не позволяет субъектам ограничиваться данными, содержащимися в реестре, и вынуждает их дополнительно проверять необходимые сведения, поскольку зарегистрированным в реестре правам могут быть по закону противопоставлены определенные возражения [55].

Проблема заключается в том, что в отечественном правопорядке отсутствует опыт формирования реестров, основанных на принципе внесения, причем наиболее показательным в этом плане является именно реестр прав на недвижимое имущество.

Немаловажен и тот факт, что в современной судебной практике сведениям, содержащимся в реестре недвижимости, не придается решающего значения при определении добросовестности приобретателя. Так, Верховный Суд РФ отметил, что, разрешая вопрос о добросовестности (недобросовестности) приобретателя недвижимости, необходимо учитывать не только его осведомленность о наличии записи в едином государственном реестре, но и была ли проявлена разумная осмотрительность при заключении сделки и какие меры принимались им для выяснения прав лица, отчуждающего это имущество (Обзор судебной практики по делам, связанным с истребованием жилых помещений от добросовестных приобретателей, по искам государственных органов и органов местного самоуправления (утв. Президиумом ВС РФ 01.10.2014)). Таким образом, при обороте недвижимого имущества приобретатели не могут ограничиваться сведениями, содержащими в ЕГРП, а обязаны выяснять и иные обстоятельства, имеющие юридическое значение, что свидетельствует о применении принципа противопоставимости [55].

Одновременно с этим (что парадоксально), одни и те же явления, в частности записи в реестре, обладающие свойством публичной достоверности, стали наделяться в

Electronic copy available at: https://ssrn.com/abstract=3888108

судебной практике различными функциями, значениями и последствиями, что не способствует формальной определенности права. Так, Конституционный Суд РФ отметил, что акт государственной регистрации в отношении объектов исключительных прав может выполнять одновременно как правообразующую, так и правоудостоверяющую функцию [57].

Проблема добросовестного поведения применительно к использованию цифровых технологий уже обсуждается в рамках частного права, в частности, касательно смарт-контрактов. В принципе, включить в компьютерную программу правило о добросовестном поведении можно, но проконтролировать его техническими средствами будет невозможно. Как отмечает А.И. Савельев, компьютер «равнодушен» к основополагающим принципам права, таким как законность, справедливость, защита слабой стороны. Вместо этого основными принципами формирования условий договора становятся определенность и эффективность [58].

Таким образом, в смарт-контракте осуществление прав, исполнение обязанностей происходит с участием компьютерных программ, которые не могут действовать добросовестно или недобросовестно.

В связи с этим действие принципа добросовестности в смарт-контрактах сужается до тех стадий развития правоотношения, в которых непосредственное участие принимают субъекты (преддоговорные контакты, создание программы, внесение в нее данных, момент заключения договора, реализация права на защиту и др.).

Но если вопрос о добросовестности бесполезно ставить по отношению к компьютеру, то само использование цифровых технологий (в нашем случае технологии распределенного реестра), в том числе в государственном управлении, добавляет к проблеме добросовестности еще один уровень.

Речь идет о добросовестности лиц, обслуживающих систему распределенного реестра, в том числе с учетом того, что наряду с государственными структурами это могут быть и частные лица. То есть блокчейн будет обеспечивать государственные цели и задачи, а обслуживать его, хотя бы частично, будут субъекты частного права, не связанные законодательством о государственной службе, нормами о прозрачности и противодействии коррупции (во всяком случае, напрямую и на данный момент).

Соответственно, необходимо распространить принцип добросовестности на особых субъектов – тех специалистов, которые обеспечивают обслуживание системы распределенного реестра, действие технологии смарт-контракта, а также создателей алгоритма. Как правильно замечено, лицо, которое обеспечивает техническое сопровождение договора, имеет возможность внесения ошибок в программный код, что в

Electronic copy available at: https://ssrn.com/abstract=3888108

дальнейшем скажется на правах и обязанностях сторон договорного отношения, к которым применяется смарт-контракт [51].

Во всем мире обслуживание цифровых технологий рассматривается как привлекательная сфера для государственно-частного партнерства, в том числе и в рамках решения задач государственного управления. Так, в настоящее время в Европе большое внимание уделяется внедрению новых законов о данных в рамках общих правил защиты данных. Объединение государственных и частных структур и объединение новых технологий со старой инфраструктурой в рамках коммерческих партнерств и совместных государственно-частных предприятий могут создать сложный комплекс отношений. Несколько поставщиков услуг и систем могут быть вовлечены в разработку, тестирование и внедрение некоторых решений, в то время как взаимодействие с существующей инфраструктурой может создать риск потенциальных правовых пробелов [59]. Очевидно, необходимо распространить принцип добросовестности на всех участников этих отношений.

И еще о двух субъектных «ответвлениях» проблемы добросовестности.

Первое – неоднозначный статус полугосударственных субъектов, до сих пор не решенный в нашем законодательстве. Для нашего исследования он имеет значение постольку, поскольку такие субъекты могут вовлекаться в систему распределенного реестра. Например, в отношении Банка России проблема однозначности правового статуса давно поднимается и в традиционном праве. Он, как известно, не является государственным органом, но занят проведением государственной политики и выполнением государственных функций. Обращалось внимание и на проблемные аспекты деятельности Банка России в вопросах взаимодействия с органами исполнительной власти государства. Для решения проблемы необходимо нормативное закрепление отнесения либо неотнесения субъекта к органам государственной власти, указание на его организационно-правовую форму. Дополнительно это поможет разрешить актуальный вопрос о правовом статусе сотрудников и должностных лиц Банка России [60]. Касательно проблематики распределенных реестров, статус любых его участников должен быть совершенно однозначным.

Второе – вопрос о субъекте, обеспечивающем достоверность сведений реестра. Достоверность классических государственных реестров основывается на том, что организатор реестра является единственным лицом, способным использовать его инструментарий и обладающим контролем над всей системой, что способствует его добросовестному поведению и позволяет участникам оборота полагаться на сведения, предоставленные компетентным субъектом.

Electronic copy available at: https://ssrn.com/abstract=3888108

Но существует и иной вариант обеспечения достоверности сведений. В России он реализован в Единой информационной нотариальной системе, ведение которой осуществляется децентрализованно, посредством внесения различными нотариусами сведений о совершенных лично ими нотариальных действиях. Тем самым, нотариусы призваны удостоверять сведения о фактах, имеющих юридическое значение, и придавать им свойство публичной достоверности. Достоверность сведений, вносимых нотариусами, обеспечивается жестким законодательным регулированием процесса получения статуса нотариуса, а также самой нотариальной деятельности.

Таким образом, использование ТРР в государственном управлении должно учитывать целый ряд уже актуализированных и еще потенциальных проблем, таких как: правовое значение сведений (данных), содержащихся в системе распределенного реестра; порядок и условия взаимодействия между организаторами и пользователями реестра; проблема установления правового статуса лица, обеспечивающего техническое сопровождение смарт-контракта, обязательного лицензирования программного обеспечения и оборудования, используемых для функционирования распределенного реестра и др.

Важно подчеркнуть, что практически невозможно (фактически и технически) проконтролировать качество и достоверность данных, вводимых в систему распределенного реестра. Частично достоверность может быть обеспечена через испытанные правовые конструкции добросовестности и судебной защиты нарушенных прав.

Оценивая перспективы применения распределенных реестров в государственном управлении, отметим инновационную (новаторскую) функцию правового риска - риск мотивирует на поиск новых решений, становится катализатором положительных изменений в правовой среде, повышает эффективность принятых решений.

В данном контексте уместно привести в пример цифровизацию юридического мира, портал госуслуг, многофункциональные центры. Конечно, претворение в жизнь идеи о создании быстрого и удобного электронного документооборота – затратная цель, которая, несмотря на риск, с лихвой себя оправдывает [61].

В целом, необходим разумный прагматичный подход к использованию цифровых технологий, в том числе блокчейна, в государственном управлении. Блокчейн, конечно, инновация, но излишнее увлечение инновациями не должно наносить урон ни государственным целям, ни правам человека. Нет смысла вводить блокчейн там, где без него можно не просто обойтись, но и обойтись лучшим образом и дешевле. Представляется, что при выборе следует помнить о преимуществе распределенного

Electronic copy available at: https://ssrn.com/abstract=3888108

реестра (на блокчейне) перед бумажным или электронным – при искажении информации (намеренном или случайном) ее довольно трудно, а иногда и невозможно восстановить. Реестр, основанный на блокчейне, позволяет хранить всю информацию у всех пользователей (разумеется, заинтересованных в ее сохранении) [49], а потому решает обозначенную проблему и обеспечивает надежное хранение данных.

Как мы показали в исследовании, преимущества блокчейна в чистом виде (открытого) значительно повышают его привлекательность, но не подходят для использования государством.

Чтобы не «уравнивать» закрытый блокчейн с традиционным вертикальным управлением, допустимо сочетание эксклюзивных и общедоступных типов блокчейна. Пример тому содержат предложения по регистрации результатов интеллектуальной деятельности: «предварительная регистрация изобретений, полезных моделей и промышленных образцов может осуществляться в открытом общедоступном блокчейне с целью обозначения приоритета, а официальная регистрация будет завершаться внесением сведений уже в государственный реестр на платформе эксклюзивного блокчейна» [49]. По аналогии, сфера применения таких сочетаний может быть расширена, в том числе за счет государственного управления.

В целом применение технологий распределенного реестра (в частности, в формате блокчейна) в государственном управлении имеет несомненные перспективы. Наше предыдущее исследование 2019 года показало, что ТРР может применяться при осуществлении любой государственной функции.

В частности, нами были предложены следующие критерии применения ТРР в государственном управлении.

1) Общие критерии в оценке применения ТРР в государственном управлении:

а) преобладание преимуществ использования технологии над затратами на ее внедрение;

б) необходимость реализации в государственном управлении распределения (как главной черты ТРР) и прозрачности;

в) необходимость неизменности записей в реестре;

г) достаточное сочетание особенностей технологии с правовыми нормами, гуманитарными принципами, кодексами поведения;

д) способствование применения ТРР осуществлению качественного (надлежащего) государственного управления.

2) Частные критерии для применения ТРР в государственном управлении:

а) низкий уровень прозрачности (транспарентности) исполнения государственной

Electronic copy available at: https://ssrn.com/abstract=3888108

функции;

б) высокий уровень коррупции при исполнении государственной функции;

в) высокие издержки на исполнение государственной функции;

г) низкий уровень доверия граждан к государственной функции;

д) длительные сроки исполнения государственной функции;

е) сложность организационной структуры исполнения государственной функции (множество задействованных структур, разноуровневость и неоднородность структур, проблемы информационного и финансового взаимодействия между ними).

Учет изложенных критериев показывает особую потенциальную эффективность применения ТРР в тех областях, где исполнение государственной функции затрагивает деятельность как государственных, так и частных субъектов (например, когда частные субъекты привлечены к исполнению государственной функции и получают соответствующее финансирование из бюджета).

С правовой точки зрения особенно ценны такие свойства ТРР, как неизменность записей и технически контролируемое согласие на транзакцию.

К примеру, одной из наиболее перспективных сфер для применения ТРР является, на наш взгляд, сфера ЖКХ. Действительно, если блокчейн-платформа уже используется для обеспечения потребителей правдивой информацией о качестве продукции (например, при производстве кур в Оверни посредством блокчейна заполняется вся история их жизни – иформация о сроке выращивания, потребляемом корме и ветеринарной помощи, оказанной курам), неужели такая же степень прозрачности не будет востребована в российском ЖКХ?

В развитие предложенной нами по результатам НИР 2019 года концепции развития правовых оснований использования технологии распределенного реестра в государственном управлении, представляется возможным сформулировать систему критериев обоснованности применения ТРР в государственном управлении:

1) критерий практической востребованности – переход к децентрализованным государственным реестрам обоснован, если их ведение и использование затрагивает одновременную реализацию прав значительного количества негосударственных субъектов (граждан и организаций) – например, реестр объектов недвижимого имущества;

2) критерий оптимизации административных процедур – внедрение ТРР позволит оптимизировать административные процедуры (сократить сроки, количество согласований, повысить прозрачность);

Electronic copy available at: https://ssrn.com/abstract=3888108

3) критерий потенциального повышения качества государственного управления – освоение ТРР позволит уменьшить необоснованное государственное вмешательство, повысить результативность и эффективность государственного управления;

4) критерий финансовой перспективности – внедрение ТРР позволит сократить издержки на выполнение государственной функции (в будущем);

5) критерий организационной многосложности – в исполнении государственной функции задействовано множество разноподчиненных субъектов с несовпадающими правовыми статусами;

6) критерий смешанности правового регулирования – система ТРР строится для обслуживания преимущественно гражданско-правовых отношений, контролируемых государством, и предполагает использование смарт-контрактов;

7) критерий коррупциогенности отношений – блокчейн, обеспечивая неизменность записей в реестре, помогает нивелировать коррупционные риски в особо коррупциогенных областях (как государственные закупки, управление государственным имуществом).

Полагаем, что в каждом конкретном случае должно присутствовать как минимум четыре (то есть больше половины) из сформулированных критериев.

В результате состоявшегося исследования правовых рисков от использования ТРР в государственном управлении можно сформулировать следующие предложения по их преодолению.

1) Для преодоления компетенционных рисков необходимо предпринять следующие меры:

- прежде всего, стоит определиться (возможно, нормативно) с выбором типа применяемого блокчейна. Абсолютное большинство экспертов сходится в том, что для нужд государственного управления подходит закрытый или консорциумный типы блокчейна, что, впрочем, не исключает для «обслуживания» реализации государственной функции применения сочетаний разных типов блокчейна (в том числе и открытого блокчейна для какой-либо части процесса). При этом за государственным органом, как правило, закрепляется роль валидатора;

- необходимо четко определить права и обязанности (компетенции) всех участников блокчейна в зависимости от выполняемых ими ролей. Это означает:

а) закрепление в нормативно определяемых статусах органов государственной власти и должностных инструкциях государственных служащих возможность и правила выполнения функций посредством технологии распределенного реестра;

Electronic copy available at: https://ssrn.com/abstract=3888108

б) определение формы легализации участия негосударственных субъектов в реализации государственных функций посредством ТРР (полугосударственные, частные субъекты, начиная от разработки алгоритма до обслуживания системы), для чего предпочтительно сочетание нормативного регулирования, учитываемого техническими протоколами, с административными договорами;

в) четкое определение как в целом, так и в каждом конкретном случае, за кем (кеми) закрепляется статус обработчика персональных данных;

- соотнести компетенционные риски с проблемой информационной безопасности, путем:

а) дифференциации режимов доступа к данным, содержащимся в реестре, по формам и объему в зависимости от компетенции субъекта, должностного лица, наличия или отсутствия у него статуса валидатора;

б) обеспечения интероперабельности данных в системе распределенного реестра;

в) особого статуса данных (части данных), идентифицируемых как тайна (государственная, профессиональная и пр.);

- разработать систему разрешения конфликтов (споров) между участниками, которую можно заложить при разработке алгоритма (а), определив компетентный суд (б), создав независимый орган (в). Возможно и сочетание этих способов.

2) Для преодоления рисков нарушения прав человека необходимо:

- четко определить необходимость идентификации участников (система распределенного реестра, создаваемая в целях государственного управления, по общему правилу, не приемлет анонимности). Кроме того, во вносимых данных будет большая доля персональных данных граждан. Соответственно, возникает неминуемый риск нарушений в области обработки персональных данных. Для его избежания необходимо:

а) создать многозвенную систему контроля за обработкой персональных данных, которая включает в себя непосредственного обладателя данных, обработчика персональных данных, инспектора (контролера) за обработкой персональных данных, а также независимого органа, осуществляющего контроль за обработкой персональных данных;

б) провести (в соответствии европейской рекомендацией) предварительную оценку обеспечения защиты персональных данных на этапе введения системы распределенного реестра в эксплуатацию;

в) ввести сертификацию соответствия системы стандартам конфиденциальности данных;

Electronic copy available at: https://ssrn.com/abstract=3888108

- дифференцировать принципы обработки персональных данных в зависимости от того, относятся ли они к идентификаторам участников или нет. Идентификаторы участников и майнеров вряд ли удастся обеспечить всей полагающейся по законодательству защитой персональных данных, поскольку их видимость есть суть работы РР. Соответственно, срок хранения таких данных будет равен сроку службы блокчейна. Что же касается других персональных данных участников, необходимо обеспечить конфиденциальность содержащихся в реестре персональных данных путем их шифрования до внесения, хранения за пределами блокчейна, введения в систему посредством хэш-отпечатка или в виде криптографического обязательства (возможно сочетание этих способов);

- определить способ реализации права на забвение в распределенном реестре. Для этого должен быть определен ответственный за обработку персональных данных (который, к тому же, осуществляет контроль за локализацией майнеров), выбран приемлемый способ исправления шибки в каждой конкретной системе распределенного реестра – например, посредством внесения изменений в последующий блок, а также определена возможность синхронизации исправления ошибки в других транзакциях (сделках) данной системы распределенного реестра (а возможно, и других с ней связанных). Для распределенных реестров, обслуживающих государственное управление, целесообразно сделать обязательным не просто сохранение внесенных данных в неизменном виде (что и так обеспечено самой системой РР), но и обязательное проставление меток времени, чтобы точно датировать все вносимые изменения и было бы невозможно скрыть внесенные искажения;

- комплексно обеспечить реализацию права на судебное обжалование действий органов власти и участников системы, не являющихся органами власти, путем:

а) установления материальных оснований для последующего определения предмета иска и определения надлежащего ответчика;

б) установления такого правила, в рамках которого досудебная (внесудебная) защита может предоставляться только в отношении прав, которые не связаны с внесением изменений в реестры, а защита прав, связанных с внесением изменений в реестры, осуществляется только в судебном порядке;

в) предоставления судам возможности вынесения решения о внесении изменений в соответствующий распределенный реестр;

г) определения порядка исполнения судебных решений о внесении изменений в реестр. Все это потребует значительной модификации процессуального законодательства.

Electronic copy available at: https://ssrn.com/abstract=3888108

3) Преодоление рисков непризнания юридической значимости транзакций (сделок) и документов. Данные риски в большой степени могут быть преодолены техническими способами, например, все, что касается формальных требований к документам и сделкам (техническая стандартизация форматов документов и их форм, а также протоколов обмена таких документов). Помимо этого, необходимо:

- обеспечить безопасность системы распределенного реестра путем:

а) введения обязательной сертификации системы распределенного реестра до ввода ее в эксплуатацию;

б) введения требований к устройствам, которые будут применяться при использовании технологии распределенного реестра в государственном управлении;

в) осуществления периодического контроля (мониторинга, аудита) за использованием системы распределенного реестра, в том числе независимого;

- создать все правовые условия для обеспечения подлинности цифровой подписи, за счет унификации:

а) требований к цифровым подписям, использование которых возможно в системе распределенного реестра;

б) сокращения количества удостоверяющих центров (в идеале – до одного-двух, но с учетом масштабов страны возможно одного на регион);

- обеспечить добросовестность участников сделок (транзакций). В данной ситуации технические меры не срабатывают, поэтому остаются механизмы традиционного права (например, презумпция добросовестности приобретателя). Также должна быть обеспечена добросовестность персонала, обсуживающего реестр, диапазон предлагаемых мер – от нормативных (требования к компетенции и ответственности) до морально-этических (кодексы поведения);

- нейтрализовать возможное недоверие к документам и транзакциям, зафиксированным посредством ТРР. Способы разрешения данной проблемы лежат во многом за пределами техники и права, в числе мер по цифровому воспитанию. Однако право также располагает механизмом «постепенной» модификации правового сознания, например, путем введения типового условия сделки о признании как транзакции, так и связанных с ней документов, сформированных посредством ТРР. В крайнем настойчивом варианте возможно введение такого правила на нормативном уровне (что нежелательно с точки зрения общественного мнения).

Большинство предложенных способов преодоления правовых рисков являются правовыми. Однако, и это характерная черта регулирования технологий, многие способы

Electronic copy available at: https://ssrn.com/abstract=3888108

являются техническими по природе. Особое внимание должно уделяться разумному и скоординированному сочетанию правовых и технических способов преодоления рисков.

Electronic copy available at: https://ssrn.com/abstract=3888108

ЗАКЛЮЧЕНИЕ

Объектом настоящего исследования являются правовые отношения, связанные с применением технологии распределенного реестра (ТРР) в государственном управлении. В процессе научного исследования были выявлены и проклассифицированы правовые риски при использовании ТРР, в том числе и прежде всего в формате блокчейна, в государственном управлении.

Изучены подходы к систематизации правовых рисков общего характера, представленные в научной литературе, проведен анализ выявленных учеными рисков в различных сферах, что позволило провести классификацию правовых рисков от использования блокчейн в госуправлении.

Первую группу рисков образуют общие правовые риски применительно к блокчейну в госуправлении, связанные с процессами правоустановления, к ним относены:

1) Риск попадания «вне правовое поле» ввиду общей неурегулированности блокчейна как прорывной технологии.

2) Риск снижения государственного регулирования блокчейна или даже полного отказа от государственного (нормативного) регулирования. Как следствие - риск утраты значения государственных органов.

3) Риск смешения публичного и частного начала в государственном управлении.

4) Риск применения частного права к публично-правовым отношениям.

Вторую группу рисков образуют специальные риски, возникающие непосредственно в связи с использованием блокчейна в госуправлении – создание и реализацию неоднозначных правовых режимов и правовых статусов в отношении объектов и субъектов государственного управления, а также девиантное поведение. Это:

1) Риск нарушения компетенции государственных органов и полномочий негосударственных субъектов (компетенционный риск).

2) Риск нарушений фундаментальных прав человека (право на защиту персональных данных, право на забвение, право на судебное обжалование решений органов власти).

3) Риск непризнания юридической значимости транзакций (сделок) и документов, сгенерированных в результате действий на базе блокчейна.

Также в ходе исследования проанализированы права, обязанности и ответственность участников блокчейна в государственном управлении, что необходимо для выявления правовых рисков компетенционного характера.

В результате исследования сформулирована система критериев обоснованности применения ТРР в государственном управлении:

Electronic copy available at: https://ssrn.com/abstract=3888108

1) Критерий практической востребованности – переход к децентрализованным государственным реестрам обоснован, если их ведение и использование затрагивает одновременную реализацию прав значительного количества негосударственных субъектов (граждан и организаций) – например, реестр объектов недвижимого имущества.

2) Критерий оптимизации административных процедур - внедрение ТРР позволит оптимизировать административные процедуры (сократить сроки, количество согласований, повысить прозрачность).

3) Критерий потенциального повышения качества государственного управления – освоение ТРР позволит уменьшить необоснованное государственное вмешательство, повысить результативность и эффективность государственного управления.

4) Критерий финансовой перспективности – внедрение ТРР позволит сократить издержки на выполнение государственной функции (в будущем).

5) Критерий организационной многосложности – в исполнении государственной функции задействовано множество разноподчиненных субъектов с несовпадающими правовыми статусами.

6) Критерий смешанности правового регулирования – система ТРР строится для обслуживания преимущественно гражданско-правовых отношений, контролируемых государством, и предполагает использование смарт-контрактов.

7) Критерий коррупциогенности отношений – блокчейн, обеспечивая неизменность записей в реестре, помогает нивелировать коррупционные риски в особо коррупциогенных областях (как государственные закупки, управление государственным имуществом).

Для подтверждения обоснованности внедрения ТРР в каждом конкретном случае должно присутствовать как минимум четыре (то есть больше половины) из сформулированных критериев.

В результате состоявшегося исследования правовых рисков от использования ТРР в государственном управлении сформулированы конкретные предложения по их преодолению.

Результаты данного исследования могут быть использованы в интересах Министерства экономического развития; Министерства цифрового развития, связи и массовых коммуникаций; Евразийской экономической комиссии, для научно-методологического обоснования правового обеспечения внедрения технологии распределенного реестра в процесс государственного управления.

Electronic copy available at: https://ssrn.com/abstract=3888108

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Batubara F. R., Ubacht J., Janssen M. Challenges of Blockchain Technology Adoption for e-Government: A Systematic Literature Review//Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age. - May 2018. - Article N 76. - P.1-9.

2. Тихомиров Ю.А. Право: прогнозы и риски. - М.: Инфра-М, 2015. - 240 с.

3. Риски финансовой безопасности: правовой формат: монография/О.А. Акопян, С.Я. Боженок, О.В. Веремеева и др.; отв. ред. И.И. Кучеров, Н.А. Поветкина. - М.: ИЗиСП, НОРМА, ИНФРА-М, 2018. - 304 с.

4. Южаков В.Н., Талапина Э.В., Добролюбова Е.И., Тихомиров Ю.А. Инициативный проект закона об обеспечении качества государственного управления. - М.: Издательский дом «Дело» РАНХиГС, 2020. - 150 с.

5. Australian Bitcoin mining firm Bitcoin Group to go public on the ASX in November. – URL :http://siliconangle.com/blog/2015/09/08/australian-bitcoin-mining-firm-bitcoin-group-to-go-public-on-the-asx-in-november/ (дата обращения 12.05.2020).

6. Välikangas L. Put Your Head on a Blockchain? A Few Notes on the Emergence of Blockchain Technologies. *Management and Organization Review*. - February 2020. - № 16:1. - PP. 199-201.

7. Кто контролирует Bitcoin. На нескольких адресах находятся 55% всех монет. - URL: https://www.rbc.ru/crypto/news/5ba10e5c9a7947709b05d131 (дата обращения 12.05.2020).

8. Чаннов С.Е. Правовые угрозы при использовании информационных систем в государственном управлении//Административное право и процесс. - 2018. - № 9. - С. 48-54.

9. Савельев А.И. Электронная коммерция в России и за рубежом: правовое регулирование. 2-е изд. - М.: Статут, 2016. - 640 с.

10. Криптовалюты и блокчейн как атрибуты новой экономики. Разработка регуляторных подходов: международный опыт, практика государств – членов ЕАЭС, перспективы для применения в Евразийском экономическом союзе. - М.: ЕАЭК, 2019. - 90 с.

11. Черепнёв М.А. Блокчейн и протокол коллективной подписи//International Journal of Open Information Technologies. - 2019. - № 6. - С. 17-23.

12. Горькова Е.В. Правовые риски в теории и практике государственного и муниципального управления//Юридическая техника. - 2019. - № 13. - С. 665-667.

Electronic copy available at: https://ssrn.com/abstract=3888108

13. MyungSan Jun Blockchain government - a next form of infrastructure for the twenty-first century//Jun Journal of Open Innovation: Technology, Market, and Complexity. - 2018. - PP. 1-12.

14. Maisie Borrows M., Harwich E., Heselwood L. The future of public service identity: blockchain//URL: https://reform.uk/research/future-public-service-identity-blockchain (дата обращения 13.05.2020).

15. Schwabe G. The role of public agencies in blockchain consortia: Learning from the Cardossier//Information Polity. 2019. – № 24 (4). - PP. 437-451.

16. Bauer, I., Zavolokina, L., & Schwabe, G. Is there a market for trusted car data? Electronic Markets. - URL: https://doi.org/10.1007/s12525-019-00368-5 (дата обращения 23.05.2020).

17. Klievink, B., Bharosa, N., & Tan, Y. H. The collaborative realization of public values and business goals: Governance and infrastructure of public–private information platforms//Government Information Quarterly. - 2016. - № 33 (1). - PP. 67-79.

18. Xu X., Pautasso C., Zhu L., Gramoli V., Ponomarev A., Tran A.B.&Chen S. The blockchain as a software connector. *13th Working IEEE/IFIP Conference on Software Architecture (WICSA)*. - 2016. - PP. 182-191.

19. Оракул. - URL: https://ru.bitcoinwiki.org/wiki/%D0%9E%D1%80%D0%B0%D0%BA%D1%83%D0%BB (дата обращения 13.05.2020).

20. Доклад о цифровой экономике «Создание стоимости и получение выгод: последствия для развивающихся стран»: обзор // ЮНКТАД. ООН. Женева. - 2019. - 31 с.

21. Петров М., Буров В., Шклярук М., Шаров А. Государство как платформа. (Кибер)государство для цифровой экономики. Цифровая трансформация // Центр стратегических разработок. – М., 2018. - 53 с.

22. Почему Китай взял на вооружение блокчейн и как он используется в России. - URL: https://rg.ru/2020/04/28/pochemu-kitaj-vzial-na-vooruzhenie-blokchejn-i-kak-on-ispolzuetsia-v-rossii.html (дата обращения 13.05.2020).

23. Поручение Председателя Правительства Дмитрия Медведева по вопросу о возможности применения технологии блокчейн в системе государственного управления и экономике Российской Федерации от 6 марта 2017 года. - URL: http://government.ru/orders/selection/401/26653/ (дата обращения 13.05.2020).

24. Михайлов С.В., Пономарева Н.В. Блокчейн в современном правоприменении//Философия права. - 2019. - № 1. - С. 60-64.

Electronic copy available at: https://ssrn.com/abstract=3888108

25. Бегларян М.Е., Добровольская Н.Ю. Блокчейн-технология в правовом пространстве//Вестник Краснодарского университета МВД России. - 2018. - № 2. - С.108-112.

26. Warkentina M., Orgeronb C. Using the security triad to assess blockchain technology in public sector applications. - URL: https://www.sciencedirect.com/science/article/abs/pii/S026840121930060X?via%3Dihub#abs0005 (дата обращения 12.05.2020).

27. Косян Н.Г., Милькина И.В. Блокчейн в системе государственных закупок//E-Management. - 2019. - № 1. - С. 33-41.

28. Bouhadana I. Le droit au respect de la vie privée à l'ère du numérique dans le système français//Эволюция государственных и правовых институтов в условиях развития информационного общества. - М.: Юркомпани, 2012. - С.135-153.

29. Pailler L. Les réseaux sociaux sur internet et le droit au respect de la vie privée. *Paris, Larcier*. - 2012. - 222 p.

30. Eur. Court H.R. NIEMIETZ v. GERMANY. - Application no. 13710/88. Judgment of - 16 December 1992. - Para. 29.

31. Eur. Court H.R. COPLAND v. THE UNITED KINGDOM. - Application no. 62617/00. - Judgment of 03 April 2007. - Para 41.

32. Директива Европейского парламента и Совета Европейского союза от 15 декабря 1997 г. № 97/66/ЕСи // Сборник документов Совета Европы в области защиты прав человека и борьбы с преступностью. - М.,1998. - 388 с.

33. Федеральный закон от 19 декабря 2005 года № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» – URL: http://www.consultant.ru/document/cons_doc_LAW_57153/ (дата обращения 10.10.2020).

34. Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных». URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения 10.10.2020).

35. Федеральный закон от 02 июля 2013 года № 142-ФЗ «О внесении изменений в подраздел 3 раздела I части первой Гражданского кодекса Российской Федерации». - URL: http://www.consultant.ru/document/cons_doc_LAW_148454/ (дата обращения 10.10.2020).

36. Приказ Роскомнадзора от 30 мая 2017 года № 94 «Об утверждении методических рекомендаций по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные

Electronic copy available at: https://ssrn.com/abstract=3888108

сведения». - URL: http://www.consultant.ru/document/cons_doc_LAW_223376/ (дата обращения 10.10.2020).

37. Савельев А.И. Проблемы применения законодательства о персональных данных в эпоху «Больших данных» (BIG DATA) // Право. Журнал Высшей школы экономики. - 2015. - № 1. - С. 43-66.

38. Thouvenin F., Hettich P., Burkert H., Gasser U. Remembering and Forgetting in the Digital Age. *Springer*. - 2018. - 274 p.

39. Статья 17. Право на удаление («право на забвение»). – URL: http://base.garant.ru/71936226/a7b26eafd8fd23d18ca4410ac5359e0e/#ixzz6btN4S1Nf (дата обращения 09.09.2020).

40. Карлаш Д.С. Права в области использования больших пользовательских данных//Предпринимательское право. Приложение «Право и Бизнес». - 2020. - № 1. - С. 46-48.

41. Определение Конституционного Суда РФ от 24 января 2006 года № 3-О по жалобе А.П. Коженова на нарушение его конституционных прав положениями п. 1 ч. 1 ст. 134 ГПК РФ, Определение Конституционного Суда РФ от 20 октября 2005 г. № 513-О по жалобе В.Ф. Шалота на нарушение его конституционных прав положениями п. 1 ч. 1 ст. 134 ГПК РФ // Доступ из справочно-правовой системы «КонсультантПлюс».

42. Лоренц Д.В. Цифровые права в сфере недвижимости: юридическая природа и способы защиты//Российская юстиция. - 2020. - № 2. - С. 57 - 60.

43. Трубин Е.М. Понятие официального документа как предмета преступления против порядка управления // Законы России: опыт, анализ, практика. - 2018. - № 5. - С. 81-85.

44. Стяжкина С.А. Официальный документ как предмет служебного подлога: понятие, признаки, виды // Вестник Удмуртского ун-та. Серия «Экономика и право». - 2014. - № 2. - URL: http://cyberleninka.ru/article/n/ofitsialnyy-dokument-kak-predmet-sluzhebnogo-podloga-ponyatie-priznaki-vidy (дата обращения 10.10.2020).

45. Обзор практики рассмотрения ФТС России жалоб физических и юридических лиц на решения, действия (бездействие) таможенных органов в области таможенного дела, направленного Письмом ФТС России от 30 декабря 2011 года N 01-11/65437. - URL: http://www.consultant.ru/document/cons_doc_LAW_143880/ (дата обращения 10.10.2020).

46. Постановление Президиума Высшего арбитражного Суда РФ от 12 ноября 2013 года № 18002/12. - URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=ARB&n=386688#07603294618748386 (дата обращения 10.10.2020).

Electronic copy available at: https://ssrn.com/abstract=3888108

47. Определение Верховного Суда РФ от 15 августа 2016 года № 303-ЭС16-6907. - URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=ARB&n=470926#009995205748736646 (дата обращения 10.10.2020).

48. Наджарян Р.В. Проблемы обеспечения юридической силы документа в условиях применения информационных технологий//Правовые вопросы связи. - 2010. - № 1. - С. 22-28.

49. Чаннов С.Е. Использование блокчейн-технологий для ведения реестров в сфере государственного управления//Административное право и процесс. - 2019. - № 12. - С. 29-34.

50. Соколова М.А. Дефекты юридических документов: монография. - М.: Юриспруденция, 2016. - 160 с.

51. Волос А.А. Реализация принципа добросовестности применительно к отношениям сторон смарт-контракта // Право и цифровая экономика. - 2020. - № 2. - С. 26-31.

52. Постановление Конституционного Суда РФ от 22 июня 2010 года № 14-П «По делу о проверке конституционности подпункта «а» пункта 1 и подпункта «а» пункта 8 статьи 29 Федерального закона «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации» в связи с жалобой гражданина А.М. Малицкого». – URL: http://www.consultant.ru/document/cons_doc_LAW_101794/ (дата обращения 10.10.2020).

53. Постановление Конституционного Суда Российской Федерации от 13 июля 2010 года № 16-П «По делу о проверке конституционности положений статей 6 и 7 Закона Краснодарского края «Об организации транспортного обслуживания населения таксомоторами индивидуального пользования в Краснодарском крае» в связи с жалобой граждан В.А. Береснева, В.А. Дудко и других». – URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=ARB&n=155161#021567963618326629 (дата обращения 10.10.2020).

54. Попова Н.Ф. Необходимость цифровизации государственного управления в РФ//Административное право и процесс. - 2020. - № 2. - С. 48-53.

55. Новоселова Л.А., Полежаев О.А. Правовые риски совершения сделок с объектами интеллектуальных прав на цифровых платформах // Закон. - 2019. - № 10. - С. 90-99.

56. Ершов О.Г., Бетхер В.А. К вопросу о правовой природе самовольной постройки//Право и экономика. - 2015. - № 4. - С. 37-41.

Electronic copy available at: https://ssrn.com/abstract=3888108

57. Постановление Конституционного Суда Российской Федерации от 3 июля 2018 г. № 28-П «по делу о проверке конституционности пункта 6 статьи 1232 Гражданского кодекса Российской Федерации в связи с запросом Суда по интеллектуальным правам». - URL: https://rg.ru/2018/07/10/intellektprava-dok.html (дата обращения: 03.09.2020).

58. Савельев А.И. Договорное право 2.0: «умные» контракты как начало конца классического договорного права//Вестник гражданского права. - 2016. - № 3. - С. 32-60.

59. Есаян А.К., Трунцевский Ю.В. Общие подходы к нормативному правовому регулированию технологии в сфере «Умный город» // Международное публичное и частное право. - 2020. № 1. - С. 36-41.

60. Осколкова Н.А. Теоретические и практические аспекты взаимодействия Банка России и органов исполнительной власти Российской Федерации//Административное право и процесс. - 2017. - № 7. - С. 76-79.

61. Ревина С. Н., Паулова Е. О. К вопросу о функциях риска в праве // Российская юстиция. - 2019. - № 12. - С. 51-54.

Electronic copy available at: https://ssrn.com/abstract=3888108