ТЕХНОЛОГИИ ИНТЕРНЕТ ВЕЩЕЙ И ПЕРСОНАЛЬНЫЕ ДАННЫЕ: ВОПРОСЫ ПРАВА СОБСТВЕННОСТИ

Эгамбердиев Эдуард Хажибаевич
И.о. доцента кафедры Гражданского права Ташкентского государственного юридического университета, доктор философии (PhD) по юридическим наукам

АННОТАЦИЯ

В этой статье анализируются, определяются и уточняются понятия собственности и персональных данных для изучения их совместимости в контексте европейского права. В работе критически рассматривается традиционная разделительная линия между персональными и не персональными данными и приводятся доводы в пользу строгого концептуального их отделения. Также рассматривается возможность применения понятия права собственности к персональным данным в контексте Интернета вещей (IoT).

Ключевые слова: *персональные данные, персональная информация, не персональные данные, данные, информация, владение, Интернет вещей, право ЕС, GDPR, право собственности.*

INTERNET OF THINGS AND PERSONAL DATA: ISSUES OF PROPERTY RIGHTS

Egamberdiev Eduard Khajibaevich
And about. Associate Professor of the Department of Civil Law of the Tashkent State University of Law, Doctor of Philosophy (PhD) in Legal Sciences

ABSTRACT

This article analyzes, defines and refines the concepts of property and personal data in order to study their compatibility in the context of European law. The paper takes a critical look at the traditional dividing line between personal and non-personal data and argues for a strict conceptual separation. The possibility of applying the concept of ownership to personal data in the context of the Internet of things (IoT) is also considered.

Key words: *personal data, personal information, non-personal data, data, information, ownership, Internet of Things, EU law, GDPR, property rights.*

ВВЕДЕНИЕ

Технологии Интернет вещей (the Internet of Things – IoT) становятся все более распространенными. Только в 28 странах ЕС оценочное количество подключенных «вещей» составляло 1,8 миллиарда в 2013 году и, как ожидалось, достигает 6 миллиардов к 2020 году [1]. Эти так называемые «умные» устройства будут способствовать нашему взаимодействию с окружающей средой, например, облегчая транспорт и логистику, а также предоставление таких услуг, как здравоохранение и безопасность. В то же время устройства IoT генерируют и собирают множество персональных данных, управление которыми вызывает серьезные этические [2] и юридические [3] вопросы. Право собственности на персональные данные лежит в основе вопросов, связанных с управлением и контролем данных, таких как конфиденциальность, доверие [4] и безопасность, а также имеет важные последствия для будущего «цифровой» экономики и торговли данными [5]. Введение концепции владения данными в качестве законного права недавно появилось на уровне ЕС [6] и за его пределами.

После принятия в ЕС Общего регламента по защите данных (General Data Protection Regulation – GDPR), стало невозможно думать о праве собственности на персональные данные. Однако проблема заключается в том, что грань между персональными и не персональными данными является движущейся мишенью, и данные, которые сейчас рассматриваются как не персональные данные, в будущем могут стать (благодаря аналитическим и технологическим достижениям) персональными [7]. Таким образом, изучение концептуальных ограничений владения персональными данными должно предшествовать обсуждению права собственности на данные, не являющиеся персональными (например, данные, используемые в интеллектуальном сельском хозяйстве) [8]. Фактически, персональные данные уже признаны одним из ключевых экономических активов [9], и таким образом, вопросы, касающиеся их собственности, проблематичны даже в свете этих экономических тенденций. Более того, необходимость анализа вытекает из природы мира IoT, в котором многие из нас уже живут. Возьмем, к примеру, «умные города», где компании, работающие с большими данными, вскоре смогут приватизировать данные (включая персональные данные), несмотря на то, что они в основном собираются без предварительного согласия субъектов персональных данных. [10] В ответ на эти вызовы ряд владельцев разрабатывают технологические решения. Одним из таких примеров является платформа AURA – система управления персональной информацией (Personal Information Management

system – PIM) [11], недавно представленная компанией Telefónica в Испании и в отличие от тенденций в «умных» городах, позволяет конечным пользователям контролировать соответствующие данные, которые их оператор мобильной связи хранит у себя (например, геолокацию пользователя) и решает, кому эти данные будут переданы [12].

ЛИТЕРАТУРНЫЙ ОБЗОР И МЕТОДЫ

Вопросами персональных данных, вещного права, в частности проблемы права собственности, нематериальные блага и ответственность за причинение вреда, а также специальными вопросами в виртуальном мире рассматривались некоторыми учеными-цивилистами Республики Узбекистан, среди которых следует выделить О. Окюлова [13, 14], Д.М. Караходжаеву [15, 16], К.М. Мехмонова [17-24], Л.М. Бурханову [25-30], У.Ш Шарахметову [31], Н.А. Кулдашева [32-38]. По данной теме мною также были изучены некоторые вопросы Интернета вещей, виртуальных объектов и их реализации [39-41].

Специальные вопросы Интернета вещей, их статус, персональные данные и проблемы их регулирования, право собственности и его положения применительно к персональным данным, а также некоторые отношения, возникающие при использовании Интернет вещей и охрана персональных данных рассматривались рядом зарубежных ученых, среди которых следует выделить S. Aguzzi, J. Van den Hoven, J. Drexl, M. Taddeo, C. Bartolini, C. Santos, C. Ullrich, F Thouvenin, R.H. Weber, A. Früh, C. Wendehorst, S. Wolfert, L Edwards, L Floridi, G. Malgieri, N. Purtova, M. Katz, P. De Hert, N. Ambika, M. Sujaritha, S. Sicari, F. Costa-Cabral, O. Lynskey, J. Kang, B. Buchner, S. Tyagi, A. Darwish, M.Y. Khan.

В ходе исследования были применены общенаучные методы познания, такие как анализ, синтез, индукция, дедукция, исторический метод, метод сравнения, системно-структурный и другие методы.

ОБСУЖДЕНИЕ И РЕЗУЛЬТАТЫ

Персональные данные юридически определены в статье 4 (1) GDPR следующим образом: «Персональные данные» означают любую информацию, относящуюся к идентифицированному или идентифицируемому физическому лицу («субъекту данных»).

Это определение иллюстрирует скользкий язык в отношении персональных данных. С одной стороны, GDPR явно желает «усилить контроль (физического лица) над его собственными данными», тем самым сделав шаг к

тому, чтобы «субъекты данных» по умолчанию владели своими личными данными. С другой стороны, персональные данные также упоминаются в GDPR как «личная информация» или просто как «информация».

Концептуальное различие между данными и информацией имеет решающее значение, когда речь идет о владении персональными данными, а не относящийся к физическому лицу. Однако такое понимание упускает из виду данные и информацию – это два разных понятия. Представьте себе камень с египетскими иероглифами. До открытия Розеттского камня одно и то же письмо представляло бы все данные, но не сообщало бы читателю никакой значимой информации [42]. В данном сценарии данные представлены иероглифами, и как таковые они являются источником информации, в зависимости от того, как мы их интерпретируем.

Таким образом, не существует информации без данных. Это означает, что нам не нужно понимать информацию, которую могут передавать любые данные, чтобы обращаться с данными как с активом, из которого в будущем может быть извлечена ценная информация.

Однако в дебатах о владении данными отсутствует четкое концептуальное различие между данными и информацией. [43] Юридические дебаты строятся на связанном, но концептуально очень четком различии между формой (обычно цифровой), в которой информация воплощена, и значением, содержащимся в ней. Это различие недавно было описано как различие между синтаксическим уровнем информации (формой) и семантическим уровнем информации (значением). Для целей обсуждения владения данными этот подход не может обеспечить желаемый уровень ясности, хотя, потому что он путает синтаксическую информацию с данными.

Одни и те же данные могут быть проанализированы неограниченное количество раз, и этот факт вызвал опасения, что данные, собранные в средах IoT, могут в конечном итоге раскрыть важную персональную информацию. Некоторые утверждают, что одна и та же часть данных может быть истолкована как подтверждающая как персональную, так и не персональную информацию в зависимости от контекста и цели ее использования, что приводит к стиранию грани между персональными и не персональным данными [44]. Контроль над любыми данными подразумевает риск контроля над персональной информацией (а не наоборот).

Сторонники собственности и рынка, напротив, хотели бы использовать данные и, следовательно, обеспечить стабильный контроль над ними. С их точки зрения, все массово собираемые данные в средах IoT (за исключением

особого класса данных, которые собираются и идентифицируются как персональные данные с самого начала) могут контролироваться, принадлежать и продаваться кем угодно.

Корень этой проблемы заключается в том, что законодательство ЕС дает обратное определение персональных данных: данные являются источником информации, а исходные данные также являются персональными. Это определение приводит к, казалось бы, парадоксальной ситуации, когда никакие данные не являются персональными с самого начала и все данные могут с самого начала стать персональными. Столкновение между приватностью и собственностью, отстаиваемое тогда, выглядит как проблема курицы и яйца, в которой неясно, что из двух на первом месте: аргументы в пользу конфиденциальности, основанные на информации, отдают предпочтение курице; аргументы свойства, ориентированные на данные, находятся на стороне яйца. Однако проблема персональной информации и данных – это другая проблема. Хитрость заключается в том, что яйцо, состоящее из данных, не обязательно должно раскрывать или содержать персональную информацию цыпленка в каждом отдельном случае, и его все же можно считать ценным и заслуживающим защиты. Мы можем оценивать яйцо на разных уровнях абстракции, чем уровень персональной информации. Например, в яйце содержится драгоценный белок, а также информация об устойчивых конструкциях. Данные и информацию просто нельзя сравнивать друг с другом на одном и том же уровне анализа, потому что это принципиально разные категории. В связи с этим становится ясно, что персональные и не персональные данные не являются концептуально несовместимыми категориями.

Чтобы примирить обе точки зрения, т.е. разрешить конфиденциальность, ориентированную на персональную информацию, а также контроль, ориентированный на персональные данные, нам необходимо ограничить объем потенциально контролируемых таким образом персональных данных с противоположной стороны. Ключевой вопрос должен заключаться в том, содержат ли некоторые данные персональную информацию по своей сути и, следовательно, нельзя ли с самого начала определить их как данные, не являющиеся персональными. Примеры таких данных можно увидеть в судебной практике Европейского суда по правам человека (ЕСПЧ). Согласно ЕСПЧ, последовательность ДНК человека или образцы клеток человека [45] «содержат значительные объемы уникальных персональных данных», и простое их сохранение нарушает, без каких-либо дополнительных оснований,

основное право человека на неприкосновенность частной жизни в соответствии со статьей 8 Европейской конвенции о правах человека от 1950. Причина, по которой даже малейшая форма контроля над этими данными (например, их хранение) представляет собой нарушение прав личности, заключается в том, что при современном уровне знаний нет осмысленной интерпретации этих данных, согласно которой они объективно не позволяют нам идентифицировать отдельного субъекта данных. Эти уникальные персональные данные содержат «внутренне частную информацию». Если использовать аналогию с курицей и яйцом, эти данные в каждом случае раскрывают персональную информацию курицы. Таким образом, такие по сути персональные данные должны быть исключены из определения персональных данных для целей вопросов собственности, хотя они представляют собой основной тип персональных данных.

Основной аргумент в пользу исключения собственно персональных данных из сферы дебатов о праве собственности на данные сочетает в себе концептуальные, этические, а также юридические аспекты. Можно возразить, что с онтологической точки зрения такие данные конституируют личность человека, потому что «нет разницы между его информационной сферой и его личной идентичностью» [46]. Право собственности на такие данные таким образом, концептуально подразумевалось бы в праве собственности на идентичность людей, и владелец сугубо персональных данных не может исключать требования человека к этим данным. Следовательно, исключительный контроль над такими данными был бы аналогичен рабовладению или торговле людьми, что является этически проблематичным [47]. Любое заявление об этих данных было бы равнозначно требованию А. отрезать и взять кусок плоти от тела Б. в обмен на его долг, и это не только неприемлемо с этической точки зрения, но и незаконно в свете основных прав человека.

Современные теории, объясняющие и обосновывающие происхождение собственности следуют либо нисходящему подходу, иногда называемому позитивистским подходом к собственности, либо восходящему подход, который иногда называют подходом естественного права к собственности.

При нисходящем подходе некий высший орган должен установить право собственности, иначе его бы не существовало. Таким образом, право собственности де-юре предшествует владению де-факто. Он объясняет и обосновывает введение права собственности какими-то авторитетными причинами и целями, т.е. ссылкой на интересы, которые считаются

достаточными независимо от интересов отдельных лиц. Однако важно подчеркнуть, что эти авторитетные и в демократических обществах общественные интересы могут полностью соответствовать предпочтениям отдельных лиц, что может быть источником путаницы при определении нисходящего подхода к владению персональными данными, и что эти индивидуальные неавторитетные интересы не имеют значения.

Напротив, идея, общая для всех восходящих подходов к собственности, заключается в том, что права собственности, владелец и ценный ресурс по своей сути предпозитивны и будут существовать независимо от официальной правовой системы. С точки зрения «снизу-вверх» фактическое владение предшествует юридическому владению, и основная причина, по которой желательно ввести юридическое право собственности, состоит в том, чтобы просто придать стабильность фактическому положению дел. Таким образом, основное различие заключается в том, что в то время как при нисходящем подходе закон устанавливает и создает собственность как фундаментально юридический институт, т.е. то, что не существовало бы без позитивных законов; при подходе «снизу-вверх» закон защищает и поддерживает право собственности как принципиально предпозитивный институт.

Как нисходящий, так и восходящий подходы должны включать четыре элемента, поддерживающих владение ресурсом: *элементы контроля, защиты, оценки и распределения данного ресурса*. Таким образом, чтобы объяснить и обосновать, почему право собственности на персональные данные должно быть введено, мы должны задаться вопросом, почему мы хотим создать чей-то стабильный де-факто контроль и защиту ценных персональных данных (путем введения де-юре права собственности в нисходящем подходе); или у кого-то уже есть де-факто возможность контролировать и защищать ценные персональные данные, т.е. способность, которой закон должен придать стабильность (путем введения права собственности де-юре в восходящем подходе).

Контроль персональных данных. Право собственности как полноценный контроль позволяет владельцу использовать персональные данные в полном объеме, т.е. получать доступ, хранить, делиться, продавать и изменять их, или обрабатывать эти данные, уничтожать или отказываться от данных. Контроль также подразумевает ответственность за то, что может быть причинено другим при его осуществлении, почти так же, как владелец автомобиля несет полную ответственность за ущерб, причиненный его автомобилем.

При подходе «сверху вниз» желательность индивидуального контроля над персональными данными, подобного владению, чаще всего объясняется экономическими терминами. Европейская комиссия, например, берет за отправную точку такое всеобъемлющее макроэкономическое объяснение. Комиссия также рассматривает право собственности на данные как юридический инструмент, облегчающий доступ, свободный поток и переносимость данных, а также как нисходящий инструмент, который может повысить конкурентоспособность и инновации в экономике данных. Однако эти нисходящие объяснения недостаточны для объяснения того, почему контроль, подобный владению, лучше всего подходит для достижения указанных экономических и фактических целей, в отличие от других моделей контроля данных, что неоднократно подвергалось критике.

Де-факто контроль уже существует благодаря сегодняшним технологиям, таким как системы управления персональной информацией, а также благодаря правовым инструментам, таким как право на переносимость данных [48] и обязанность получить информированное согласие, прежде чем персональные данные могут быть собраны и использованы.

Однако восходящий подход также сталкивается с некоторыми серьезными трудностями. Информационное самоопределение и контроль над персональными данными (если рассматривать их как основные права) противоречат неотъемлемости основных прав. Согласно этой критике, персональные данные не могут фактически контролироваться в полном объеме. Более того, эта точка зрения на основные права дискриминирует передачу по умолчанию права собственности на персональные данные кому-либо, кроме субъектов данных. Те учетные записи, которые рассматривают фактический контроль над персональными данными, независимо от нормативного обоснования такого контроля, сталкиваются с двумя тесно связанными проблемами. Во-первых, они не могут говорить о фактическом полном контроле, потому что правила защиты данных, такие как GDPR, уже ограничивают потенциальную сферу контроля. Во-вторых, даже если бы правил защиты данных не было, архитектура IoT делает практически невозможным полномасштабный фактический контроль над персональными данными. В системах IoT один и тот же тип персональных данных может иметь несколько токенов (копий), и никто (на данный момент) не контролирует все токены. Таким образом, трудно рассматривать персональные данные как конкурирующий и, следовательно, исключительно контролируемый объект. Более того, встроенный облачный уровень систем IoT требует от нас решения

проблем комплексного управления данными в облаке [49]. Этот вопрос необходимо решать в первую очередь на технологическом уровне без ущерба для оптимальной модели размещения таких данных [50].

Защита персональных данных. Пассивный аспект прав собственности воплощает в себе заинтересованность в исключении других из управления персональными данными и заинтересованность в средствах правовой защиты в случае нарушения прав собственности. Поскольку пассивный и активный аспекты прав собственности являются двумя сторонами одной медали, аргументы, представленные выше, применимы и здесь. Тем не менее необходимо сделать пару дополнительных замечаний, поскольку защитный аспект права собственности тесно связан с вопросом конфиденциальности и потому, что вопросы конфиденциальности озадачивают дебаты о праве собственности на персональные данные.

Причины, поддерживающие желательность владения персональными данными в целом, то есть потенциально отчуждаемое право любого лица на владение такими данными, часто смешиваются с причинами конфиденциальности, поддерживающими желательность неотъемлемого права собственности только субъекта данных на его персональные данные. Несмотря на то, что эти две группы причин переплетаются, они различаются по крайней мере в одном аспекте, имеющем решающее значение для дебатов о собственности. Как правила, регулирующие право собственности на персональные данные, так и правила, регулирующие защиту персональных данных, обязательно относятся к персональным данным. Пока что они взаимосвязаны. Тем не менее, защита прав собственности должна относиться к персональным данным как к конечному объекту прав собственности, а не к персональным данным как к промежуточному инструменту защиты личной информации и прав личности. Пока что они различаются. Следовательно, аргументы, объясняющие желательность владения персональными данными, должны быть сосредоточены на информационном аспекте персональных данных, а не на личном аспекте персональных данных. Это совпадение экономического, ориентированного на рынок подхода к персональным данным, а подход к персональным данным, ориентированный на конфиденциальность, можно проиллюстрировать, например, совпадающими законами ЕС о конкуренции и защите данных [51].

В контексте Интернета вещей нисходящий подход пытается предложить дополнительное объяснение того, почему желательна защита, подобная праву собственности. Некоторые утверждают, что право собственности на данные,

созданные IoT, необходимо, потому что действующая правовая база для авторского права, прав на базы данных, ноу-хау, коммерческой тайны, а также для общей защиты данных не всесторонне регулирует эти вопросы. Таким образом, нынешние дебаты о праве собственности, как и о защите персональных данных, неправдоподобно строятся сверху вниз.

Подход «снизу-вверх», напротив, опирается на фактические данные. Субъекты данных могут, с одной стороны, эффективно исключить других из сбора или обработки, относящихся к ним персональных данных, например, даже не предоставляя первичные данные или не давая согласия на сбор или обработку этих данных. С другой стороны, предполагается, что сборщики и обработчики персональных данных уже могут де-факто исключать других из использования и доступа к данным, что было одной из причин, по которой право на удаление данных и право на переносимость данных были закреплены в статьях 16 и 20 GDPR. Таким образом, объяснительная сила подхода «снизу-вверх» к владению персональными данными явно превосходит альтернативу «сверху вниз».

Оценка персональных данных. Вопрос прозрачности напрямую связан с оценкой персональных данных, поскольку персональные данные в конечном счете должны иметь определенную полезность и прозрачную ценность для их потенциальных владельцев. Следовательно, должна быть возможность воплотить эту ценность в персональных данных как в торгуемый, контролируемый и достойный защиты товар. Таким образом, по крайней мере в принципе, должна быть возможность добиться прозрачной оценки персональных данных, если мы хотим оправдать желательность их собственности.

С точки зрения «сверху вниз» заманчиво создать стабильную оценку персональных данных, потому что на макроэкономическом уровне использование персональных данных ускоряет экономический рост и стимулирует инновации. Таким образом, обычная линия нисходящих аргументов подразумевает, что персональные данные имеют некоторую внутреннюю полезность или экономическую ценность. В свете экономического успеха компаний, работающих с большими данными, принято считать, что данные, включая персональные данные, являются новой нефтью или золотом экономики данных и, следовательно, должны олицетворять собой огромную и растущую ценность. В этом свете оценка персональных данных путем создания права собственности на них обещает обеспечить их универсальную и стабильную ценность.

Однако нисходящий вывод о желательности наделения персональными данными ценности неубедителен. Как, например, говорится в отчете ОЭСР, данные сами по себе не имеют внутренней ценности, и «их ценность зависит от контекста их использования», а также от того, как из них можно извлечь личную информацию. Таким образом, подход «сверху вниз» не может объяснить, почему ценность (и ее защита, подобная праву собственности) должна заключаться в данных, а не, например, в аналитических алгоритмах или инновационных предприятиях, которые используют эти данные. В контексте IoT это означает, что подход «сверху вниз» может убедительно объяснить только желательность владения более крупными функциональными единицами, такими как элементы физической инфраструктуры IoT, но не может объяснить, почему также необходимо обращаться с самими данными как с элементарной единицей стоимости. Аналогичная аргументация была использована Европейской комиссией, когда она предположила, что те, кто владеет инструментами для сбора или обработки данных, могут иметь достаточное право собственности на данные, поскольку они делают значительные инвестиции на более высоком функциональном уровне и, таким образом, (косвенно) придают ценность данным. Достаточно интересно, что Комиссия не рассматривала это как аргумент против права собственности на данные как таковые.

С точки зрения «снизу-вверх» персональные данные считаются ценными сами по себе. Это может быть продемонстрировано существованием брокеров данных, которые продают персональные данные аналогично тому, как другие брокеры продают различные сырьевые товары в диапазоне от сырой нефти до золота. Таким образом, при подходе «снизу-вверх» метафора персональных данных как торгуемого товара остается в силе. Собственность встроена в право ЕС и национальные правовые системы как нечто ценное само по себе, и в этом отношении персональные данные ничем не отличаются. Политики и ученые совместно признают стратегическую, личную, политическую, экономическую и многие другие ценности, воплощенные в персональных данных. Дело в том, что на данный момент ценность персональных данных считается несомненной, и введение права собственности на этот актив таким образом лучше объяснить снизу-вверх. Тем не менее, даже при подходе «снизу-вверх» часто бывает проблематично определить, является ли ценный актив набором персональных данных, каждым отдельным персональным данным или даже личной информацией.

Размещение персональных данных. Предыдущие три элемента вместе могут обосновать, почему закон должен вводить право собственности на персональные данные, т.е. почему персональные данные должны квалифицироваться как собственность в юридическом смысле. Предположим, что причины приватизации персональных данных убедительны. Остается ответить, кому должны быть переданы эти персональные данные. До тех пор, пока персональные данные имеют высокую экономическую ценность, реальный вопрос не в том, должны ли быть права собственности на персональные данные, а в том, чьи они должны быть.

При обсуждении распределения прав собственности на персональные данные наиболее распространенным исходным уровнем абстракции, на котором определяются потенциальные владельцы, является то, что они либо должны быть субъектом данных, либо нет [52]. Право собственности на персональные данные, конечно, не должно игнорировать требования конфиденциальности. Тем не менее, возможно и даже необходимо поместить эти основные права личности в скобки, имея в виду, что если владелец персональных данных нарушает эти права, всегда должно быть предусмотрено средство правовой защиты. При этом полезно напомнить себе, что право собственности на личные данные должно быть уточнено до права собственности на внешне персональные данные. Нет смысла анализировать право собственности в отношении персональных данных, которые по своей сути несут личную информацию о субъекте данных. Как объяснялось ранее, простое сохранение персональных данных представляет собой нарушение права на неприкосновенность частной жизни, изложенного в статье 8 Европейской конвенции о правах человека. Если уточнить только внешние персональные данные, убеждение в том, что персональные данные принадлежат или должны принадлежать субъектам данных в каком-то фундаментальном и, возможно, также естественном смысле, теряет свои объяснительные и оправдательные основания и остается открытым для пересмотра.

Чтобы объяснить все элемента владения (внешними) персональными данными снизу-вверх, нам, во-первых, нужно иметь возможность решить проблему полного контроля над токенами данных и изучить, возможно ли это и как это возможно. Это будет юридический, философский, а также технологический вызов.

Во-вторых, необходимо решить проблему прозрачности персональных данных как объекта защиты прав собственности. Эта задача будет в первую

очередь технологической. Похоже, что до тех пор, пока не появятся необходимые технологические достижения, защита, подобная праву собственности, будет оставаться необъяснимой с точки зрения «снизу-вверх». В контексте повседневного IoT (например, в умных городах) ни фактический, ни законный владелец не смогут определить, были ли повреждены, украдены, изменены или использованы неправомерно его персональные данные. В свою очередь, предполагаемый правонарушитель не будет знать, покушался ли он на чью-то законную собственность. Эта проблема может быть решена с помощью восходящих технологических решений, таких как платформа AURA или Solid [53]. Напротив, фактическая защита прав собственности на данные не может быть реализована на бумаге (модель «сверху вниз»). Вместо этого они должны быть встроены в аппаратные и программные реализации IoT [54]. Законы могут установить систему фикций и санкций, чтобы облегчить такое правоприменение и стимулировать систему владения персональными данными, однако такое регулирующее вмешательство не объясняет и не оправдывает право собственности в целом.

В-третьих, хотя персональные данные уже считаются ценными, остается аналогичная технологическая проблема, связанная с тем, как элемент оценки собственности может быть прозрачно закреплен за персональными данными.

Решения всех этих трех вопросов должны предшествовать любой обработке персональных данных по принципу «снизу-вверх». Учитывая сильные экономические стимулы как сверху вниз, так и снизу-вверх, мы можем ожидать, однако, что они будут решены (по крайней мере, теоретически) в недалеком будущем.

ЗАКЛЮЧЕНИЕ

Мы видели, что владение персональными данными не может быть всесторонне объяснено и оправдано ни одним из двух подходов к владению (восходящий и нисходящий). В то время как подход «сверху вниз» оказался совершенно непригодным для объяснения и обоснования права собственности на персональные данные в IoT в целом и отчасти непригодным для объяснения вопросов, связанных с контролем, защитой, оценкой и распределением персональных данных в IoT, подход «снизу-вверх» был отчасти успешным на обоих фронтах.

Чтобы справиться с дальнейшими проблемами восходящего подхода, мы выступаем за пересмотренную версию восходящего объяснения и обоснования права собственности на персональные данные. Однако, если этот новый подход

увенчается успехом, он должен лучше охватывать концептуально персональные данные как потенциальные объекты прав собственности и IoT как ключевую будущую среду для транзакций данных. Концептуально – это означает устранение неоднозначности информации из данных и рассмотрение прав собственности исключительно в отношении данных.

Необходимо устранить неоднозначность внутренних персональных данных от внешних. Только вторая категория может рассматриваться как потенциальный объект права собственности и что эти две категории не могут быть заменены традиционной двойственностью между персональными и не персональными данными.

При распределении прав собственности должен использоваться какой-то неизбирательный тест, который не рассматривает субъектов данных как привилегированную категорию потенциальных владельцев. При этом этот подход можно легко совместить с защитой прав личности.

ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА

1. S Aguzzi and others, Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination (European Commission 2014) 10, 26, 61.
2. J Van den Hoven, Internet of Things Factsheet Ethics (European Commission 2013).
3. J Drexl and others, ‘Data Ownership and Access to Data – Position Statement of the Max Planck Institute for Innovation and Competition of 16 August 2016 on the Current European Debate’ (2016) Max Planck Institute for Innovation & Competition Research Paper No 16-10.
4. M Taddeo, ‘Trusting Digital Technologies Correctly’ (2017) 27 Minds & Machines 565.
5. C Bartolini, C Santos and C Ullrich, ‘Property and the cloud’ (2018) 34 CLSRev 358.
6. F Thouvenin, RH Weber and A Früh, ‘Data ownership: Taking stock and mapping the issues’ in M Dehmer and F Emmert-Streib (eds), Frontiers in Data Science (CRC Press 2018).
7. C Wendehorst, ‘Of Elephants in the Room and Paper Tigers: How to Reconcile Data Protection and the Data Economy’ in Lohsse, Schulze and Staudenmayer (eds) (n 6) 332.
8. S Wolfert and others, ‘Big Data in Smart Farming – A review’ (2017) 153 Agricultural Systems 69.

9. World Economic Forum, Personal Data: The Emergence of a New Asset Class (Geneva 2011).
10. L Edwards, 'Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective' (2016) 2 EDPLR 28, 29, 33–34.
11. European Data Protection Supervisor, 'EDPS Opinion on Personal Information Management Systems' (Opinion No 9/2016) // https://perma.cc/X236-GR48.
12. Telefónica, 'Telefónica presents AURA, a pioneering way in the industry to interact with customers based on cognitive intelligence' (press release, 26 February 2017) // https://www.telefonica.com/en/web/press-office/-/telefonica-presents-aura-a-pioneering-way-in-the-industry-to-interact-with-customers-based-on-cognitive-intelligence.
13. Окюлов О. Гражданский кодекс Республики Узбекистан в новой редакции: каким должен быть IV раздел. – 2019.
14. Окюлов О. Правовой статус интеллектуальной собственности: дис.… д-ра юрид. наук //Т.: ТГЮИ. – 2000. – С. 14.
15. Караходжаева Д. М. Проблемы развития и совершенствования законодательства о праве собственности юридических лиц в Республике Узбекистан: дис.… докт. юрид. наук //Т.: ТГЮИ. – 2008. – С. 44.
16. Караходжаева Д. Новые механизмы защиты частной собственности как основа улучшения инвестиционного климата //Обзор законодательства Узбекистана. – 2019. – №. 1. – С. 34-35.
17. Mehmonov K. M., Musaev E. T. Legal Regime of Digital Rights //Ilkogretim Online. – 2021. – Т. 20. – №. 3. – С. 1683-1686.
18. Мехмонов К. М. Особенности Правового Режима Цифровых Прав //Журнал Правовых Исследований. – 2021. – Т. 6. – №. 1.
19. Mehmonov Q. A. Civil legal protection of a database according to the legislation of foreign countries //Review of law sciences. – 2018. – Т. 2. – №. 1. – С. 11.
20. Mekhmonov K. Issues of legal regulation of relations related to information and communication technologies //Review of law sciences. – 2020. – Т. 4. – №. 1. – С. 17.
21. Мехмонов К. М. ВОПРОСЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ОТНОШЕНИЙ, СВЯЗАННЫХ С ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫМИ ТЕХНОЛОГИЯМИ //Review of law sciences. – 2020. – №. 1. – С. 75-78.
22. Mekhmonov K. The legislative framework and the principles of civil-law regulation of relations connected with the Computer programs and databases in the Republic of Uzbekistan //Theoretical & Applied Science. – 2017. – №. 3. – С. 23-28.

23. Мехмонов К. М. ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИНВЕСТИЦИЙ В СФЕРЕ ИНФОРМАЦИОННОКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ //ПРАВОВЫЕ ОСНОВЫ СТАНОВЛЕНИЯ И УКРЕПЛЕНИЯ РОССИЙСКОЙ. – 2019. – С. 30.
24. Мехмонов К. М. НЕКОТОРЫЕ ОСОБЕННОСТИ ДОГОВОРОВ, СВЯЗАННЫХ С ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫМИ ТЕХНОЛОГИЯМИ //INTERNATIONAL SCIENTIFIC REVIEW OF THE PROBLEMS OF LAW, SOCIOLOGY AND POLITICAL SCIENCE. – 2019. – С. 54-62.
25. Бурханова Л. М. Правовая характеристика частной собственности отдельных видов юридических лиц в условиях перехода Республики Узбекистан к рыночным отношениям //Вестник Пермского университета. Юридические науки. – 2010. – №. 2. – С. 88-98.
26. Бурханова Л. ВОПРОСЫ ПРАВОПРИМЕНЕНИЯ ИНСТИТУТА ОБЩЕЙ СОВМЕСТНОЙ СОБСТВЕННОСТИ НА ПРИМЕРЕ ОБЩЕЙ СОВМЕСТНОЙ СОБСТВЕННОСТИ СУПРУГОВ //Review of law sciences. – 2020. – №. 3. – С. 61-69.
27. Караходжаева Д. М., Бурханова Л. М. Особенности осуществления реформ частной собственности на землю в Республике Узбекистан //Science and Education. – 2021. – Т. 2. – №. 5. – С. 1083-1096.
28. Бурханова Л. НОВЫЕ ПОДХОДЫ К ОПРЕДЕЛЕНИЮ ПОНЯТИЙ НЕМАТЕРИАЛЬНЫЕ БЛАГА В ПРОЕКТЕ НОВОЙ РЕДАКЦИИ ГРАЖДАНСКОГО КОДЕКСА РЕСПУБЛИКИ УЗБЕКИСТАН //Review of law sciences. – 2020. – №. 4. – С. 21-29.
29. Бурханова Л. М. Вопросы совершенствования правового регулирования нематериальных благ как особого объекта гражданского права в проекте новой редакции Гражданского кодекса Республики Узбекистан. – 2021.
30. Бурханова Л. М. Защита средств индивидуализации в сетях Интернет посредством доменных имен. – 2019.
31. Dilorom K., Burkhanova L., Sharakhmetova U. Features of determining the legal status of legal entities in the draft new version of the civil code of the republic of Uzbekistan and the need to introduce new institutions in the legislation: Theoretical developments and proposals //European Journal of Molecular & Clinical Medicine. – 2020. – Т. 7. – №. 2. – С. 2151-2161.
32. Kuldashev N. TORT LIABILITY ISSUES FOR HARM CAUSED BY THE INTERNAL AFFAIRS BODIES //International Scientific and Current Research Conferences. – 2021. – С. 8-14.

33. Кулдашев Н. А. ОРГАНЫ ВНУТРЕННИХ ДЕЛ КАК СУБЪЕКТЫ ДЕЛИКТНЫХ ОТНОШЕНИЙ //Третьи цивилистические чтения памяти профессора МГ Прониной. – 2021. – С. 111-114.
34. Кулдашев Н. Improvement of the legal regulation system of tort relations with the participation of internal affairs organs //Общество и инновации. – 2020. – Т. 1. – №. 2. – С. 199-208.
35. Кулдашев Н. Совершенствование системы правового регулирования деликтных отношений с участием органов внутренних дел //Общество и инновации. – 2020. – Т. 1. – №. 2. – С. 199-208.
36. КУЛДАШЕВ Н. А. СОВЕРШЕНСТВОВАНИЕ СИСТЕМЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ДЕЛИКТНЫХ ОТНОШЕНИЙ ПРИ УЧАСТИИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ //Право и жизнь. – 2019. – №. 2. – С. 80-87.
37. Kuldashev N. Ҳуқуқбузарликлар содир этилиши оқибатида етказилган зарарларни қоплаш институтини такомиллаштиришга оид мулоҳазалар //O ‘zbekiston qonunchiligi tahlili. – 2017. – №. 3. – С. 67-69.
38. Qo‘ldoshev N. Ички ишлар органлари фуқаровий-ҳуқуқий муносабатлар субъекти сифатида //O ‘zbekiston qonunchiligi tahlili. – 2008. – №. 3-4. – С. 10-15.
39. Эгамбердиев Э. Х. Правовые вопросы осуществления торговли объектами виртуального мира за реальные денежные средства //ИННОВАЦИОННЫЕ НАУЧНЫЕ ИССЛЕДОВАНИЯ В СОВРЕМЕННОМ МИРЕ: ТЕОРИЯ, МЕТОДОЛОГИЯ, ПРАКТИКА. – 2022. – С. 100-105.
40. Hajibaevich E. E. CIVIL LAW STATUS OF VIRTUAL OBJECTS AND THEIR REFLECTION IN THE NEW CIVIL CODE OF THE REPUBLIC OF UZBEKISTAN //Web of Scientist: International Scientific Research Journal. – 2023. – Т. 4. – №. 1. – С. 47-54.
41. Khajibaevich E. E. Civil law status of virtual world objects //Eurasian Research Bulletin. – 2023. – Т. 16. – С. 33-41.
42. L Floridi, ‘Semantic Conceptions of Information’, The Stanford Encyclopedia of Philosophy (Spring edn, 2017) https://plato.stanford.edu/archives/spr2017/entries/information-semantic.
43. G Malgieri, ‘Property and (Intellectual) Ownership of Consumers’ Information: A New Taxonomy for Personal Data’ (2016) 4 Privacy in Germany 133.
44. N Purtova, ‘Do property rights in personal data make sense after the Big Data turn? Individual control and transparency’ (2017) Tilburg Law School Research Paper No 2017/21, 13–17 // https://ssrn.com/abstract=3070228
45. Aycaguer v France App no 8806/12 (ECtHR, 22 June 2017), (2017) EHRLR 519; S v United Kingdom (2009) 48 EHRR 50 (ECtHR).

46. L Floridi, 'The Ontological Interpretation of Informational Privacy' (2005) 7 Ethics Inf Technol 185, 195.
47. M Katz, 'Philosophy of Property Law, Three Ways' in Cambridge Companion to Law and Philosophy (CUP 2018) 5 https://ssrn.com/abstract=3076251
48. P De Hert and others, 'The right to data portability in the GDPR: Towards user-centric interoperability of digital services' (2018) 34 CLSRev 193, 201.
49. N Ambika and M Sujaritha, 'A Data Ownership Privacy Provider Framework in Cloud Computing' (2017) 2 IJSRCSEIT 462.
50. S Sicari and others, 'A security-and quality-aware system architecture for Internet of Things' (2016) 18 Inf Syst Front 665/
51. F Costa-Cabral and O Lynskey, 'Family Ties: The Intersection Between Data Protection and Competition in EU Law' (2017) 54 CML Rev 11.
52. J Kang and B Buchner, 'Privacy in Atlantis' (2004) 18 HarvJL& Tech 229, 238 fn 37.
53. Solid // https://solid.mit.edu/
54. S Tyagi, A Darwish and MY Khan, 'Managing computing infrastructure for IoT data' (2014) 4 Advances in Internet of Things 29.