ПРАВОВЫЕ АСПЕКТЫ ВНЕДРЕНИЯ ИНТЕРНЕТА ВЕЩЕЙ

[1]Исаков В.Б., [2]Сарьян В.К., [3]Фокина А.А.

[1]Национальный исследовательский университет «Высшая школа экономики» (НИУ ВШЭ), 101000, Россия, г. Москва, ул. Мясницкая, д.20, e-mail: visakov@hse.ru

[2]Федеральное государственное унитарное предприятие «Научно-исследовательский институт радио», 105064, г. Москва, ул. Казакова, д.16, e-mail: sarian@niir.ru

[3]Московский технический университет связи и информации, 111024, г. Москва, ул. Авиамоторная, д. 8а, e-mail: anna.a.fokina@gmail.com

На протяжении последних лет можно наблюдать стремительное развитие Интернета вещей (IoT). Его роль в жизнедеятельности человека указывает на необходимость регламентации правового статуса IoT. Выполнению такой задачи способствует разработка нормативно-правовой базы, обеспечивающей, что при удовлетворении вещи установленным критериям возможно её подключение к Сети. Соответствующее разрешение может выдаваться в виде сертификата специально уполномоченным органом.

Ключевые слова: Интернет вещей, правовое регулирование, вещь, идентификация, интеграция, нормативно-правовая база, сертификация, уполномоченный орган.

LEGAL ASPECTS OF THE IMPLEMENTATION OF THE INTERNET OF THINGS

In recent years, one can observe the rapid development of the Internet of Things (IoT). Its role in human life indicates a need for regulation of the legal status of IoT. Such a task supported by the development of the legal framework to ensure that the items meet the established criteria it is possible to connect to the Internet. A permit may be issued in the form of a certificate specially authorized body.

Keywords: Internet of Things, regulation, thing, identification, integration, legal framework, certification, authorized body.

Введение

С момента своего зарождения в 1999 году Интернет вещей претерпел колоссальное развитие, образовалась сложная система элементов и взаимодействий, для регулирования которых необходима нормативная база.

Масштабность IoT хорошо видна в цифрах. В 2003 году население Земли составляло около 6,3 миллиарда человек, а к Интернету было подключено 500 миллионов устройств (то есть примерно по 0,08 такого устройства на каждого человека). Уже через семь лет, к 2010 году, количество подключенных устройств выросло в 25 раз - до 12,5 миллиардов, тогда как население Земли увеличилось на полмиллиарда и составило 6,8 миллиарда человек. Таким образом, на каждого человека стало приходиться 1,84 подключенного устройства[8]. Что повлияло на бурный рост Интернета вещей?

Одним из значимых событий был запуск протокола IPv6 - новой версии межсетевого протокола, призванной решить проблемы, с которыми столкнулась предыдущая версия IPv4 за счёт использования длины адреса 128 бит вместо 32. Технической проблемой

эффективного использования протокола IPv6 называют сложность маршрутизации: необходимость работы с длинными именами приводит к усложнению таблиц маршрутизации и проблемам с прокладкой маршрутов. Возможно, преодоление сложности маршрутизации выявит необходимость особого нормативно-правового регулирования конкретно для этого аспекта.

Другой причиной бурного роста Интернета вещей можно назвать увеличение числа новых технологий, используемых в повседневной жизни, и увеличение количества устройств, подключенных к Интернету, при одновременно снижающейся их стоимости.

Помимо этого росту Интернета вещей способствует увеличение количества населения Земли, подключенного к Интернету. Так, в настоящий момент информирование населения во многом происходит за счет широкополосного доступа (ШПД). Генеральный секретарь ООН Пан Ги Мун призвал обеспечить данной услугой уже к 2015 году более половины населения Земли.

Оценивая потенциал Интернета вещей видится возможным привести следующий пример. Национальный разведывательный совет США - орган, обеспечивающий работу директора разведывательного сообщества США и представляющий собой центр долгосрочного стратегического анализа - в 2008 году опубликовал исследование, в котором среди шести гражданских технологий с наибольшей «взрывной силой» назван Интернет вещей[15]. По мнению авторов отчета, к 2025 году узлами Интернета вещей смогут стать все окружающие нас предметы. В отношении количественных прогнозов касательно Интернета вещей - к 2020 Gartner предполагает около 26 миллиардов устройств в сети, ABI Research – 30 миллиардов, а согласно прогнозам компании Ericsson, к сети будет подключено 50 миллиардов устройств[4]. Экономика анализируемого явления поражает не меньше: International Data Corporation (IDC) оценивает мировой рынок IoT в $665,8 миллиардов долларов США, а согласно европейскому исследованию американской некоммерческой организации Research ANd Development (RAND), влияние IoT на мировую экономику к 2020 году может быть оценено в сумму от 1 до 14 биллионов долларов США[13] (для сравнения: последняя сумма примерно равна ВВП Европейского Союза).

Широкое распространение Интернета вещей, наиболее вероятно, потребует детальной нормативной проработки как в отношении самого Интернета вещей, так и в других, смежных, сферах. Обозначению отдельных правовых аспектов регулирования IoT и посвящена данная работа.

Некоторые актуальные юридические вопросы в связи с развитием Интернета; их применимость к Интернету вещей

Несмотря на расхожие прогнозы касательно количества вещей, которые могут быть подключены к Интернету в ближайшие годы, по всем имеющимся оценкам, это количество растет и будет продолжать расти. По данным нескольких консалтинговых компаний и международных организаций, технологии Интернета вещей могут оказать существенное влияние на мировую экономику и обеспечить несколько дополнительных триллионов долларов в течение ближайших лет. Так, например, согласно прогнозу International Data Corporation (IDC), рост объема рынка Интернета вещей ежегодно будет составлять 16,9%, таким образом вырастет с 655,8 миллиардов долларов в 2014 до 1,7 триллиона в 2020[9]. Вряд ли такое экономическое воздействие возможно без четкого регуляторного вмешательства. Иначе неминуемо возникнут нарушения, злоупотребления и споры.

Одной из возможных отправных точек рассмотрения юридических вопросов может быть анализ характера отдельных существующих норм регулирования Интернета. В разных странах законодательство, бесспорно, находится на разных уровнях развития, но при этом можно выделить «болевые точки», вокруг которых либо уже идут дебаты, либо могут начаться в ближайшее время. Это касается таких вопросов, как разработка понятийного аппарата юридической науки, проблема идентификации лиц, повышения уровня правосознания пользователей, защиты персональной информации, ответственности субъектов права, действия права в пространстве и по кругу лиц, сбор доказательств и подтверждения юридических фактов и др.

Сразу несколько упомянутых проблем можно проиллюстрировать на примере отечественной правоприменительной практики, а именно - официального мнения Суда по интеллектуальным правам РФ, подготовленного к расширенному заседанию Научно-консультативного совета при Суде по интеллектуальным правам РФ об ответственности информационного посредника. В документе дается разъяснение по вопросу «О возможности признания Интернет-ресурсов, используемых для продажи товаров через информационно-телекоммуникационную сеть Интернет, информационными посредниками в смысле положений статьи 1253.1 Гражданского кодекса Российской Федерации (далее – ГК РФ)»[1]. Актуальность вопроса обусловлена, в частности, ответственностью за нарушение исключительного права при наличии вины.

Ответственность

Ранее в судебной практике был выработан подход, согласно которому при привлечении к ответственности владельцев Интернет-ресурсов судам необходимо проверять, в частности, получил ли провайдер прибыль от деятельности, связанной с использованием исключительных прав других субъектов, которую осуществляли лица, пользующиеся услугами этого провайдера[2]. Данный подход был выработан до вступления в силу статьи 1253.1 ГК РФ, которая критерия источника получения вознаграждения не устанавливает. Вместе с тем логичным видится подход, согласно которому лицо, не получающее вознаграждение от предоставления возможности размещения материалов или информации в Интернете либо предоставления возможности доступа к ним, не подпадает под определение информационного посредника как такового. Возможным видится разграничение лиц, являющихся и не являющихся информационными посредниками, исходя из того, кем размещается информация на Интернет-сайте, проверяет ли Интернет-ресурс контент перед его размещением и должен ли он соответствующую проверку осуществлять.

У такого подхода есть ярые противники. Например, д.ю.н. профессор М.А. Рожкова отрицает саму возможность признания Интернет-ресурса информационным посредником, приводя в подтверждение п. 1 ст. 1253.1 ГК РФ, под информационными посредниками называющий исключительно субъекты права: оператора связи (лицо, осуществляющее передачу информации и данных в сети Интернет); хостинг-провайдера (лицо, создающее возможность размещения информации и данных с использованием сети Интернет); владельца информационного ресурса (лицо, предоставляющее возможность доступа к информации и данным в сети Интернет). По мнению профессора, из следует отличать от Интернет-ресурсов: поисковых машин, порталов, корпоративных и частных сайтов, домашних страниц и т.п., которые обеспечивают генерацию, хранение, передачу информации и данных[3].

На этом небольшом примере затрагивается важность понятийного аппарата, ответственности субъектов права, действия права в пространстве и по кругу лиц, сбора доказательств и подтверждения юридических фактов и др. Если обратиться к вопросу устройства Интернета вещей, широкая архитектура составляющих его элементов может вызвать еще больше вопросов. Любой из этих элементов способен выйти из строя, связь между ними может быть потеряна, возможно вмешательство внешних факторов. Для регулирования релевантных отношений необходимо четкое понимание как технических, так и юридических аспектов.

Безопасность информации

Пометить объекты реального мира, вещи, метками и организовать считывание с них сведений не представляется сверхсложной задачей. Технические возможности для этого уже есть: интернет-протокол IPv6 предоставляет огромное число IP-адресов, микрочипы и беспроводные модули для их подключения, но далеко не просто обеспечить соответствие средств обработки персонифицированных данных требованиям законодательства. В России обработка персональных данных регулируется рядом законодательных актов, в том числе Федеральным законом РФ «О персональных данных» № 152-ФЗ от 27 июля 2006 года и подзаконными актами ряда ведомств. Согласно Закону о персональных данных, обрабатывать персональные данные можно только с письменного согласия субъекта персональных данных и хранить их можно только в течение действия договора. Исключения могут составлять лишь те случаи, которые предписаны другими нормативно-правовыми актами. После окончания срока договора данные должны быть либо удалены, либо обезличены. Особые требования по защите информации к системам предъявляются как с точки зрения типа хранимой информации, так и с точки зрения ее объемов.

В IoT каждая вещь, помимо физического выражения, существует онлайн. Использование беспроводных методов передачи данных открывает много возможностей, в том числе, и неправомерного использования, для защиты от которого нужны методы криптографии и физической защиты. В случае взаимодействия вещей ситуация осложняется тем, что необходимо согласие субъекта права на то, чтобы собирать, хранить, обрабатывать, передавать информацию о нем. Вопрос о том, в какой степени упомянутые акты будут применимы к Интернету вещей, в частности, зависит от возможности признать правосубъектность вещей, в него входящих.

Киберпреступность

С развитием технологий киберпреступность находит все новые формы распространения. На текущий момент, пожалуй, наиболее часто она выражается в распространении вредоносных вирусов, взломах паролей, краже информации, её изменении и распространении через Интернет, а также вредоносном вмешательстве через компьютерные сети в работу различных систем. Из «громких» дел можно отметить взлом сайта американской частно-разведывательной компании Stratfor Global Intelligence в конце 2011 года хакерами группы Anonymous. В результате более 5 миллионов имейлов, содержащих личную информацию, были опубликованы в Интернете.

Применительно к Интернету вещей киберпреступность выглядит не менее угрожающей. В 2010 году в компьютерной системе иранского ядерного центра, являющегося важной составляющей ядерной программы Исламской республики, был обнаружен вирус Stuxnet, изменивший скорости вращения центрифуг, что привело к их выходу из строя. Это яркий пример того, как при помощи кибератак можно выводить из строя или, напротив, приводить в действие вещи, взаимодействующие через Интернет.

Российское законодательство, регламентирующее ответственность за преступления в сфере куберпреступлений весьма фрагментарно. Глава 28 Уголовного кодекса Российской Федерации содержит, по сути три применимых статьи, охватывающие три состава: неправомерный доступ к компьютерной информации (ст. 272 УК РФ), создание, использование и распространение вредоносных программ для ЭВМ (ст. 273 УК РФ) и нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274 УК РФ). Приговоры вынесенные различными судами по однородным уголовным делам, зачастую расходятся в вопросах квалификации действий преступника и размеров наказания. Постановления или определения Верховного Суда РФ по вопросам применения статей о компьютерных преступлениях отсутствуют.

При этом явно, что законодательное регулирование киберпространства в рамках одной юрисдикции малоэффективно. Необходимы наднациональные нормы. Примеры международного сотрудничества в борьбе с куберпреступностью уже существуют. Одним из них является Европейская конвенция по киберпреступлениям 2001 года, принятая в рамках Совета Европы. Однако, на момент написания данной статьи Россия её не ратифицировала. Очевидно, развитие как отечественной, так и международной законодательной базы в отношении киберпреступлений необходимо, и станет еще более необходимым с распространением Интернета вещей.

Патентная защита

Как на национальном уровне, так и между государствами растет конкуренция в отношении инструментов влияния на развитие Интернета вещей. Некоторые игроки рынка уже в значительной мере продемонстрировали свое техническое лидерство в соответствующих технологических областях, обеспечив патентную защиту многочисленным объектам интеллектуальной собственности. Среди стран-лидеров явно обозначились США, за которым следуют несколько азиатских государств: Япония, Корея, Китай. Из компаний, имеющих наибольшее количество патентов, в тройку лидеров входят LG Electronics, Ericsson и Qualcomm[11]. Анализ портфеля патентов компаний в сфере Интернета вещей показывает, что с среди компаний, помимо прямого патентования, получили распространение несколько корпоративных стратегий. Так, компании осуществляют взаимное лицензирование патентов, происходит значительное количество слияний и поглощений компаний, а также осуществляются иные виды сотрудничества. Среди примеров можно выделить поглощение компанией Google компании Nest и уже упоминавшимся Qualcomm компании CSR. Стоимость указанных сделок составила около 3 миллиардов и 2,5 миллиардов долларов соответственно, что говорит, в том числе, о высокой оценке принадлежащих компаниям патентов в области Интернета вещей.

Таким образом, патентование в исследуемой области развивается очень активно. В то же время названная тенденция одобряется не всеми. Например, в коммюнике Европейской комиссии от 18 июня 2009 года «Интернет вещей: план действий для Европы» подчеркивается, что развитие Интернета вещей не может быть оставлено частному сектору ввиду социальных перемен, которые оно несет с собой[10]. Аналогичные вопросы высказываются отдельными юристами[6] и, очевидно, требуют весьма срочного разрешения, учитывая количество оформляемых в сфере Интернета вещей патентов.

Актуальность регулирования Интернета вещей и определения юридического статуса вещей, подключенных к Интернету

Выше были приведены рассуждения о тесной взаимосвязи между технической и юридической стороной этой системы, и юридический анализ ниже также связан с технической стороной Интернета вещей. Создание полноценного IoT потребует возможного пересмотра многих составляющих современного Интернета, от общих архитектурных принципов существующих технологий и управления сетями до обеспечения безопасности и соблюдения прав личности. В Интернете людей с 1994 года утверждена система универсальных идентификаторов ресурсов (Uniform Resource Identifier, URI), включающих в себя указание на механизм, используемый для доступа к ресурсу, компьютер, на котором ресурс находится, и имя ресурса (обычно имя файла). Однако в случае Интернета вещей ресурсы более разнообразны и сложнее организованы. Невозможно обойтись одним идентификатором в силу того, что вещь может существовать в разных контекстах. В IoT каждая вещь, предположительно, имеет свой уникальный идентификатор или виртуальный идентификатор, которые совместно образуют континуум вещей, способных адресоваться друг другу, создавая временные или постоянные сети. Кроме того, вещь может проходить по цепочке поставок от первых этапов производства как отдельное изделие (например, акселерометр может представлять собой часть системы управления жесткого диска компьютера для активации механизма защиты от повреждений, диск – часть компьютера, а компьютер – входить, например, в систему оповещения о риске стихийного бедствия). Особенности правового регулирования должны будут учитывать, что, по меньшей мере, в ряде случаев, нельзя раскрывать подлинное имя вещи, потребуется уникальный идентификатор и средства его перевода для поддержки жизненного цикла вещи в соответствующих обстоятельствах, а также нормы, позволяющие это сделать конфиденциально, безопасно, без нарушения прав правообладателей. Среди существующих примеров можно назвать стандарты, используемые в логистике. Но их область применения ограничена. Необходимо продолжать и расширять исследования и разработки, чтобы обеспечить совместимость гетерогенных систем и разнородных ресурсов, включая людей, вещи, программное обеспечение. Чтобы реализовать такую задачу необходима совместная работа технических и юридических экспертов.

Исходя из сложной системы Интернета вещей и предполагаемой независимости в принятии вещью, подключенной к такой системе, решений, логично предположить, что подключаемые вещи должны соответствовать определенным стандартам, возможно, сертифицированы. Стандарты должны содержать принципы агрегации, хранения, анализа и передачи больших массивов разнородных данных для функционирования системы. Логичным кажется предположение, что с учетом актуальности обозначенных выше юридических вопросов для таких принципов необходима разработка специфической нормативно-правовой базы, как на государственном уровне, так и международной. Говоря о российском законодательстве, необходимо существенно проработать позитивное право, и сделать это с учетом транснационального характера вопроса. При этом в силу огромного и постоянного вклада частных игроков рынка Интернета вещей в его развитие важно учесть такие инициативы и договорное регулирование (саморегулирование его участников).

В аспекте транснациональности, глобальном масштабе Интернета вещей интересен опыт международных организаций, надгосударственных образований и их органов. Так, Европейская комиссия уже давно определила Интернет вещей как одну из важных сфер развития. В 2009 году ею был разработан уже упоминавшийся план, отражающий важные

направления работы[10]. Глобальные инициативы реализуются сегодня сектором стандартизации телекоммуникаций Международного союза электросвязи (МСЭ-Т). В рамках этих инициатив, среди прочего, различными исследовательскими комиссиями МСЭ выполняется комплекс работ по стандартизации Интернета вещей и сетей следующих поколений.

Важность обеспечения безопасности, конфиденциальности информации и других прав, связанных с развитием IoT, не должна однако привести к чрезмерной регламентации этой сферы, препятствующей её дальнейшему развитию. Когда в рамках принятого ранее плана Европейская комиссия 2013 году проводила консультации по вопросу IoT с частным сектором, были высказаны разнообразные мнения о том, насколько в действительности необходима специальная регламентация Интернета вещей. Оппоненты подвергали сомнению меры государства в силу того, что (1) Интернет вещей появился недавно и все еще бурно развивается, а потому предусмотреть все случаи необходимости регламентации невозможно, (2) большую роль в развитии отрасли играют частные игроки, поэтому должная степень свободы и саморегулирования необходимы; (3) установленные правила могут даже препятствовать дальнейшему развитию[1]. Аналогично, в докладной записке Федеральной торговой комиссии США (далее – «ФТК США») отмечается, что специальное законодательство в отношении Интернета вещей преждевременно. При этом ФТК США обращает внимание на саморегулирование различных отраслей промышленности в целях улучшения методов обеспечения конфиденциальности и безопасности данных[12].

Заключение

Число и разнообразие устройств, относящихся к Интернету вещей, и технологий, обеспечивающих их взаимодействие с другими вещами, растет в геометрической прогрессии. Аналогично, увеличивается и количество сфер их применения. Эти процессы приводят к повышающейся технической сложности системы и увеличивают разрыв с системой регуляторной. Какого рода регулирование необходимо в этой связи, чтобы устранить такой разрыв и для создать надежную инвестиционную инфраструктуру? Очевидно, что для создания надежных и безопасных, способствующих развитию Интернета вещей и служащих главной цели - улучшению качества жизни человека - решений необходимо разработать соответствующий требованиям технологической системы подход. Такой подход должен учитывать как специфику отрасли, так и соотношение с другими отраслями. При этом однозначно важным является определение статуса вещи, подключенной к Интернету и адекватное совмещение этого статуса с иными составляющими архитектуры Интернета вещей. Для определения такого статуса может быть необходимым разработка процесса стандартизации вещи, критериев такой стандартизации и путей взаимодействия с иными составляющими системы IoT.

Список литературы

1. Ответственность информационного посредника. Использование товарных знаков в информационно-телекоммуникационной сети Интернет // Справка к заседанию Научно-консультативного совета при Суде по интеллектуальным правам. URL: http://ipc.arbitr.ru/node/13619 (дата обращения 12.10.2015).

2. Постановление Президиума Высшего Арбитражного Суда Российской Федерации от 01.11.2011 № 6672/11. URL: http://arbitr.ru/bras.net/f.aspx?id_casedoc=1_1_be87c7b7-ec2b-4325-82c4-e1ae94f34e16 (дата обращения 12.10.2015).
3. Рожкова М.А. Найти отличия: технические и правовые аспекты Интернета. // Сайт журнала Суда по интеллектуальным правам. URL: http://www.ipcmagazine.ru/legal-issues/find-differences-technical-and-legal-aspects-of-the-internet (дата обращения 12.10.2015).
4. Храмцов П. Всеобъемлющий Интернет: прогнозы и реальность // Открытые системы. - 2013. №4. URL: http://www.osp.ru/os/2013/04/13035552/ (дата обращения 12.10.2015).
5. Черняк Л. Платформа Интернета вещей // Открытые системы. -2012. №7. URL: http://www.osp.ru/os/2012/07/13017643/ (дата обращения: 12.10.2015).
6. Barbry E. The Internet of Things. Legal Aspects. What Will Change (Everything) // Digital Economic Journal. - 2012. 3Q. No. 87. - P. 90.