УДК 342.951:351.862.68(5:265)

DOI dx.doi.org/10.24866/1813-3274/2018-1-2/131-139

Я.О. Кучина¹

Дальневосточный федеральный университет, г. Владивосток, Россия

E-mail: kuchina.yao@dvfu.ru

ЗАКОНОДАТЕЛЬНОЕ РЕГУЛИРОВАНИЕ ОБЛАЧНЫХ ТЕХНОЛОГИЙ В НЕКОТОРЫХ СТРАНАХ АЗИАТСКО-ТИХООКЕАНСКОГО РЕГИОНА

Аннотация. Цифровые технологии в современном мире зачастую лишены границ и ограничений. Как и любая конкурентоспособная ИТ, технологии, специализирующиеся на обороте услуг в облаке, разработанные в одной стране, функционируют практически так же, как и в других странах. Это может быть основанием полагать, что законы в этих странах должны быть одинаковыми, но это не так. Особенности конкретной правовой системы, правовой истории и традиции государства приводят к различиям в этой сфере. Кроме того, влияние на особенности правового регулирования облачных технологий оказывают международные акты, которые активно изменяются в связи с эволюцией сферы регулирования, судебные прецеденты, инциденты в сфере предоставления услуг. Благодаря этому постепенно начинает формироваться новый институт правового регулирования – национальное облачное право, состоящий, на данный момент, из целой системы разнородных нормативных актов. В данной статье автор предпринимает попытку кратко изложить основные особенности уже сложившегося правового регулирования на примере нескольких стран Азиатско-Тихоокеанского региона, уделяя внимание вновь принятым законодательным актам, путям предполагаемого развития нормативных актов, становящимся ключевыми в современном мире облачных услуг.

Ключевые слова: облачные технологии, облачные вычисления, регулирование облачных технологий, национальное законодательство в сфере ИТ, киберправо, цифровые отношения, право стран АТР, Китайская Народная Республика, Республика Корея, Австралия.

¹ Ярослава Олеговна Кучина, кандидат юридических наук, LL.M., доцент, доцент кафедры уголовного права и криминологии Юридической школы Дальневосточного федерального университета, г. Владивосток, Россия.

Для цитирования: Кучина Я.О. Законодательное регулирование облачных технологий в некоторых странах Азиатско-Тихоокеанского региона // Азиатско-Тихоокеанский регион: экономика, политика, право. 2018. № 1–2. С. 131–139.

Yaroslava O. Kuchina¹

Far Eastern Federal University, Vladivostok, Russian Federation

E-mail: kuchina.yao@dvfu.ru

**LEGISLATIVE REGULATION OF CLOUD TECHNOLOGIES
IN SOME COUNTRIES OF ASIA PACIFIC REGION**

Abstract. Digital technologies in the modern world often have no borders or limitations. Like any competitive IT, technologies that specialize in the circulation of services in the cloud, developed in one country, mostly function similarly in other countries. There may be grounds for believing that laws in these countries should be the same, but it is not the case. The specific features of the specific legal system, legal history and traditions of the state lead to differences in this area. In addition, international acts that are actively changing in connection with the evolution of the regulatory sphere, judicial precedents, and incidents in the provision of services have an impact on the specifics of the legal regulation of cloud technologies. Thanks to this, a new institution of legal regulation is gradually being formed - a national cloud law, consisting, at the moment, of a whole system of diverse normative acts. In this article, the author attempts to briefly outline the main features of the already established legal regulation in the case of several countries in the Asia-Pacific region, paying attention to the newly adopted legislative acts, the paths of prospective development that become key factors in the modern world of cloud services.

Keywords: cloud technologies, cloud computing, cloud technology regulation, national IT legislation, cyber law, digital relations, the law of the APR countries, People's Republic of China, The Republic of Korea, Australia.

Транснациональная природа облачных услуг вызывает больше правовых вопросов, чем «локализованные» компьютерные технологии, особенно в плане соотношения национального законодательства, международных норм и системы соглашений (договоров), которые непосредственно регулируют предоставление облачных услуг. Исследование ряда научных работ позволяет заключить, что национальной нормой в этой системе отведено последнее место, поскольку виртуализованная технология не может быть привязана к юрисдикции конкретной страны. Однако такой вывод будет ошибочным, поскольку в настоящее время большинство государств, заинтересованных в тех преимуществах, что приносят экономике облачные технологии, активно развивают законодательное регулирование в этой области.

¹ Yaroslava O. Kuchina, Candidate of Law Sciences, Assistant Professor of the Department of Criminal law and Criminology, Law School, Far Eastern Federal University, Vladivostok, Russian Federation.

For citing: Kuchina Yaroslava O. Legislative regulation of cloud technologies in some countries of the Asia Pacific region // ASIA-PACIFIC RIM: Economics, Politics, Law. 2018. N 1–2. P. 131–139.

На основе законодательной практики ряда стран АТР мы можем выделить несколько важных моментов, касающихся национального облачного регулирования. Во-первых, было бы разумно предположить, что, поскольку в технологическом смысле облака одного государства ничем не отличаются от облаков в другом, законодательное регулирование также должно совпадать в ряде ключевых моментов. Однако это не так. Необходимо отметить, что не только правовая система, но и государственная политика, история права и прочие элементы существенным образом влияют на облачное законодательство в пределах каждой конкретной страны. А потому различия существенны.

Первым государством (и, насколько нам удалось определить, единственным на данный момент), имеющим специализированный нормативно-правовой акт о регулировании облачных технологий, стала Республика Корея. 9 сентября 2015 г. южнокорейское министерство науки (Ministry of Science, ICT and Future Planning, MSIP) установило и объявило о «Мерах защиты информации для повышения эффективности облачных сервисов» [1] в ожидании активного использования облачных вычислений на основе реализации Закона «О продвижении облачных вычислений и защите пользователей» от 28 сентября 2015 г.

Этот закон представляет собой попытку законодательно урегулировать повышение соревновательного потенциала страны в общей гонке за развитие облачных технологий, которую Республика Корея в настоящий момент проигрывает Китаю. Закон представляет собой интереснейший опыт урегулирования облачного рынка, позволяя частному облачному сервису принимать участие в государственном секторе, стимулирует инвестиции в исследования и обязывает строить законодательную базу для адекватной защиты данных пользователей облачных вычислений – т.е. содержит в себе положения относительно государственной политики разрешения всех тех проблем, что становятся «роковыми» для национальных облачных провайдеров, особенно в условиях конкуренции с компаниями-гигантами из США.

Закон также устанавливает обязанность провайдера сообщать об утере информации пользователям, которые, в свою очередь, получают право требовать доступа к персональным данным, хранящимся за рубежом. Кроме того, Закон запрещает раскрытие информации третьим лицам и инструктирует их уничтожать информацию пользователя, когда они перестают предоставлять услугу, тем самым закрепляя принцип о «праве быть забытым». В нём также предусмотрена ответственность облачных провайдеров за ущерб пользователю, явившийся последствием нарушения конфиденциальности данных. Это положение является редчайшим примером исключения возможности ограничения ответственности провайдера, принятого в мире как одна из распространённых договорных практик в облачных соглашениях стандартного типа. При этом, согласно разъяснениям экспертов-юристов, Закон также обязывает иностранных провайдеров раскрывать личную информацию о

пользователях, хранящуюся за рубежом, причем эти положения обязательны для любых поставщиков облачной услуги, включая «мировых монополистов» вроде Google или Apple [2].

«Меры защиты информации для повышения эффективности облачных сервисов» представляют собой план по выдвижению на передний план ряда проблем, которые будут решены к 2019 г. В число этих проблем включены следующие:

1. Совершенствование уровня информационной безопасности облачных сервисов и создание системы реагирования на аварийные ситуации:

1.1. Подготовка и внедрение стандартов защиты облачной информации, включая административные и технические меры, которые должны соблюдать облачные провайдеры в целях защиты информации.

1.2. Создание и использование аналитического центра обмена информацией в облаках в качестве системы предотвращения случаев нарушения облака и управления группой реагирования на аварийные ситуации с целью сведения к минимуму ущерба, если такие случаи произойдут.

2. Создание Фонда защиты облачных пользователей:

2.1. Внедрение системы регистрации пользовательской информации для предотвращения потери информации пользователями и обеспечения совместимости между различными облачными службами.

2.2. Установка и распространение стандартного облачного соглашения, чтобы предотвратить ущерб пользователей, и подготовка документа «Стандарт качества и производительности облачного сервиса».

2.3. Подготовка и распространение «Рекомендаций по безопасному использованию облака» [3].

«Меры защиты информации для повышения эффективности облачных сервисов» связаны с повышением доверия к провайдерам облачных вычислений и защите пользователей, согласно прямому указанию в ст. 4 Закона «О продвижении облачных вычислений и защите пользователей». Меры направлены на смягчение проблем с нарушениями информационной безопасности, что является самым серьезным препятствием, которое в настоящее время мешает распространению облачных услуг среди пользователей, особенно корпоративных. Меры являются частью тенденции постепенного совершенствования правил, касающихся защиты информации, реализуемой корейским правительством с 2011 г. [4].

Применительно к этому нужно отметить, что национальное регулирование облачных технологий не может полностью избежать международного влияния. Это происходит либо тогда, когда причина изменения процедуры предоставления услуг монополистами в этой области ИТ начинает ограничивать национальный рынок, либо же когда судебный прецедент (или иная правоприменительная практика) начинает диктовать международную политику и существенно влияет на политику

внутри конкретной страны. Так было в случае с инцидентом Эдварда Сноудена, после которого множество государств, независимо друг от друга, приняли законы о запрете хранения персональных данных за пределами государственных границ, существенно повлияв на транснациональные характеристики облачных услуг. Однако это же порой ведёт к ситуации, когда одна и та же компания, одновременно предоставляя облачные услуги для местного и иностранного потребителя, предлагает им разные по форме и содержанию договоры.

Это порождает тенденцию, которая, на наш взгляд, является самой важной: если национальные и международные стандарты разнятся слишком сильно, в пределах государства возникает «закон в законе», что делает национальное облачное право практически мертвым, особенно если в стране отсутствуют судебные споры в этой области. Это свойственно ряду стран СНГ, где компьютерное законодательство отстаёт от своего же технологического рынка.

Эта тенденция не слишком очевидна правоприменителю или участнику облачного правоотношения, только пока не наработано достаточно количества судебной практики в данной сфере (например, в Австралии нами было найдено всего два иска, в 2005 и в 2014 гг.). Но очевидно, что такая ситуация не может длиться бесконечно, особенно если на национальном рынке относительно облачных технологий возрастает потребительский интерес. Мы считаем необходимым заметить, что полагать, будто национальное облачное регулирование изначально более низкого качества, чем международные нормы, – неверно. Однако бездействие в описанной ситуации может губительно сказаться на развитии рынка облачных технологий вообще, потому что, устав ждать достаточного уровня единообразия, потребители обратятся к иностранным провайдерам, которые следуют менее двусмысленной практике.

Основными областями правового регулирования, с которыми сталкиваются государства, являются те же – защита данных, неприкосновенность личности, вопросы применимого права, доступ третьих лиц и т.д., однако пути их решений могут разниться, и при том существенно. Так в Австралии в 2014 г. были введены в действие тринадцать новых Принципов конфиденциальности (в рамках действующего Закона о конфиденциальности 1998 г.), с целью как можно более подробно урегулировать вопросы собирания, хранения, использования и передачи персональных данных. Эти Тринадцать принципов заменили Национальные принципы конфиденциальности, которые действовали в отношении юридических лиц. С ними можно ознакомиться в Поправке о конфиденциальности от 2012 г. [5, 6, 7, 8]. На данный момент они устанавливают пределы использования персональных данных для всех государственных органов, действующих на территории Австралии и Норфолкских островов, для некоммерческих и коммерческих организаций, для субъектов, предоставляющих медицинские услуги, и некоторых представителей малого и среднего предпринимательства. Помимо этого они могут быть применены как к

компьютерной, так и облачной технологиям. Остановимся на основных принципах, которые стоит рассмотреть, применительно к исследованию регулирования облачных технологий.

Первый принцип обязывает провайдеров обрабатывать персональные данные, руководствуясь принципами открытости и прозрачности. Сюда входит необходимость указывать актуальную информацию о конфиденциальности, которая должна быть размещена открыто и раскрывать, каким образом данные собираются и для чего, а также какая информация подлежит сбору. Такие требования открывают большие перспективы для облачных провайдеров, поскольку делают облачные договоры понятнее для потребителя, а также позволяют провайдеру не нести ответственность за информацию, которая им не собиралась для обеспечения предоставления услуги.

Второй принцип регулирует вопросы анонимизации данных и устанавливает правило, согласно которому ряду лиц может быть дано право не идентифицировать себя, взаимодействуя с технологией или услугой. Этот принцип также определяет, что именно является персональными данными, а что нет, включая такие сложные для определения моменты, как содержание электронной почты.

Третий принцип касается сбора запрошенных личных данных, которые определяются как данные, которые «объективно необходимы или напрямую относятся» [9] к осуществлению провайдером определённых функций или предоставлению конкретных услуг.

Шестой принцип регулирует вопросы раскрытия информации третьим лицам, что, как мы уже объясняли, является наиболее деликатным вопросом предоставления облачных услуг. Согласно этому принципу, собранная информация не может быть раскрыта, если она собиралась для конкретной цели, а цель раскрытия – иная. Перечень назначения сбора информации и исключений из принципа прилагается. И здесь сразу необходимо упомянуть восьмой принцип, касающийся трансграничного раскрытия данных. Это возможно только если субъект, ответственный за сбор персональных данных, предпримет все возможные обоснованные меры исключить нарушение Принципов субъектом, которому данные будут переданы.

Последним принципом, относящимся к облачным технологиям, является одиннадцатый. Он регулирует правила обеспечения сохранности персональных данных и обязанность уничтожить персональные данные. Согласно ему «уничтожение или деперсонализация персональных данных» обязательны, если они более не нужны для целей, для которых были собраны или им угрожает раскрытие [9].

Как мы видим, сама система Принципов и то, как они организованы, отличаются в лучшую сторону от широко применяемых нормативно-правовых актов, проанализированных в предыдущих частях исследования. Полагаем, что такая система формулирования и изложения несомненно более подходит для эффективного регу-

лирования предоставления облачных услуг, поскольку она в упорядоченной и категоричной манере устанавливает стандарты наиболее важного (для пользователя) аспекта использования облаков – сохранности данных, которые им туда помещены. Особенности облачных технологий позволяют существенно злоупотреблять этой привилегией, поскольку это позволяет «неочевидность» технологических процессов для потребителя. Решением этой проблемы становятся именно такие упорядоченные правила обращения с персональными данными, какие представляют из себя Тринадцать принципов. К сожалению, сравнительно недавнее их введение исключает наличие судебной практики, позволяющей оценить, насколько эффективными они являются при предъявлении исковых требований и какие проблемы могут возникать в ходе применения нормы. Однако на данный момент нами не обнаружена хоть сколь-нибудь существенная их критика.

Отметим также, что, после ряда инцидентов с раскрытием данных пользователей третьим лицам без уведомления, многие государства решились на введение запрета хранить данные за пределами государства и связали их нахождение с местонахождением дата-контроллера.

Так, в 2015 г. Китайская Народная Республика (КНР) представила «Руководство о содействии инновациям и развитии облачных технологий с целью создания новых видов информационных услуг», которое определяет национальную политику и стратегическое развитие китайской облачной индустрии [10] и является базовым актом для дальнейшего развития законодательного регулирования облачных и сопутствующих услуг. В руководстве отдельно выделены вопросы безопасности данных и их защиты в облаках, а также вопросы раскрытия данных третьим лицам и вопросы хранения их в пределах и за пределами КНР.

Таким образом мы видим, что законодательство в сфере облачных технологий постепенно обретает свою форму и тенденции развития, при этом они не всегда следуют тому, что диктуют международные акты или сложившаяся контрактная практика облачного регулирования. Более того, складывается впечатление, что ряд стран предпринимает попытки «выйти» за пределы навязываемых им облачными провайдерами-монополистами рамок. Более всего это очевидно в сфере регулирования предоставления облачных услуг частного характера или для государственных нужд. Однако, как мы можем заметить, и обычный потребитель, вступающий в публичное правоотношение с облачным провайдером, постепенно попадает в сферу интересов законодателя, что, вполне возможно, приведёт к созданию национальных облачных законодательных институтов.

СПИСОК ЛИТЕРАТУРЫ

1. New Cloud Computing Legislation In South Korea [Электронный ресурс] // MAPPING Policy Observatory. – Режим доступа: <https://observatory.mappingtheinternet.eu/item/new-cloud-computing-legislation-in-south-korea>.
2. South Korea Cloud Computing Legislation Labelled «World First». [Электронный ресурс]. – Режим доступа: http://www.e-comlaw.com/data-protection-law-and-policy/article_template.asp?ID=1328&Search=Yes&txtsearch=put.
3. Ministry of Science, ICT and Future Establishes «Information Protection Measures for Vitalization of Cloud Services» [Электронный ресурс]. – Режим доступа: <https://s3.amazonaws.com/documents.lexology.com/ca41d0ff-0334-4093-971b-5202d0d3017d.pdf>.
4. BSA report on the level of legislative regulation of cloud security in the Republic of Korea [Отчет BSA об уровне законодательного регулирования безопасности облачных технологий в Республике Корея] [Электронный ресурс] // Country_Report_Korea. – Режим доступа: http://cloudscorecard.bsa.org/2012/assets/PDFs/country_reports/Country_Report_Korea.pdf.
5. Privacy Act 1988 [Электронный ресурс]. – Режим доступа: http://www5.austlii.edu.au/au/legis/cth/consol_act/pa1988108/.
6. Privacy fact sheet 2: National Privacy Principles (replaced on 2014, March 12) [Электронный ресурс]. – Режим доступа: <https://www.oaic.gov.au/privacy-law/privacy-archive/privacy-resources-archive/privacy-fact-sheet-2-national-privacy-principles>.
7. Australian Privacy Principles 2014 [Электронный ресурс]. – Режим доступа: <https://www.oaic.gov.au/privacy-law/privacy-act/australian-privacy-principles>.
8. Privacy Amendment (Enhancing Privacy Protection) Act 2012 [Электронный ресурс]. – Режим доступа: <https://www.legislation.gov.au/Details/C2012A00197>.
9. De Busser, E. Data Protection in EU and US Criminal Cooperation: A Substantive Law Approach to the EU Internal and Transatlantic Cooperation in Criminal Matters between Judicial and Law Enforcement Authorities / E. De Busser. – Antwerp ; Apeldoorn ; Portland : Maklu, 2009. – 474 p.
10. Руководящие мнения по содействию инновациям и развитию облачных вычислений для развития новых видов информационных услуг (2015 г.) [Электронный ресурс]. – Режим доступа: http://www.gov.cn/zhengce/content/2015-01/30/content_9440.htm. – Кит.

REFERENCES

1. New Cloud Computing Legislation in South Korea. *MAPPING Policy Observatory*. Available at: <https://observatory.mappingtheinternet.eu/item/new-cloud-computing-legislation-in-south-korea> (accessed 14 May 2018).

2. South Korea Cloud Computing Legislation Labelled «World First». Available at: http://www.e-comlaw.com/data-protection-law-and-policy/article_template.asp?ID=1328&Search=Yes&txtsearch=put (accessed 14 May 2018).

3. *Ministry of Science, ICT and Future Establishes «Information Protection Measures for Vitalization of Cloud Services»* Available at: <https://s3.amazonaws.com/documents.lexology.com/ca41d0ff-0334-4093-971b-5202d0d3017d.pdf> (accessed 14 May 2018).

4. BSA report on the level of legislative regulation of cloud security in the Republic of Korea. *Country_Report_Korea*. Available at: http://cloudscorecard.bsa.org/2012/assets/PDFs/country_reports/Country_Report_Korea.pdf (accessed 14 May 2018).

5. *Privacy Act 1988*. Available at: http://www5.austlii.edu.au/au/legis/cth/consol_act/pa1988108/ (accessed 14 May 2018).

6. *Privacy fact sheet 2: National Privacy Principles (replaced on 2014, March 12)*. Available at: <https://www.oaic.gov.au/privacy-law/privacy-archive/privacy-resources-archive/privacy-fact-sheet-2-national-privacy-principles> (accessed 14 May 2018).

7. *Australian Privacy Principles 2014*. Available at: <https://www.oaic.gov.au/privacy-law/privacy-act/australian-privacy-principles> (accessed 14 May 2018).

8. *Privacy Amendment (Enhancing Privacy Protection). Act 2012*. Available at: <https://www.legislation.gov.au/Details/C2012A00197> (accessed 14 May 2018).

9. De Busser, E. *Data Protection in EU and US Criminal Cooperation: A Substantive Law Approach to the EU Internal and Transatlantic Cooperation in Criminal Matters between Judicial and Law Enforcement Authorities*. Antwerp; Apeldoorn; Portland: Maklu, 2009. 474 p.

10. *Guiding Opinions for Promoting the Innovation and Development of Cloud Computing to Cultivate New Types of Information Industry Services (2015)*. Available at: http://www.gov.cn/zhengce/content/2015-01/30/content_9440.htm (accessed 14 May 2018). (In Chinese).