ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ ОБЛАЧНЫХ СЕРВИСОВ

Сатикова Дария Маратовна
Аспирант,
Сколковский институт науки и технологий

THE PROCESSING OF PERSONAL DATA USING CLOUD SERVICES

D. Satikova

Annotation

Currently, the topic of cloud computing is not well developed in the legal field and the use of cloud technologies raises many questions in connection with the application of tax legislation, the definition of the applicable contract structure, the application of personal data law and other aspects. "The areas of relations that need to be resolved when using cloud technologies are the same for any legal system. In most countries, state regulation of the use of cloud technologies is carried out by international and national legislation, which can be classified as sectoral or "sector". There are also certain aspects of legal relations, the rules of which are applied by analogy with the law or by analogy with the law" says Yu. S. Kozhevnikova [1].

International law provides a jurisdictional framework for the regulation of cloud computing in different countries in accordance with its extraterritorial effect [2]. Basically, the legal regulation of cloud computing combines international and national legislation in a specific area of law. Many provisions on cloud computing are also postulated by guidelines and technical documents, such as corporate rules related to processor processing [3] or international standards (e.g. ISO standards).

Until recently, the company worked mostly with isolated localized data sets and processes. The ability to transmit information was technically limited by the number of participants and the amount of information. Over the past few years, cloud computing has begun to be used by an incredible number of users, including large companies such as Google, Microsoft and Amazone, who have moved their data to the clouds. As has already been shown, the cloud computing market is growing, especially on social networks: Facebook, Twitter or Instagram [4].

Thus, the majority of offenses arising in the field of cloud computing regulation are often connected with public law, such as criminal and antitrust laws or personal data protection issues [5].

Keywords: legal framework, international law, offence, jurisdiction, corporate rules.

Аннотация

В настоящее время тема облачных вычислений мало проработана в правовом поле и использование облачных технологий вызывает множество вопросов в связи с применением налогового законодательства, определением применимой договорной конструкции, применением законодательства о персональных данных и другими аспектами. "Сферы отношений, урегулирование которых требуется при использовании облачных технологий, одинаковы для любой правовой системы. В большинстве стран государственное нормативное регулирование использование облачных технологий осуществляется международными и национальными законодательными актами, которые можно отнести к категории отраслевых, или "секторных". Также есть отдельные аспекты правоотношений, нормы к которым применяются по аналогии закона или по аналогии права" отмечает Кожевникова Ю.С. [1]

Международное законодательство предоставляет юрисдикционную основу для регулирования облачных вычислений в разных странах в соответствии с его экстерриториальным эффектом [2]. В основном правовое регулирование облачных вычислений сочетает международное и национальное законодательство в конкретной области права. Многие положения об облачных вычислениях также постулируются рекомендациями и техническими документами, например корпоративными правилами, связанными с обработкой процессором [3] или международными стандартами (например, стандарты ISO).

До недавнего времени компании в основном работали с локализованными изолированными наборами данных и процессами. Возможность передачи информации была технически ограничена количеством участников и объемом информации. В течение последних нескольких лет облачные вычисления начали использоваться невероятным числом пользователей, включая такие крупные компании, как Google, Microsoft и Amazone, которые перенесли свои данные в "облака". Как уже было показано, рынок облачных вычислений растет, особенно в социальных сетях: Facebook, Twitter или Instagram [4].

Таким образом, большинство правонарушений, возникающих в области регулирования облачных вычислений, часто связанно с публичным правом, таким как уголовное и антимонопольное законодательство или вопросы защиты персональных данных [5].

Ключевые слова:

Правовое поле, международное законодательство, правонарушение, юрисдикция, корпоративные правила.

Субъектами отношений по обработке персональных данных являются субъект персональных данных, оператор персональных данных и Лицо, осуществляющее обработку персональных данных по поручению оператора (технический посредник). В случае с использованием облачных сервисов возможны несколько основных сценариев распределения ролей и много вариантов смешанных сценариев. В данной таб-

лице анализируются только роли пользователя и провайдера без учета третьих лиц, участвующих в формировании экосистемы облачного сервиса, например владельцев серверных мощностей, интегрированных сервисов и прочих. Вся совокупность лиц участвующих в создании облачной экосистемы представлена провайдером.

Сейчас почти полностью отношения между пользователем и провайдером регулируются договором [6]. Более того, большая часть облачных сервисов работает по модели "click–through", без права обсуждения и внесения правок в такое соглашение. Так, например, благодаря такому соглашению сервис может в процессе использования собирать информацию cookies пользователя с целью таргетирования рекламы. Кристофер Миллард отмечает, что на практике провайдеры часто меняют условия таких соглашений в одностороннем порядке [7].

По модели заключения договора с провайдером возможно несколько вариантов:

- прямые отношения: провайдер и пользователь заключают договор напрямую; при этом провайдер может использовать дополнительные сервисы, но стороной договора с пользователем выступает именно он;
- отношения через интегратор, когда облачный сервис входит в интегратор и договор заключается между интегратором и пользователем;
- система договоров пользователя с интегратором и сервисами.

При таком количестве участников, пользователю, при заключении договора надо в том числе понимать, как выглядит экосистема облачного сервиса и сколько реальных провайдеров в нее интегрировано.

В соответствии с Конституцией РФ "сбор, хранение и распространение информации о частной жизни лица без его согласия не допускается", что безусловно прямо затрагивает категорию "персональных данных". Человек и его права и свободы стоят во главе угла для законодателя. Закон о персональных данных также содержит принципы и правила обработки персональных данных.

В соответствии со ст.19 закона персональных данных на оператора персональных данных возлагается обязанность по принятию необходимых правовых, организационных и технических меры защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения и иных неправомерных действий. Иными словами оператор должен осуществлять контроль за процессами обработки персональных данных, что в случае с использованием облачного сервиса сложнее, чем при использовании внутренних систем по описанным далее причинам.

В соответствии с зарубежным опытом ответственность за проверку надежности облачного сервиса также перекладывается на оператора (например, по закону о данных о страховании здоровья граждан (Health Insurance Portability and Accountability Act) или в соответствии с законом Грэма–Лича–Блайли (Gramm–Leach–BlileyAct)). Именно оператор должен убедиться в соответствии мер технической защиты требованиям законодательства и обработке данных исключительно в заявленных целях. Требования, которые бы распространялись на оператора, если бы обработка данных осуществлялась на его внутренних ресурсах, соответствуют требованиям обработки во внешней среде облачного сервиса. Также, если доступ к данным есть у персонала облачного сервиса, необходимо убедиться, что их действия также соответствуют вышеперечисленным требованиям [8].

Таким образом, оператор персональных данных вынужден понимать структуру облака, в том числе знать место нахождения не только основных серверов, но и серверов с резервными копиями данных. Например, резервные копии данных Amazon.com Inc. хранятся в крупнейших центрах данных в США и Ирландии в силу организации технических внутренних процессов компании, однако такое решение может встретить серьезные правовые проблемы, например, обязанность получить дополнительное согласие от субъекта персональных данных на трансграничную передачу.

В опубликованном в апреле 2013 года на сайте Минкомсвязи исследовании "Нормативно– правовое обеспечение возможности использования облачных технологии органами государственнои власти и органами местного самоуправления"также были обозначены проблема неурегулированности вопросов безопасности данных, в частности отсутствие четко–определённой административной, граданско–правовой или уголовной ответственности у провайдера облачного сервиса [9]. Фактически п. 3 ст. 6 перекладывает на оператора обязанности по информированию лица, осуществляющего обработку данных по поручению (если даже отнести провайдера к данной категории) о принципах и условиях обработки данных. Оператор обязан в рамках договора с третьей стороной обеспечить законодателем закрепленный уровень безопасности данных, что подтверждается существующей судебной практикой [10].

Тем не мене, хоть облачные технологии и представляют собой сложную структуру, однако структуру контролируемую, и миф об абсолютной невозможности контроля за данными при использование облачного сервиса не обоснован. Требования безопасности обработки конфиденциальных данных (в том числе не только персональных, но и данных, конфиденциальность которых предусмотрена в рамках коммерческой и государственной тай–

ны) диктуют свои условия рынку облачных технологий и находят соответствующие технологические решения с помощью алгоритмов шифрования данных и иных. На данный момент халатность сотрудника предоставляет для данных, помещенных в облако угрозу большую, чем хакерская атака или несовершенства технологии [11]. В соответствии с данными аналитиков InfoWatch по утечке конфиденциальных данных за 2017 год в 61,8% случаев утечка происходила по вине так называемых "внутренних хакеров" – сотрудников компании, внутренних подрядчиков и бывших работников [12]. В данном случае облачное решение, из которого сотрудник не имеет возможности "выкачать" базу данных работодателя может являться гораздо более безопасным, чем база данных размещенная на ноутбуке сотрудника.

Облачный сервис благодаря масштабируемости, удаленному доступу и инфраструктурным возможностям представляет собой крайне эффективный инструмент ведения бизнеса, поэтому крупные компании заинтересованы в поиске решений, которые будут удовлетворять требования законодательства о защите данных, в том числе персональных, но не будут при этом мешать пользоваться преимуществами такого сервиса.

В связи с использованием облачных сервисов для обработки персональных данных можно выделить следующие проблемные аспекты обработки:

1. Хранение данных

По мнению экспертов, вопросы безопасности облачных хранилищ данных в 2017 году являются приоритетным направлением развития технологии, так как "облака" становятся самым удобным инструментом долгосрочного хранения и обработки данных [13].

Контроль качества предоставляемой услуги, в том числе безопасности данных в системе на данный момент регулируется преимущественно в рамках SLA. Однако, особенно если сервис бесплатный, поставщик услуги не сильно связывает себя обязательствами относительно качества сервиса. Не так давно компания Google удалила целиком онлайн дневник американского писателя Дениса Купера с сервиса Blogspot без объяснения причины. Пропал уникальный контент, который автор создавал 14 лет, и если бы не большой общественный резонанс, который вызвала эта ситуация, представители компании могли отписаться от жалобы без объяснения причин, что они и пытались сделать [14]. Сервисы компании Google нельзя назвать по-настоящему бесплатными, так как они магнетизируют данные, которые по умолчанию получают от пользователей в "оплату" доступа. Тем не менее, законодательно не урегулировано, являются ли такие бартерные отношения основанием требовать определенного уровня качества сервиса.

Экс-директор по безопасности Моторолла солушнс Патрик Кэнингем в одном из выступлений акцентировал внимание на том, что даже платное облако не является гарантом безопасности данных. Может оказаться, что фирма, предоставляющая услуги по хранению и обработке данных, на самом деле арендует сервера у японской компании, которая размещает их где-то в Южной Африке и это достаточно типичная ситуация [15].

Глава фонда свободного программного обеспечения (Free Software foundation, FSF) Ричарда Столлман подвергает сомнению безопасность облачных сервисов: "В случае услуги вместо программы у пользователя нет даже исполняемого файла программы, которая проводит его вычисления: он находится на чужом сервере, где пользователи его не видят и не осязают. Таким образом, для них невозможно проверить, чем в действительности занята программа, и невозможно изменить ее" [16].

А. Бережной отмечал, что в вопросах безопасности данных внутри системы не всегда можно полагаться на поставщика услуг в том числе в связи не проработанностью правового регулирования облачных сервисов. В связи с развитием экономического значения "облаков" по мнению А. Бережного скоро последует развитие нормативно правовой базы [17]. На данный момент ответственность за безопасность персональных данных лежит на операторе данных, однако, как было указанно ранее он не всегда может контролировать внутренние процессы облачного сервиса. Одним из выходов из данной ситуации является уже опоминавшаяся ранее стандартизация услуг доступа к облачным сервисам (например, ISO). Насколько применимы в данной сфере законодателем установленные требования к качеству предоставляемых услуг, например, механизмы законодательства о защите прав потребителей, – большой вопрос.

А. И. Савельев указывает на еще одну особенность хранения данных: "Поскольку стоимость хранения упала, оправдать сбор и хранение огромных массивов информации стало гораздо проще, что стимулирует менеджмент организаций к принятию прагматичных решений об игнорировании принципа ограничения обработки персональных данных заранее определенной целью, равно как и ряд иных положений законодательства о персональных данных" [18], таким образом нельзя быть до конца уверенным, что провайдер не оставил себе резервную копию с базой данных оператора. Без прозрачной структуры облачного сервиса отследить такие незаконные действия провайдера представляется очень сложным.

2. Передача данных

Одна из особенностей облачных сервисов состоит в том, что серверы (технические мощности) могут физически быть расположены в любой стране мира и даже в ко-

смосе [19]. Это означает, что ценная информация может физически находиться где угодно. Некоторые протоколы шифрования специально разбирают информацию на бессмысленные части и размещают ее на разных серверах, так чтобы только пользователь мог получить доступ к целому файлу.

Особенности структуры облака таковы, что пользователь может даже не знать о происходящей трансграничной передаче данных.

Одним из первых случаев в сфере государственного регулирования трансграничной передачи данных является инцидент с конца 1980-х годов, связанный с Fiat-France и Fiat-Italy, двумя компаниями, которые обменивались информацией о сотрудниках [20]. Франция приняла закон о защите данных, в то время как Италия не имела такого института в правовой системе, поэтому Fiat-France было настоятельно рекомендовано подписать соглашение с Fiat-Italy, устанавливающее уровень защиты персональных данных в соответствии с французским законодательством. Только после подписания такого соглашения правительство разрешило компаниям передавать данные.

В настоящее время невозможно представить, чтобы правительство контролировало каждую передачу персональных данных, в том числе с помощью облачных сервисов. Объем глобальных данных значительно возрос. Рабочая группа ЕС по защите данных подтвердила: "Облачные вычисления чаще всего основаны на полном отсутствии устойчивого местоположения данных в сети провайдера облачных вычислений. Данные могут находиться в одном центре обработки данных в 2 часа дня и на другой стороне света в 16:00" [21]. Законодатель вынужден вместо личного контроля закреплять требования о надлежащем уведомлении субъекта персональных данных о передаче в менее защищенную страну.

Проблема трансграничной передачи типична не только в отошении стран третьего мира, но и остро стоит в трансатлантических отношениях между европейскими странами и США, в силу отличия требований национального законодательства к уровню защиты данных. Попытки унифицировать законодательство в этой сфере с помощью создания европейско-американской системы защиты персональных данных (EU-US Privacy Shield) встречают сложности с американской стороны и вынуждают крупные международные компании дополнительно вырабатывать внутренние стандарты[22].

3. Обработка баз данных внутри облака

Как отмечает Нестерова И.А. в своем исследовании со ссылкой на основные тренды в области развития облачных сервисов: "Прозрачность отношений и обязательств сторон по вопросам защиты данных и пользовательского контроля над данными сегодня является очень важным и основополагающим моментом для физических лиц в части защиты персональных данных от утечки и несанкционированного доступа и возможности контролировать локализацию и распространение таких данных"[23].

Одним из последних случаев, показывающих разницу в европейской и американской правовых моделях, является то, что власти ЕС в сфере защиты персональных данных возражают против политики Google в отношении конфиденциальности при компиляции персональных данных из всех их сервисов: Google Apps, Gmail и Документов Google, YouTube и Google+ [24].

По мнению властей, такая широкая политика конфиденциальности нарушает право пользователя контролировать данные, которые будут обрабатываться в разных целях, и тогда Google получит доступ к неограниченной информации о пользователе. В Комиссии по защите данных Рабочей группы по статье 29 установлено, что пользователь облачного сервиса не может "определить, какие категории персональных данных обрабатываются ... и точные цели, для которых эти данные обрабатываются".

Google указал на пользу получаемых в результате услуг для потребителей, но такой аргумент сработал только в США, в то время как европейские власти поставили Google под контроль национальных комиссий по защите данных. Это вынудило Google внести некоторые улучшения, например, брать с пользователей согласие на обновления, установить дополнительные механизмы согласия, прежде чем объединять данные сервисы [25].

На данный момент в России отсутствует централизованное законодательное регулирование облачных сервисов, однако совершаются определенные движение в направлении развития облачных инфраструктур и соответственно определенного регулирования в данной сфере. В рамках Российской ассоциации электронных коммуникации была сформирована комиссия по правовым вопросам использования SaaS – технологий, целью которой является изучение лучших международных и зарубежных практик [26].

Разработанная группой концепция правового регулирования облачных вычислений содержит следующие существенные выводы:

- российское законодательство не содержит специального регулирования облачных вычислений, основу регулирования отношений возникающих при использовании облачных сервисов составляет гражданское законодательство, международное частное право, законодательство о персональных данных и информационное право;

- договор между провайдером и потребителем составляет смешанный характер;
- действующее законодательство регулирует возникающие отношения рамочно, но не способствует развитию облачных технологий, а иногда и мешает ему [27].

На данный момент правовое регулирование облачных технологий существенно не изменилось и нуждается в корректировки соответственно требованиям баланса публичных и частных интересов, в частности в сфере защиты персональных данных.

ЛИТЕРАТУРА

1. Кожевникова Ю.С. Проблемы регламентации отношений, формирующихся при использовании облачных технологий: сочетание регулирования и саморегулирования. // ЮРИСТ, № 13,2014. [Электронный ресурс] ;
2. Vineeth Narayanan, "Harnessing the Cloud: International Law Implications of Cloud–Computing", 12 Chi. J. Int'l L. 783 (2011–2012)
3. Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, adopted on 6th June 2012: http://ec.europa.eu/justice/data–protection/article–29/documentation/opinion–recommendation/files/2012/wp195_en.pdf
4. Anthony Hemond, "Canadian Perspectives on Cloud Computing and Consumer", Final report to Industry Canada?s Office of Consumer Affairs, available at http://uniondesconsommateurs.ca/docu/vieprivee/CloudComputingE.pdf?
5. Vineeth Narayanan, "Harnessing the Cloud: International Law Implications of Cloud– Computing", 12 Chi. J. Int'l L. 783 (2011–2012)
6. Нестерова И.А. Правовое регулирование отношений, возникающих при использовании облачных технологий: Дисс. ... канд. юрид. наук. – М., 2016.
7. Cloud computing Law, edited by Christopher Millard // Oxford University Press, 2013.
8. Вик Дж. Р. Уинклер Облачные вычисления: Конфиденциальность данных в облаке [Электронный ресурс] / Режим доступа: https://technet.microsoft.com/ru–ru/magazine/jj554305.aspx (Дата обращения: 20.04.2017)
9. Электронный ресурс / Режим доступа: http://www.minsvyaz.ru/ru/documents/3831/#tdocumentcontent (Дата обращения: 11.01.2016)
10. Постановление Федерального арбитражного суда Северо–Западного округа от 29 апреля 2013 г. N Ф07–1799/13 по делу N А44–5910/2012; Постановление Арбитражного суда Северо–Западного округа от 6 мая 2015 г. N Ф07–488/15 по делу N А21–4273/2014
11. Lothar Determann Data privacy in the cloud: a dozen myths and facts. Aprill, 2012 [Электронный ресурс] / Режим доступа: URL: http://www.iitr.us/publications/14–data–privacy–in–the–cloud–a–dozen–myths–and–facts.html (Дата обращения: 01.12.2016)
12. Ли И. Россия стала второй после США по числу утечек конфиденциальных данных [Электронный ресурс] / Режим доступа: URL: http://www.rbc.ru/technology_and_media/23/03/2017/58d2bbb39a794721422e1588 (Дата обращения: 01.12.2016)
13. Jon Tilbury Opinion Preserving the future: What's next for digital preservation? https://www.information–management.com/opinion/preserving–the–future–whats–next–for–digital–preservation
14. Dennis Cooper's blog re–launched after Google censorship criticisms // https://www.theguardian.com/books/2016/aug/31/dennis–cooper–dcs–blog–relaunched–google–censorship
15. Источник: лист рассылки RECMGMT–L https://lists.ufl.edu/cgi–bin/wa?A2=ind1607C&L=RECMGMT–L&P=R2346&D=0
16. Richard M. Stallman. What Does That Server Really Serve? // Boston review URL: http://www.bostonreview.net/richard–stallman–free–softwareDRM (дата обращения 20.04.2017)
17. Бережной А. Облачные вычисления: Новое или хорошо забытое старое? // Системный администратор, спецвыпуск "Облачные вычисления", март 2011. С. 5
18. 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.
19. ConnectX wants to put server farms in space //http://www.geek.com/chips/connectx–wants–to–put–server–farms–in–space–1614728/
20. Commission nationale de l'informatique et des libertes, 1oe rapport dactivite [national commission on informatics and liberties, 10th activity report] 32 (1989). Reports of the National Commission are available online back through 1999, see Rapports d'activiti, Commission nationale de l'informatique et des libertes // http://www.cnil.fr/en–savoir–plus/rapports–dactivite/accessible/non
21. Article 29 Data Prot. Working Party, Opinion o5/2012 on Cloud Computing 17,(EC) No. 01037/12, WP 196 (July 1, 2012), availableat http://ec.europa.eu/justice/data–protection/article–29/ documentation/opinion–recommendation/files/2o12/wpl96en.pdf.
22. Lomas N. Trump order strips privacy rights from non–U.S. citizens, could nix EU–US data flows https://techcrunch.com/2017/01/26/trump–order–strips–privacy–rights–from–non–u–s–citizens–could–nix–eu–us–data–flows/
23. Нестерова И.А. Правовое регулирование отношений, возникающих при использовании облачных технологий: Дисс. ... канд. юрид. наук. – М., 2016.
24. Google's New Privacy Policy:I ncomplete Informationand Uncontrolled Combination of Data Across Services, Commission nationale de l'informatique et des libertrs (Oct. 16,2012)// http://www.cnil.fr/english/news–and–events/news/article/oogges–newprivacy–policy–incomplete–information–and–uncontrolled–combination–of–data–across–ser
25. Eric Pfanner, Google Faces More Inquiriments in Europe Over Privacy Policy, N.Y. TIMES, Apr. 3, 2013, at B4
26. Электронный ресурс / Режим доступа: http://raec.ru/rg/2552/ (Дата обращения: 23.12.2015)
27. Электронный ресурс / Режим доступа: http://easier.pro/news/legal/on_the_concept_of_legal_regulation_of_cloud_computing/ (Дата обращения: 23.12.2015)