

COMPUTAÇÃO EM NUVEM E CONSIDERAÇÕES CONTRATUAIS

Juliana Falci Sousa Rocha Cunha¹

RESUMO

A computação em nuvem é uma realidade tecnológica que está sendo amplamente adotada pelas empresas de grande porte. Assim sendo, visando a contextualização do tema em análise, o presente estudo aborda a *cloud computing* e a segurança da informação, sendo apresentadas algumas das vantagens e desvantagens/riscos, modelos de implantação e de serviço, bem como os principais serviços oferecidos pelos fornecedores de computação em nuvem. Em seguida, são abordadas questões jurídicas do contrato de *cloud computing*, com enfoque nas partes contratantes, no seu objetivo e nas principais cláusulas que devem ser tratadas neste contrato atípico, dentre elas a integridade e confidencialidade dos dados e informações, as possíveis falhas nos servidores e a responsabilidade do contratado, os requisitos para fornecimento de informações e o destino do conteúdo armazenado em caso de quebra de contrato.

PALAVRAS-CHAVE: computação; nuvem; tecnologia; responsabilidade; contrato.

CLOUD COMPUTING AND CONTRACTUAL CONSIDERATIONS

ABSTRACT

Cloud computing is a technological reality that is being increasingly adopted by big companies. To contextualise this subject the study deals with cloud computing and information security: advantages and disadvantages/risks, models of service and implementation and also the main services offered by cloud computing providers. Then legal issues of cloud computing contract will be presented, focussing on contracting parties, its goal and the main clauses which should be presented on this atypical contract, as the integrity and confidentiality of data and information, the possible failures in servers and the service provider responsibility, the requirements for supplying information and the destination of the content stored in case of contract breach.

KEY WORDS: computing; cloud; technology; responsibility; contract.

¹ Advogada e Professora Universitária. Mestranda em Direito Empresarial - Faculdade Milton Campos. Especializada em Direito Empresarial - Faculdades Milton Campos e em Direito Civil Faculdades Milton Campos. Graduada em Direito - Faculdades Milton Campos, Tecnologia em Processamento de Dados – Centro Universitário UNA e Administração de Empresas – Centro Universitário UNA. E-mail: jfcunha.bh@terra.com.br.

1 Introdução

O estudo proposto tem como tema central a computação em nuvem, o qual cada dia ganha mais relevância tanto no contexto internacional da tecnologia da informação quanto no âmbito jurídico e organizacional. Mas, o foco do presente estudo é a *cloud computing* utilizada por companhias de grande porte e não por pessoas físicas e empresas de pequeno porte.

Inicialmente será realizado o estudo da computação em nuvem e da segurança da informação, haja vista a necessidade de contextualização desta inovação tecnológica e de existirem muitos dados e/ou informações confidenciais armazenadas em nuvens que estão sujeitas, por exemplo, à acesso por pessoal não autorizado. Assim sendo, serão destacadas, por exemplo, as principais vantagens e desvantagens/riscos deste modelo de prestação de serviço, os modelos de implantação e de serviços e os diversos serviços ofertados pelas empresas fornecedoras de computação em nuvem.

Posteriormente será realizada uma análise do contrato de computação em nuvem, incluindo a sua classificação jurídica, o seu objeto e principalmente as cláusulas mais relevantes a serem discutidas e incluídas neste tipo de contrato, dentre elas a responsabilidade por possíveis falhas nos equipamentos do provedor do serviço, a confiabilidade e privacidade das informações, o fornecimento de informações a terceiros não autorizados, incluindo-se aí autoridades policiais e órgãos da justiça, bem como o destino das informações em caso de quebra de contrato.

Assim sendo, verifica-se que com a globalização e a crescente utilização do serviço de tecnologia da informação é essencial que as grandes corporações utilizem o serviço de computação em nuvem, tendo em vista as diversas vantagens que serão apresentadas. Entretanto, é essencial que o assunto seja analisado tanto sobre o enfoque da tecnologia da informação quanto jurídico, posto que os dados e informações estratégicas e sensíveis são armazenadas e processadas em nuvem de responsabilidade de um terceiro prestador de serviço. Desta maneira, é imprescindível um contrato de prestação de serviço bem elaborado, com cláusulas que abordem, por exemplo, a integridade da informação, a responsabilidade e o plano de ação do fornecedor do serviço em caso de indisponibilidade do serviço e a criptografia de dados.

2 A computação em nuvem e a segurança da informação

Atualmente as organizações encontram grande dificuldade de sobreviverem sem o suporte da tecnologia da informação, a qual possibilita significativas melhorias na competitividade organizacional.

Além disto, verificam-se o crescimento da velocidade da internet, a rápida e eficiente interação entre sistemas e o desenvolvimento de tecnologias que permitem fazer *online* o que anteriormente somente era realizado *off-line*, tais como a computação em nuvem.

Desta maneira, a *cloud computing* oferece mais vantagens do que desvantagens ao seu usuário, como por exemplo, permite que a empresa contratante foque no seu negócio e não em atividades meio como tecnologia da informação, gera maior produtividade, disponibiliza grande poder de processamento de dados e proporciona redução de custos.

Este novo recurso de informática possibilita que as organizações armazenem e processem os dados e/ou informações de maneira remota, inclusive permitindo com que eles sejam acessados à qualquer momento e de qualquer local, conforme os modelos de implantação e de serviço contratados.

Os serviços ofertados pelos provedores de computação em nuvem, podem ser vários, dentre eles o armazenamento de arquivos, a realização de *backups*, a disponibilização, gerenciamento e atualização de softwares e o suporte ao serviço.

Entretanto, para que as informações inseridas nas nuvens pelas empresas estejam seguras, é essencial que elas não sejam acessadas por terceiros, dentre eles concorrentes e governo. Desta feita, quanto à segurança da informação é importante que o prestador do serviço esteja atento, por exemplo, à identificação dos usuários que acessam as informações armazenadas, à utilização de criptografia e à segurança da infraestrutura dos seus provedores.

2.1 Conceito

Segundo MENKEN (2008):

Cloud computing is a style of computing in which dynamically scalable and often virtualized resources are provided as a service over the Internet. (...) Users need only be concerned with their terminal and Internet connection, so they can access the tools that the cloud can provide.

Para a referida autora, a computação nas nuvens é um serviço ofertado através da internet, no qual o usuário não se preocupa com os seus meios, mas somente com os resultados. Assim sendo, cabe ao prestador de serviço providenciar, por exemplo, os equipamentos e a segurança da informação.

Para VERAS (2013), o conceito de *cloud computing* é abordado de outra maneira:

O conceito de nuvem (...) é o conceito atual de nuvem pública (*PUBLIC CLOUD*). A ideia central da nuvem pública é permitir que as organizações executem boa parte dos serviços que hoje são executados em *DATA CENTERS* corporativos em *DATA CENTERS* na rede, providos por terceiros, podendo sair de um modelo baseado em Capex (custo de capital) para um modelo baseado em Opex (custo de operação) e onde agora os indicadores de desempenho estão atrelados aos níveis de serviço, principalmente disponibilidade e desempenho, acordados entre clientes e provedores. (...) A nuvem na verdade é um conjunto de grandes pontos de armazenamento e processamento de dados e informações. (...) *CLOUD COMPUTING* é um conjunto de recursos virtuais facilmente utilizáveis e acessíveis, tais como hardware, software, plataformas de desenvolvimento e serviços.

Como se pode observar, trata-se de um conceito voltado mais para a área de tecnologia da informação, tendo inclusive abordado questão empresarial relacionada ao investimento, que passa do modelo de aquisição de equipamentos para a aquisição de serviços, além dos indicadores de desempenho dos fornecedores do serviço. Ao final, o estudioso inclusive afirma que podem ser armazenados virtualmente tanto dados de interesse do cliente quanto aplicativos.

Para MARCHINI (2010) *cloud computing refers to the delivery of computing capability by a provider remotely over a communications link. It comes in many different varieties, serving a wide variety of computing needs*. Esse conciso conceito apresenta uma visão geral do que é computação nas nuvens, abrangendo o provedor do serviço e a remotabilidade do serviço oferecido.

De acordo com MONTERO (2013):

Algunos especialistas prefieren dividir la definición sobre el Cloud Computing en dos partes bien diferenciadas: por un lado, hacen referencia a los servicios en la nube como “productos, servicios y soluciones de consumo y empresariales que se ofrecen y consumen en tiempo real por Internet”; y por otro lado, definen la informática en la nube como “un modelo emergente de desarrollo, implementación y prestación de tecnologías de la información que permite la entrega en tiempo real de productos, servicios y soluciones por Internet (es decir, facilita los servicios de la nube).

Assim sendo, este autor acredita que a computação em nuvem é uma ferramenta de tecnologia que visa o fornecimento de serviços para terceiros.

Enfim, frente aos conceitos apresentados pode-se dizer que a computação em nuvens é um serviço ofertado por uma empresa às pessoas físicas ou jurídicas, mediante um contrato atípico, que permite o armazenamento de dados, informações, aplicativos etc em servidor da empresa contratada, possibilitando que o contratante ou outras pessoas autorizadas por ele tenham acesso seguro ao conteúdo armazenado de qualquer lugar e à qualquer momento.

2.2 Principais vantagens e desvantagens/riscos da computação em nuvem

2.2.1 Vantagens

Muitas são as vantagens que podem ser citadas para a adoção da computação em nuvem, mas a principal delas é o fato do usuário, a empresa no caso do presente estudo, não se preocupar em lidar com tarefas complexas de indexação de dados, podendo assim focar no seu *core business* e conseqüentemente ser mais competitivo, eficiente e rentável.

Outra vantagem é a possibilidade do usuário do serviço poder se beneficiar do enorme poder de processamento que lhe é ofertado pelo prestador do serviço de *cloud computing*, sem ter que investir grande capital em *hardware* e *software* (bem na sua manutenção e atualização) e na gestão da tecnologia.

Conseqüentemente, outra vantagem é a redução do custo, o que permite que o capital do cliente possua outra destinação relacionada ao negócio da empresa, como por exemplo, desenvolvimento de produto, pesquisa e recursos humanos. Para que a computação em nuvem seja implantada basta a disponibilização da internet, o que todas as grandes empresas já possuem, sendo que os dispositivos de conexão não precisam possuir recursos avançados, podendo ser muito mais simples do que aqueles que até então eram adquiridos pelas empresas que mantinham seus próprios centros de processamentos dados. Assim sendo, acredita-se que no futuro a organização que não transferir suas informações para a nuvem terceirizada certamente terá que arcar com grande despesa financeira.

Outra possibilidade de redução de custos está relacionada à contratação do serviço de *cloud computing* com o pagamento somente pelo serviço utilizado (*Pay-As You-Go*), de acordo com a conveniência da empresa contratante e não pela infraestrutura total que lhe é disponibilizada e que de fato não será totalmente utilizada. Neste caso, o contratante pode inclusive optar por realizar o pagamento do serviço por usuário que o utiliza. Todavia, algumas empresas contratantes preferem manter o contrato de infraestrutura disponibilizada, pois temem que podem aumentar significativamente os dados e/ou informações a serem

armazenados e a empresa provedora do serviço não terá capacidade de disponibilizar imediatamente o recurso necessário.

Sobre os custos envolvidos na computação em nuvens, MENKEN (2008) afirma que *cloud computing may be cheaper than in-house equipment, but giving away data to the cloud must be a calculated risk.*

É também importante abordar a vantagem na otimização da capacidade de processamento de dados. Na grande maioria dos casos as empresas deixam de utilizar parte dos seus recursos computacionais fora dos seus horários de pico. Entretanto, ao contratarem o serviço de *cloud computing* os fornecedores do serviço sempre lhes disponibilizam os recursos de processamento solicitados, sendo possível processar o que for necessário durante todo o expediente, e disponibilizam o recurso subutilizado à outra companhia que esteja demandando-o naquele momento, sem qualquer prejuízo àquela organização.

Além disso, utilizando este tipo de serviço o usuário não precisará estar sempre preocupado com a taxa de crescimento de suas informações e dados armazenados na nuvem, posto que esta atividade, na maioria dos casos, é deslocada para o provedor do serviço, o que consequentemente reduz o custo de pessoal e o investimento em capacidade de processamento por parte do contratante. Entretanto, é importante ressaltar que o contrato de fornecimento do serviço pode também estabelecer um limite de armazenamento, prevendo ou não a responsabilização do provedor por eventuais aumentos de volume, o que pode acarretar custos extras ao contratante. Mas, cada empresa e fornecedor de serviço apresenta características específicas, o que requer com que os contratos sejam customizados.

Outra grande vantagem da computação em nuvem é o fato das organizações globais possibilitarem que os seus empregados utilizem as informações em qualquer parte do mundo, à qualquer momento e de qualquer plataforma (móvel ou não). Anteriormente era comum ambientes corporativos com provedores próprios e que não permitiam o acesso fora de um determinado local.

Ademais, com o acesso pela nuvem o trabalho colaborativo é fortalecido, permitindo com que os colaboradores possam acessar e modificar documentos. Desta maneira, o trabalho poderá estar em andamento durante 24 (vinte e quatro) horas por dia, podendo ser realizado ao mesmo tempo por diversas pessoas de diversas áreas da organização, o que consequentemente aumenta a produtividade empresarial.

Outra vantagem que se verifica está relacionada à negócios sazonais ou cíclicos, que não precisam constantemente de grande capacidade de processamento de dados. Este tipo de organização pode contratar o serviço de computação em nuvem por um período específico e

de acordo com as suas necessidades, sem precisar realizar grandes investimentos em computação e pessoal, bem como contratar um serviço superestimado para os seus negócios.

Quanto ao risco da perda de dados com a adoção da computação em nuvem nota-se que ele é reduzido. Os processadores do prestador de serviço são muitos, sendo que existe estrutura de *hardware* específica para realização de *backups* periódicos, caso contratado. Além disso, fornecedor do serviço também pode ser responsabilizado pela perda de dado ou informação armazenado pelo seu cliente, caso isto tenha sido tratado contratualmente acordado. Acrescenta-se à isto o fato do tráfego de equipamentos periféricos com informações da empresa (exemplo: *pen drive*), algumas delas altamente confidenciais e que podem colocar em risco as estratégias empresariais, também é diminuído com a implantação do *cloud computing*, tendo em vista a grande disponibilidade de acesso destas informações pelos usuários da tecnologia.

As empresas que trabalham com computação em nuvem reduzem o espaço destinado à equipe de tecnologia e aos equipamentos. Na empresa que não adota a computação em nuvem, na grande maioria das vezes para atender demandas pontuais de grande processamento de dados é necessário realizar suntuosos investimentos, o que com a adoção da tecnologia em estudo não se faz necessário. Assim sendo, a contratante não precisa disponibilizar grande espaço físico à área de tecnologia da informação, podendo otimizá-lo de acordo com a sua necessidade.

Outra vantagem é a eficiência energia das empresas que utilizam a *cloud computing*. A energia dispendida com um grande centro de armazenamento e processamento de dados destinado à prestação de serviço de computação em nuvem é inferior à utilizada em vários centros de processamento de dados tradicionais, posto que aqueles dispõem de programas de eficiência energética e buscam consumir energia limpa ou estão instaladas em localidades onde a temperatura é baixa, visando reduzir a utilização dos resfriadores das máquinas. Neste sentido MENKEN (2008) diz que:

(...) cloud computing can also achieve energy efficiency for organizations. It is more efficient for power hungry servers to all be in one location so that data center managers can better optimize them using power saving procedures. This can be achieved through a variety of methods, which could include timed power saving modes on servers to reduce power usage, or even being located near a renewable energy source.

Assim sendo, nota-se que são muitas as vantagens para a empresa que decide utilizar o serviço de *cloud computing*, cabendo à ela avaliar os riscos existentes e decidir se deve ou não adotar esta nova ferramenta tecnológica.

2.2.2 Desvantagens e/ou riscos

Mesmo considerando todas as vantagens abordadas anteriormente, também existem desvantagens na utilização deste serviço, como, por exemplo, a possibilidade de vazamento de informações. Desta maneira, é essencial que a equipe responsável pela sua contratação realize uma análise detalhada de todas elas e elabore um contrato de serviço detalhado, buscando obter o máximo de garantias do provedor do serviço. Entretanto, estas desvantagens não podem ser utilizadas como desculpa para que a organização não adote esta inovadora tecnologia.

Ao decidir implantar o *cloud computing* a empresa deve ter em mente que não terá controle exclusivo sobre os seus dados e/ou informações processados e/ou armazenados na nuvem, não podendo assim adotar medidas técnicas e organizacionais no que tange, por exemplo, à disponibilidade, confiabilidade, integralidade e portabilidade do conteúdo, o que fica à cargo do prestador do serviço, de acordo com o previsto em contrato.

Outras desvantagem é o risco de perda de dados e/ou informações sensíveis pela empresa contratante, o que pode impactar diretamente nos seus resultados. Assim sendo, é importante conhecer o plano de *backup* do fornecedor do serviço, mas muitos fornecedores negam-se à fornecê-lo, alegando tratar-se de informação confidencial.

Além disso, a segurança da informação (incluída a privacidade) é um ponto crítico de qualquer serviço de computação em nuvem, principalmente nos dias atuais que tanto se aborda questões relacionadas ao vazamento e furto de dados e informações. Sobre a segurança da informação, MENKEN (2008) afirma: (...) *when in the cloud, an organization can lose their ability to keep track of resources: this includes who controls them and who is currently using the resources.*

Assim sendo, é importante que sejam firmados contratos bem elaborados e também SLA – *Service Level Agreement* (ou Acordo de Nível de Serviço). Neste documentos, segundo MONTERO (2013), os provedores do serviço *se comprometen a llevar un control de la seguridad de la aplicación y la infraestructura, así como la privacidad de la información almacenada en sus instalaciones.*

Outra preocupação de algumas empresas é a possibilidade do concorrente acessar as suas informações, principalmente as estratégicas. Neste ponto, destaca-se a importância da atuação da equipe de tecnologia da informação, que é responsável pela segmentação das informações em diferentes nuvens. Por exemplo, em uma nuvem podem constar dados relacionados à produção e em outra informações mais sensíveis, como estratégia comercial de médio e longo prazo ou até mesmo informações da área de recursos humanos, como números da previdência social, carteira de trabalho, CPF e carteira de identidade dos colaboradores.

Quanto à confiabilidade do conteúdo armazenado é importante ressaltar que mesmo que o contrato possua cláusula específica de confiabilidade, o provedor pode ser obrigado por ordem judicial à disponibilizá-las e/ou revelá-las. Desta maneira, é importante que o contratante tenha conhecimento da legislação de proteção de dados dos países onde terá seu conteúdo processados e/ou armazenado, o que será posteriormente detalhado.

A largura de banda do provedor do serviço de *cloud computing* também é um ponto crítico a ser analisado. As empresas fornecedoras devem planejar e ter certeza de que serão capazes de processar e armazenar as informações no cenário de maior demanda possível por parte de seus clientes, de tal maneira que alguns deles não fiquem impossibilitados de executar qualquer tarefa na nuvem. Além disto, eles devem fazer a previsão de crescimento da demanda de serviço dos seus clientes, para que não ocorra qualquer problema no fornecimento do serviço. Enfim, que o provedor deve trabalhar tanto com a antecipação da demanda quanto com a sua volatilidade, além de um plano de contingência caso haja algum equívoco no planejamento.

Também é importante tratar da importância da disponibilização efetiva da internet. Com o crescimento da utilização da internet e com a migração de muitos recursos de informática para a nuvem, podem ocorrer falhas que impossibilitem o acesso de parte ou de todo o conteúdo armazenado pelo contratante na nuvem. Infelizmente as interrupções têm sido maiores do que o desejado, o que pode acarretar prejuízo à organização que disponibiliza os seus dados no ambiente virtual e que com a dificuldade de acesso via internet pode ter prejudicada a realização de suas atividades, dentre elas, o atendimento aos clientes, o que impacta diretamente no faturamento da companhia.

2.3 Modelos de implantação

Existem alguns modelos de implantação de computação nas nuvens que podem ser escolhidos pela empresa contratante, conforme a sua necessidade. Eles são a nuvem privada, pública, híbrida e comunitária.

A nuvem privada (ou nuvem interna) é aquela implantada e gerenciada pela própria organização, o que acarreta custos de desenvolvimento, implantação, manutenção. A sua utilização é privada, ou seja, realizada somente pela empresa e pelos usuários autorizados. Todavia, ela pode ser hospedada pela própria empresa ou por um provedor de serviço. Apesar da dependência desta empresa ser mínima em relação à outras empresas e órgãos externos, ainda assim ela será parcialmente dependente da internet pública, posto que para acessá-la é necessária a sua utilização. A nuvem privada apresenta como vantagem o maior controle de segurança e capacidade de apoio em caso de recuperação de conteúdo. Sobre este modelo de implantação de computação em nuvem MONTERO (2013) afirma:

(...) los principales beneficios de la nube privada es que puede ajustarse a las necesidades específicas de una organización, que tiene mayores niveles de automatización, aprovisionamiento y orquestación los despliegues, si no se es capaz de escalar sus infraestructuras, en el modo que se garantisse el control sobre los datos al incrementar el personal técnico informático.

Las nubes privadas son muy adecuadas para flujos de trabajo de misión crítica con grandes tratamientos que requieren altos niveles de seguridad, y disponibilidad, así como para aplicaciones que por razón de cumplimiento normativo, exigen um mayor grado de control de la propiedad de los datos.

Já a nuvem pública é disponibilizada publicamente, pela qual o usuário paga pelo serviço utilizado. São oferecidas por grandes empresas multinacionais, sendo que geralmente possuem baixo custo, economia de escala e gerenciamento simplificado. Ao tratar desta nuvem, MONTERO (2013) nos ensina que:

Es recomendable comenzar el despliegue de servicios bajo los denominados “Cloud públicos” con proyectos sencillos que manejen información del negocio de baja sensibilidad para que, en un futuro, una vez evolucionados los servicios de carácter más complejo, puedan operar con información más crítica para el negocio.

A nuvem comunitária é compartilhada por diversas empresas com princípios e interesses comuns, como, por exemplo, requisitos de segurança, podendo ser administrada por algumas ou todas organizações que dela fazem parte ou por terceiro por elas designado.

Finalmente, a nuvem híbrida tem a sua estrutura é composta por mais de uma modalidade de nuvem, como a nuvem pública e a privada. MONTERO (2013) afirma que aquela nuvem:

*(...) presenta como característica fundamental el disminuir sensiblemente la complejidad, y el coste de la nube privada.
(...) esta opción, al menos inicialmente, estará probablemente reservada a aplicaciones simples, que no tengan condicionantes, que no requieran de ninguna sincronización o necesiten bases de datos complejas.*

Desta forma, cabe à cada empresa analisar e adotar o modelo de implantação adequado às suas necessidades e prioridades.

2.4 Modelos de serviços

Os três principais modelos de serviço de *cloud computing* são a infraestrutura como serviço, a plataforma como serviço e o software como serviço.

No primeiro caso, também conhecido como *Infrastructure as a Service* – IaaS, o provedor oferece o processamento e o armazenamento, sendo que o controle da infraestrutura física é de responsabilidade de uma outra empresa fornecedora do serviço, enquanto o usuário possui o controle sobre as máquinas virtuais (armazenamento, aplicativos etc). Entretanto, segundo MONTERO (2013), este modelo não é geralmente utilizado por empresas de grande porte: *esta categoría ha sido objeto de una mayor aceptación y adopción entre pequeños e medianos proveedores de software independientes, y de empresas que no poseen los recursos o economías de escala para construir grandes infraestructuras de tecnologías de la información.*

A plataforma como serviço (*Platform as a Service* – Paas) é o modelo de serviço em que o provedor oferece o desenvolvimento de aplicativos que serão disponibilizados na nuvem e poderão ser nela executados. Para MENKEN (2008), este tipo de plataforma *refers to renting server technology in order to use its development capabilities*”. Além disso, a referida autora afirma que *many small tech companies need a platform from which to process their customized code. Platform as servisse offers these organizations this hability while saving huge amounts of money that would otherwise be sent on hardware resources.*

O terceiro modelo de serviço a ser tratado é o software como serviço, ou *Software as a Service* – SaaS, no qual os aplicativos de interesse do usuário ficam armazenados na nuvem (ex. Office), sendo que todo o seu gerenciamento, manutenção e atualização fica sob a

responsabilidade do provedor de serviço. Exemplo deste modelo de serviço é o e-mail *online* que permite ao usuário guardar um grande volume de dados sem a necessidade de possuir muitos servidores com grande capacidade de processamento. Para MONTERO (2013) este modelo é atualmente o mais adotado em função da *velocidad y la facilidad con la que se pueden adquirir y consumir las aplicaciones*.

2.5 Segurança dos dados

O assunto de maior relevância no que se refere à computação em nuvem é a segurança, posto que é um terceiro que armazena os dados e informações de uma empresa, algumas vezes sem qualquer gerenciamento e controle efetivos por parte do contratante.

Essa preocupação se deve à importância das informações e dados armazenados, os quais muitas vezes são mais valorizados do que os bens físicos da empresa. Entretanto, é fato que com a disponibilização de informações somente nas nuvens e não em computadores há a redução significativa do risco de perda ou furto de informação estratégica, além de ser mais fácil o monitoramento do seu acesso.

Assim sendo, a responsabilidade pela segurança é do responsável por disponibilizar e gerenciar a nuvem, mas é essencial que o contratante e seus colaboradores estejam conscientes de que eles também são peça fundamental para a manutenção da segurança do conteúdo armazenado.

Quando se verifica qualquer tipo de incidente ou erro que viole a segurança de uma nuvem cabe ao contratado agir imediatamente. Nestes casos alguns fornecedores clonam a máquina virtual para análise *off-line*, permitindo assim que a nuvem fique o menor tempo possível indisponível ao contratante.

Não é apenas o fornecedor da nuvem e o contratante que podem ser culpados pelo vazamento de dados. Atualmente deve-se preocupar também com o *man-in-the-middle*, que segundo VELTE (2011) é “um ataque feito na comunicação entre o cliente e o provedor de serviços, onde o criminoso obtém acesso aos dados e se faz passar ora por usuário, ora por provedor.”

É importante que os controles do provedor de computação em nuvem devem ser realizados em toda a infraestrutura e no material armazenado. Isto é essencial tanto na nuvem particular quanto na pública.

Nos últimos anos, tem-se verificado a aplicação de técnicas como a criptografia, a autenticação e a autorização. Na criptografia, segundo VELTE (2011), “um algoritmo

complexo é usado para codificar a informação. Para decodificar os arquivos criptografados, o usuário precisa de uma chave de criptografia.” Já o processo de autenticação requer que o usuário possua um *login* e uma senha de acesso e a autorização refere-se à permissão que a companhia contratante libera para que determinadas pessoas, sejam elas empregados, fornecedores e até mesmo clientes tenham acesso à nuvem. Nota-se que a autorização pode ser dada em diversos níveis, permitindo assim acesso diferenciado de acordo com o tipo de usuário. O cliente, por exemplo, para poder acessar a extranet da empresa pode ter um acesso muito inferior àquele liberado para o empregado da área financeira ou de negócios. Já o empregado da área de manutenção geral poderá ter um acesso mais restrito do que o colaborador que assessora a diretoria da organização.

Finalmente, mas não menos importante, é interessante lembrar que todas empresas que possuem seus dados armazenados em nuvens devem possuir um planejamento de tecnologia da informação que trate das ações relevantes a serem imediatamente tomadas quando verificado vazamento de qualquer tipo de informação. Este plano pode até ser desenvolvido em conjunto com a empresa fornecedora da nuvem, mas deve ser constantemente revisado.

2.6 Dos serviços prestado pelas empresas fornecedoras do serviço de computação em nuvem

Os principais serviços ofertados pelas companhias de *cloud computing* são o armazenamento de arquivos, *backups* e *downloads/uploads*.

No que tange ao armazenamento os fornecedores do serviço asseguram que é possível guardar qualquer tipo de arquivo, seja documento, planilha, música, foto, apresentação etc, trazendo assim vantagem de armazenamento confiável, disponível e de custo inferior.

A disponibilização, gerenciamento e atualização de aplicativos também é oferecido por alguns fornecedores de *cloud computing*, permitindo que o empregado da companhia contratante trabalhe de qualquer lugar do mundo, de qualquer dispositivo com acesso à internet, de maneira segura e com acesso a todos os *softwares* e informações que necessita, reduzindo gastos, por exemplo, com a aquisição e atualização contínua de aplicativos nas máquinas utilizadas pelos empregados da empresa.

Outro serviço que é disponibilizado ao mercado é a confiabilidade dos dados e informações disponíveis na nuvem. Sem dúvida alguma nenhum fornecedor de *cloud computing* pode garantir 100% de confiabilidade, mas eles têm aumentado cada vez mais suas ações e investimentos relacionados à segurança, posto que este é um dos requisitos essenciais para as empresas contratantes.

Mais um importante serviço oferecido é a disponibilidade das informações 24 horas por dia, durante 7 dias na semana, com o menor índice de instabilidade possível. Este item, assim como os já citados anteriormente, devem ser tratados no contrato firmado entre o fornecedor e o contratante, sendo que devem ser estabelecidas metas de estabilidade do serviço e também sanções para o caso destes indicadores não serem atingidos, como será tratado oportunamente.

Além disto, outros serviços oferecidos pelos fornecedores de computação em nuvem é o suporte da sua equipe técnica. Com a adoção da computação em nuvem as equipes de tecnologia da informação da empresa contratante tendem a ser reduzidas, sendo importante que o fornecedor do serviço disponibilize suporte seja telefônico ou físico, visando sanar eventuais problemas ou dúvidas operacionais dos usuários, inclusive os que não podem ser solucionados pela equipe interna de tecnologia da informação do contratante.

Assim sendo, nota-se que existe uma infinidade de possibilidade de combinação de serviços a serem contratados pelas empresas, podendo inclusive serem desenvolvidos serviços personalizados. Isto posto, a configuração ideal varia de organização para organização e devem ser analisadas detalhadamente pela equipe responsável.

3 Contrato de computação em nuvem

O estudo jurídico da computação em nuvem ainda é muito pequeno, tanto no Brasil quanto na América e na Europa, havendo poucas publicações específicas sobre o tema, sendo que algumas destas apresentam abordagem superficial. Isto se deve principalmente à novidade do tema e provavelmente aos poucos problemas jurídicos envolvendo o assunto, o que gera uma pequena ou quase nula criação de jurisprudência sobre o tema.

A relação entre os provedores de *cloud computing* e seus clientes pode gerar conflitos, principalmente por envolver um serviço de tecnologia de ponta e segurança da informação. Por isto, para que as empresas utilizem o serviço de computação em nuvem é necessário que seja firmado um contrato com o prestador do serviço. Quando se trata de empresa de grande porte, a qual é o foco do presente estudo, é ainda mais importante um contrato claro e bem delineado, tendo em vista a grande quantidade dos dados e informações sensíveis que estarão em jogo, envolvendo desde desenvolvimento de produtos até informações pessoais de colaboradores e clientes.

Geralmente quando o contratante é uma grande empresa o contrato de serviço pode ser customizado, visando atendimento aos seus objetivos e metas específicos, o que não ocorre

quando o contratante é pessoa física ou empresa de pequeno porte, os quais estão sujeitos tão somente à um contrato de prestação de um serviço padrão, sem qualquer adaptação.

No contrato firmado por grandes empresas é necessária a presença de requisitos essenciais à todos os tipos contratos como as partes e o objeto do serviço. Entretanto, deve ser realizada uma análise detalhada dos requisitos importantes para ambos contratantes, os quais devem ser discutidos e após entendimentos devem constar no contrato de *cloud computing*. Por exemplo, alguns itens a serem tratados são a privacidade das informações, a interrupção no fornecimento do serviço e a segurança dos dados e/ou informações. À respeito deste assunto, MILLARD (2013) alega que:

Generally, bigger users, particularly from regulated industries, try to negotiate more. Some even require contracts to be on their standard IT services or outsourcing terms, on a 'take it or leave it' basis. Such users, mainly government bodies and financial institutions, may have more purchasing power. Also, their internal procedures may make it difficult and time-consuming to contract on terms other than their own (eg, bank may require director sign-off for changes to their standard terms). To secure such users' business quickly, some providers may accept the user's terms, even though some terms may not be cloud-appropriate.

3.1 Classificação do contrato de computação em nuvem

O contrato de *cloud computing* é bilateral (ou sinalagmático). Ele visa estabelecer obrigações e direitos tanto para o provedor do serviço quanto para o contratante.

Ele não está previsto na legislação brasileira, bem como na maioria das legislações dos outros países que o utilizam. Assim sendo, trata-se de um contrato atípico, sendo desenvolvido de acordo com o entendimento realizado entre as partes, considerando sempre a autonomia da vontade dos envolvidos.

Quando o contrato é firmado por consumidores finais e/ou pequenas empresas, geralmente não existe a autonomia do consumidor e a possibilidade de negociação de cláusulas entre as partes, sendo assim considerado um contrato de adesão. Entretanto, quando o contratante é uma companhia de grande porte existe maior abertura para que as cláusulas sejam discutidas entre as partes, podendo-se assim ser considerado como um contrato paritário.

Os contratos de *cloud computing* são solenes, pois para terem validade jurídica devem obedecer à forma prescrita em lei para todos os contratos. Desta forma, nota-se que a simples vontade das partes não basta para a formação do contrato, devendo serem seguidas as formas gerais previstas na legislação nacional.

Além disso, são contratos reais, nos quais é exigido além do consentimento, a entrega do serviço (objeto do contrato). Todavia, antes da disponibilização do serviço ele é considerado somente como uma promessa de contratar.

Tratam-se de contrato principal, posto que é um contrato autônomo cuja existência não depende de qualquer outro.

No mercado de computação em nuvem, nota-se que existem serviços que são oferecidos de forma gratuita, como o *Hotmail*, o *Facebook* e o *Google Docs*, mas como o foco do presente estudo são as grandes empresas, o contrato por elas firmado não é gratuito mas sim oneroso, com uma prestação patrimonial por parte do contratante frente à prestação de um serviço pelo contratado.

Ademais, cabe acrescentar que existem contratos que são firmados à título gratuito e que posteriormente passam a ser onerosos, como é o caso de nuvem que fornece o armazenamento de informações e a licença de uso de *software* por um período determinado. Durante este tempo o cliente poderá avaliar o programa oferecido e ao final poderá optar por se vincular à ele, o que transforma o contrato gratuito em oneroso.

Frente ao exposto, observa-se que existem três tipos de contratos: os gratuitos, os onerosos e os que nascem gratuitos e ao longo do seu curso tornam-se onerosos.

Além disso, o contrato em análise é de execução/trato sucessivo ou continuado, sendo o serviço prestado por atos reiterados e não em um só ato em momento futuro (contrato diferido) ou após a sua celebração (contrato instantâneo ou imediato). Ou, seja, os serviços de computação em nuvem não se executam em um só instante, mas possuem duração prolongada e diferida no tempo. Geralmente o contrato se realiza por um determinado período de tempo pactuado entre as partes, podendo ou não ser prolongado automaticamente, de acordo com a intenção das partes. Entretanto, existem juristas que acreditam que o contrato de computação em nuvem é um contrato de execução imediata, como VALENZUELA e MONTOYA (2012):

El hecho de que ele contrato sea de ejecución inmediata implica que en el momento en que se pacte el contrato y se entienda celebrado el negocio jurídico, deberá comenzar a prestarse el servicio de manera inmediata, a menos que por alguna falta de los requisitos previamente pactados se heciere de forma diferente.

3.2 Partes

Ao firmar um contrato de *cloud computing* as partes contratantes são a empresa fornecedora do serviço e o cliente que utilizará o armazenamento em nuvem.

O contratante é a parte interessada em adquirir o serviço ofertado pelo fornecedor e que está disposto à firmar o contrato de *cloud computing*, visando beneficiar-se dos serviços prestados pelo contratado, mediante pagamento.

Sobre o cliente no contrato de computação em nuvem, VALENZUELA e MONTOYA (2012) afirmam que “*estas características del tipo de cliente al que se dirige el servicio Cloud tienen directa relación con el modelo de negocio que se adopte (naturaleza del servicio), e inclusive también con la calidad de un contrato oneroso o gratuito*”.

O contratado é o provedor de serviço em nuvem. Na grande maioria das vezes ele é uma pessoa jurídica, mas nada impede que seja uma pessoa física, desde que possua toda a infraestrutura e demais recursos necessários para o fornecimento do objeto do contrato. Entretanto, na pesquisa realizada para a elaboração deste estudo não foi encontrado provedor pessoa física que ofereça este tipo de serviço à nível mundial.

3.3 Objeto do contrato

De acordo com o modelo de serviço de *cloud computing* a ser adotado é possível detalhar o melhor objeto do contrato. Por exemplo, o objeto do contrato de prestação de serviço de aplicativo (SaaS) é diferenciado daquele contrato que visa disponibilizar tão somente a infraestrutura (IaaS). Todavia, basicamente em todos os modelos de serviço o objeto básico é o armazenamento e processamento de dados e/ou informação, sendo que o objeto secundário varia de acordo com o modelo a ser escolhido.

Sobre o objeto do contrato de *cloud computing* VALENZUELA e MONTOYA (2012) fazem a seguinte consideração:

- *SaaS: Cuando se contrata en un modelo de negocio SaaS hay un interés en obtener por parte del proveedor del servicio una plataforma ya desarrollada con software que permita el almacenamiento de información y la transferencia de datos entre los integrantes de la empresa que contrata el servicio.*
- *PaaS: en este tipo de modelo de negocio, el objeto del contrato versa sobre el alquiler de la infraestructura y las herramientas necesarias para el desarrollo del software que necesite adaptar la empresa que contrata, para el almacenamiento, procesamiento y transferencia de información. En este modelo, el proveedor de servicio ofrece como materia prima la infraestructura y algunos atributos básicos del servidor para el desarrollo de los programas que requieren la empresa.*
- *IaaS: este modelo obliga al proveedor de servicio al alquiler de la infraestructura con capacidad de almacenamiento, procesamiento y funcionamiento en red, en donde se permite un espacio de acceso único al cliente para que desarrolle cualquier actividad lícita dirigida al desarrollo de su industria por ese medio.*

Para finalizar é importante destacar que a descrição e alcance do objeto do contrato é muito relevante, sendo determinante com relação ao alcance técnico do serviço a ser prestado e o conteúdo das obrigações das partes.

3.4 Cláusulas contratuais mais relevantes

Ao utilizar um programa de computador ou um serviço prestado através da internet, o usuário pessoa física ou pessoa jurídica deve aceitar o acordo ou contrato proposto pela empresa fornecedora. Isto também ocorre com a computação das nuvens, devendo o cliente estar de acordo com os termos do contrato de prestação de serviço apresentado pelo seu fornecedor.

Geralmente, quando os clientes do serviço de *cloud computing* são grandes empresas alguns termos são discutidos e negociados. Entretanto, para pequenas empresas e consumidores finais os provedores de serviço lhe oferecem pacotes padrões de serviço. Por exemplo, quando eles se cadastram em um serviço de armazenamento de informações em nuvem, como, por exemplo, o “Mega”, eles clicam em aceitar os termos do serviço, não podendo alterar qualquer cláusula, ou seja, trata-se de um contrato de adesão.

Mas, qualquer que seja o tipo de cliente a ser atendido por um contrato de computação em nuvem, ele deve sempre ser o mais claro possível e ser interpretado de acordo com a intenção das partes. Sobre o referido contrato, VALENZUELA e MONTOYA (2012) afirmam:

Como característica distintiva de esta contratación se percibe una variedad de contratos que se requieren para que un esquema de Computación en la Nube cumpla las funciones y requerimientos de las distintas partes, proveedores, clientes y usuarios. Esas relaciones jurídicas tienen en principio un interés común de colaboración con el fin de que la información sea protegida en su integridad y de que su custodia sea realizada de manera diligente.

Ademais, nota-se que são diversos os itens que podem ser abordados no contrato de prestação deste serviço. Ele deve ser adequado ao modelo de negócio e também ao tipo de cliente, conforme nos ensinam VALENZUELA e MONTOYA (2012):

(...) suele haber cierto prototipo de cláusulas comunes en estos contratos y que estas varían de forma específica según cada “modelo de negocio” y cada tipo de cliente. Así encontramos que hay contratos Cloud diferentes para la prestación de un servicio SaaS, PaaS e IaaS y para cada uno también si el objetivo de mercado (cliente final) es un individuo, un servicio de prestación media o un servicio

corporativo o público, de una pequeña comunidad de personas o de grandes corporaciones.

Assim sendo, neste tópico serão brevemente tratadas algumas questões que podem ser discutidas entre as partes e que deverão constar em cláusulas de contratos firmados por grandes companhias.

Para o desenvolvimento do contrato é interessante que o representante jurídico da empresa contratante tenha conhecimentos de tecnologia da informação, posto que este contrato é atípico e pode gerar muitas dúvidas e discussões quanto aos diversos aspectos de suas cláusulas, principalmente no ambiente corporativo. Ademais, é essencial a participação de representante da área de informática, o qual efetivamente conhece a realidade do negócio da empresa, a tecnologia disponibilizada pelo provedor e as necessidades corporativas.

VALENZUELA e MONTOYA (2012) citam as cláusulas de uso aceitável ou permitido, que são aquelas que disciplinam as regras de como o cliente deve utilizar o serviço ofertado pelo provedor, bem como o comportamento que o provedor deve ter durante a vigência contratual. Segundo tais autores, estas cláusulas buscam *encauzar el comportamiento de las partes dentro de una política ética y de buena fe en el uso de los servicios y de la información que se use dentro de los sistemas de información*. Assim sendo, eles acrescentam que estas cláusulas:

(...) están dirigidas a impedir el uso de los sistemas o servicios para el envío de publicidad; se prohíbe también el acceso a zonas en la que el proveedor no ha dado acceso al cliente (hacking), y algunos prohíben la propagación de información o imágenes de pornografía y de racismo, actividades abusivas, manejo de material con virus, y en general, cualquier tipo de abuso que constituya un abuso para el servicio.

Assim sendo, nota-se que as cláusulas de uso aceitável podem variar de acordo com os interesses e princípios tanto do provedor de serviço de *cloud computing* quanto do seu cliente. Geralmente a infração de tais cláusulas implica na resolução do contrato.

Cláusula relevante no contrato de fornecimento do serviço de computação em nuvem é a integridade do dado e/ou informação, a qual está atrelada à responsabilidade do contratado pelo seu armazenamento e conservação. Muitos provedores de serviço não admitem a inclusão desta cláusula contratual, principalmente aqueles que prestam serviços de forma não remunerada. Nestes casos, eles no máximo se comprometem a realizar o “melhor esforço” para manter a integridade das informações armazenadas em sua nuvem, o que faz com que caso ocorra qualquer perda de dado e/ou informação eles não sejam responsabilizados. Assim

sendo, alguns destes provedores oferecem o serviço de *back up* à custo adicional, visando recuperar dados eventualmente perdidos. Entretanto, quando se trata de grandes empresas, a integridade da informação é ainda mais importante, sendo que em grande parte dos contratos esta cláusula é admitida, o que se deve ao significativo valor do contrato e à relevância do cliente. Além disso, também pode ser estipulado que esta integralidade de dados seja auditada pelo cliente ou por um terceiro por ele indicado, o que será abordado em seguida.

Os requisitos de segurança dos contratos, como abordado anteriormente, podem constar no SLA – *Service Level Agreement* (ou Acordos de Nível de Serviço). Sobre tal disposição contratual MARCHINI (2010) nos ensina que:

The contract should set out an obligation upon the provider to comply with a particular security standard. It could be in general terms (such as, 'the provider will use reasonable efforts to keep data secure') but it would be better, as far as the customer is concerned, to set out some level of detail about what in fact will be provided.

A cláusula de disponibilidade do serviço assegura que o contratado disponibilizará o serviço de processamento, armazenamento e acesso dos dados e/ou informação, se possível, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, principalmente quando se trata de organizações globais. Entretanto, sabe-se que isto é praticamente impossível, sendo geralmente estabelecidos índices de performance de acordo com a eficiência do provedor, como, por exemplo, 97% ou 99%. Além disso, alguns fornecedores descrevem em contrato situações em que poderão não disponibilizar o serviço, os quais são excepcionais.

É importante abordar também as falhas nos servidores. Eventualmente este tipo de incidente ocorre, apesar dos provedores de *cloud computing* não confirmarem tal fato. Desta maneira, uma das maneiras de minimizar o possível impacto desta falha é prever contratualmente a manutenção do conteúdo armazenado em diferentes máquinas virtuais, reduzindo assim o risco de perda por parte do contratante.

Outro item importantíssimo que não pode deixar de ser abordado é a questão da proteção e privacidade das informações armazenadas na nuvem, posto que caso isto não seja previsto no documento de ajuste, teoricamente o fornecedor poderá utilizar tais informações e até mesmo repassá-las à terceiros. Sobre a proteção dos dados, MONTERO (2013) diz que *las cláusulas de protección de datos incorporados al contrato deben ser redactadas de forma que provean un completo soporte a las obligaciones del usuario en el marco legal de la protección de datos de carácter personal que le sea de aplicación.*

Para preservar a privacidade das informações e dados armazenados e processados na nuvem, o fornecedor de serviço deve assegurar contratualmente que realizará os registros de atividades em seu ambiente. Assim, ele guardará os *logs* efetuados com data e hora, visando possibilitar resposta rápida e precisa quando incidentes eventualmente ocorrerem. Estes *logs* podem ser disponibilizados ao cliente, mas não devem ser alterados em qualquer hipótese seja pelo cliente seja pelo provedor. Também deve haver previsão do prazo que o contratado estará obrigado a armazenar tais dados. Outra possibilidade é a inclusão da obrigação do provedor do serviço realizar testes aleatórios da disponibilidade de *logs* com o envio do resultado ao seu cliente para acompanhamento.

Atrelado à privacidade das informações armazenadas na nuvem está a sua divulgação. Quanto o cliente é uma organização empresarial a divulgação por parte do provedor é muito restrita ou até mesmo proibida contratualmente, tendo em vista muitas delas serem informações sensíveis que podem prejudicá-lo, por exemplo, frente à concorrência ou ao mercado. Segundo VALENZUELA e MONTOYA (2012):

Hay diferentes formas de divulgación de la información revelantes en estos contratos: en primer lugar, está la información que se maneja entre los usuarios del servicio Cloud, en donde se establecen reglas para su divulgación; en segundo lugar, está la información que se divulga por parte del proveedor de servicios hacia terceros; finalmente, se tiene la información que se utiliza por parte de los usuarios y cuya titularidad pertenece a los mismos proveedores.

Sobre a divulgação de informações também é interessante estudar a possibilidade de inclusão de cláusula contratual que preveja a possibilidade do cliente ser notificado à respeito de requerimentos legais para fornecimento de informações, com exceção dos casos em que a autoridade legal proíbe que tal comunicação seja realizada, como, por exemplo, quando é necessário preservar a confidencialidade de uma investigação criminal.

Também é importante a inclusão de cláusula de confidencialidade, posto que os empregados e subcontratados pelo provedor de serviço podem ter acesso à informações sensíveis do cliente, em função do desempenho de sua função. O provedor deve esclarecer aos seus empregados ou subcontratados a importância da cláusula de confidencialidade, sendo que algumas empresas pedem que eles firmem um termo de compromisso sobre isto.

No que tange aos subcontratados é relevante analisar a possibilidade dos provedores contratá-los ou não, o que deve estar previsto no contrato de *cloud computing*. Por exemplo, pode ser estipulado que a subcontratados somente serão admitidos à título eventual mediante aprovação expressa do cliente. Caso seja permitida a subcontratação também devem ser

acordadas condições de segurança aplicáveis aos subcontratados. Algumas empresas podem inclusive ter interesse em conhecer a identidade destes terceiros e tomar conhecimento quando o fornecedor efetuar troca de pessoal, o que deve constar no contrato de serviço. Sobre este assunto MONTERO (2013) lembra que: *los subprocesadores están sujetos a los mismos deberes contractuales que el proveedor en la nube.*

Ademais, as empresas contratantes devem estar atentas à lei aplicável ao contrato em questão, já que os dados e informações podem ser armazenados em diversos locais (países). Desta forma, o contratante terá conhecimento da lei que regerá diversas questões, dentre elas a guarda, a segurança, o sigilo dos dados e/ou informações e questões tributárias. Todavia, é difícil encontrar provedor que aceite esta cláusula, posto que muitos deles possuem infraestrutura em diversos países, de acordo com o baixo custo de manutenção, custo e disponibilidade de energia e os recursos tecnológicos disponibilizados. Sobre isto, VALENZUELA e MONTOYA (2012) afirmam que:

El lugar donde se almacena la información ofrece diferentes tipos de responsabilidad para la compañía de servicios Cloud, como para la persona contratante, sin dejar de lado, además, las facultades que la misma ley otorga a ciertos terceros frente a la información y al no respecto de la confidencialidad de la misma.

MONTERO (2013) acrescenta que:

(...) puede ser difícil abordar esta cuestión desde el punto de vista contractual. No obstante, se ha de destacar la extrema importancia que para el usuario del servicio tiene ser plenamente consciente de la ubicación de los datos, especialmente el caso de posibles transferencias de datos a países terceros que no garanticen un nivel adecuado de protección.

Este é o caso dos Estados Unidos da América, que possui legislação que autoriza que o país tenha acesso à qualquer tipo de informação armazenada e processada no país, desde que por razões ligadas à segurança nacional.

A questão da legislação contratualmente eleita pelas partes também pode envolver a jurisdição aplicável às partes em caso de conflitos, a regulamentação que deverá ser aplicada em caso de instauração de arbitragem e a legislação de propriedade intelectual e industrial aplicável.

Quanto à propriedade intelectual VIZCAYA (2012) nos ensina:

(...) las cláusulas de propiedad intelectual e industrial son fundamentales en este tipo de acuerdos pues, como resuelta evidente, los medios necesarios para prestar

los servicios objeto del contrato (programas informáticos, aplicaciones, sistemas de gestión, etcétera) se encuentran protegidos por derechos de este tipo.

Ademais, acrescentam VALENZUELA e MONTOYA (2012):

El tratamiento de la información en la Nube y los resultados de ese procesamiento pueden ser amparados por el secreto empresarial y eventualmente por la propiedad intelectual. Lo anterior en cuanto a que la protección tradicional de los programas de computación y las bases de datos, fundamento estructural de la Nube, se realiza por vía de los derechos de autor por asimilación a las obras literarias. El uso de los programas y las bases de datos produce unos resultados diferentes a los datos inicialmente introducidos. La principal cuestión radica en si la opción de proteger tales resultados está en cabeza del titular original de la información o si el proveedor de servicios Cloud que detenta derechos sobre el software y las bases de datos puede apropiarse de los resultados.

Algumas empresas somente autorizam acesso aos seus dados a partir de determinadas localizações. Neste caso é prudente especificar os locais no contrato, mas vale ressaltar que isto restringe muito a utilização do serviço em nuvem, pois um colaborador em viagem à trabalho à outra localidade, por exemplo, não terá acesso às informações e/ou dados armazenados na localidade delimitada pelo contratante.

Normalmente a empresa contratante divide o ambiente da nuvem com outros clientes da empresa contratada. Assim, é importante que as partes negociem e façam constar em contrato a adoção da criptografia dos dados armazenados e o programa de criptografia a ser utilizado. Além disto, nestes casos também é importante que seja tratada contratualmente a separação e segregação dos dados, posto que caso isto não seja realizado poderá impactar diretamente no acesso e recuperação dos dados criptografados.

Questão que também deve ser discutida e analisada pelos contratantes é a possibilidade de recuperação de conteúdo se eventualmente estes for apagado ou indevidamente alterado, bem como se a empresa contratada realizará *back up* das informações e/ou dados armazenados e com qual frequência.

Outro ponto importante que a discutido e incluído no contrato de *cloud computing* é a elaboração e disponibilização pelo contratado de um plano específico no caso de algum problema na prestação do serviço, como por exemplo, a sua não disponibilização ou utilização dos dados e/ou informações armazenados por terceiros não autorizados.

E a possibilidade de realização de auditorias, por exemplo, com relação à segurança e integridade dos dados e/ou informações armazenados? Estas auditorias não devem se restringir somente com relação ao prestador direto do serviço, mas também aos seus subcontratados. Entretanto, caso não haja previsão contratual neste sentido a empresa

contratada não estará obrigada às referidas auditorias, podendo negar-se à permitir que elas sejam realizadas dentro das suas dependências. As auditorias são significativamente difíceis de serem realizadas, posto o grande número de servidores, as diversas localidades onde se encontram, além do alto custo envolvido na atividade, mas são muito importantes.

De acordo com PINHEIRO (2012), alguns indicadores podem ser estabelecidos para que a auditoria verifique, tais como:

I - Confidencialidade: análise da robustez e suficiência dos mecanismos de criptografia e padrões de senha, entre outros fatores, aplicados em todo o ciclo de vida da informação, bem ainda, análise das políticas e procedimentos que garantam o sigilo dos dados perante terceiros, incluindo clientes e fornecedores da CONTRATADA;

II - Integridade: análise da implementação de ferramentas de prevenção à perda e corrupção de dados e testes de recuperação de Backups.

III - Disponibilidade: análise das medidas de contingência e recuperação de desastres, cumprimento dos níveis de serviço contratados e qualidade dos serviços.

Caso alguns destes indicadores não sejam atingidos, pode-se prever a rescisão contratual, desde que a vulnerabilidade ou falha encontrada não seja devidamente corrigida em tempo hábil pelo prestador de serviço.

Também no que tange à auditoria, MILLARD (2013) faz o seguinte comentário:

Many financial services users felt they needed right to require post-contract audits, at least when the user's regulator (or end user's regulator) required it. However, most providers refused, for security and cost reasons; providers were more willing to allow audits if users met all costs. Even enterprise-oriented SaaS providers that allowed audits would not offer the unfettered rights financial institutions required, but generally restricted audits narrowly, for instance, once annually per user, only if required by the user's regulator, or only with the provider's consent. Or, they agreed only to 'commercially reasonable' cooperation rather than full audit rights.

E quanto à eventualidade do fornecedor deixar de existir ou for adquirido por uma outra companhia? Muitas vezes a nova empresa não quer manter alguns clientes ou as estratégias anteriores, o que pode acarretar descarte indevido de informações e dados dos clientes. Assim, deve-se estipular contratualmente que a empresa contratante não pode ficar sem acesso à tais dados e informações, devendo o contratado possuir um plano de recuperação de dados no caso de ocasional perda de todo ou parte do conteúdo armazenado. Sobre isto MARCHINI (2010) afirma que *the risks of a provider insolvency or breach as it relates to the customer having reliable access to its own data is compounded when the data is not actually in the hands of the provider but instead in the hands of one of its subcontractors.*

Outro assunto que deve fazer parte do contrato de prestação de serviço é quanto à preservação da informação quando o provedor tiver terminado a sua prestação de serviço, ou seja, quando o contrato for extinto. Neste caso, teria o provedor direito à informação ou ela deve ser devolvida ao cliente? Quem sabe é melhor que ela seja enviado à outro provedor de serviço indicado pelo contratante? Ou ele somente deve ser responsável por eliminar estas informações? Elas serão destruídas de forma segura tanto de suas localizações principais quanto dos arquivos de *back up*? Segundo VALENZUELA e MONTOYA (2012):

Algunas compañías establecen en los modelos contractuales que la información se quedará en sus servidores durante un tiempo prudencial, en caso de que el cliente quiera volver a acceder al servicio o en algún momento sea relevante para el cliente solicitarla de nuevo al proveedor de servicio. Así mismo, algunas compañías plantean que la información debe ser devuelta al cliente y por lo mismo se deja en los servicios por un término de gracia para que puedan estos regresar por ella. Todo depende de la forma que termine el contrato. Amazon retira este beneficio en caso de una terminación del contrato por incumplimiento contractual.

Isto posto, nota-se que esta cláusula é importantíssima para a empresa contratante, posto que a manutenção dos seus dados e/ou informações são essenciais para a continuidade das atividades de qualquer organização. Assim, é essencial prever o destino das informações caso haja a extinção do contrato.

E no caso de ocorrer uma invasão ou tentativa de invasão? É interessante discutir a possibilidade de adoção de cláusula que assegure que o fornecedor do serviço comunique à empresa contratante este tipo de acidente, as medidas que tenham sido tomadas, bem como qual conteúdo foi acessado, se for o caso. Esta também é a opinião de MONTERO (2013): “*debe haber un compromiso de notificación inmediata al usuario de cualquier quebra de la seguridad que afecte a datos (...), incluyendo aquellas relativas a los procedimientos utilizados para corregir y mitigar los efectos de la quebra*”.

Os contratos de prestação de serviço de computação nas nuvens nada mais são do que contratos de terceirização do serviço. Desta feita, sugere-se que seja exigido da empresa contratada que cumpra as obrigações tributárias, trabalhistas e previdenciárias previstas na legislação, bem como comprovem que tais obrigações foram cumpridas. Isto assegura que o inadimplemento de tais obrigações não recaiam sobre a empresa contratante, como, por exemplo, prevê a Súmula 331, inciso IV do TST, no que tange às obrigações trabalhistas: “o inadimplemento das obrigações trabalhistas, por parte do empregador, implica a responsabilidade subsidiária do tomador dos serviços quanto àquelas obrigações (...)”.

É importante prever em contrato as penalidades por quebra de contrato, como por exemplo, em caso de vazamento de informações à terceiros não autorizados, o não fornecimento da capacidade de serviço conforme o contratado, bem como eventuais planos de contingência a serem adotados pela empresa contratada. Devem ser previstas as punições e responsabilizações à serem impostas ao provedor do serviço, como compensação financeira pelos danos causados, o que em determinadas situações torna-se de difícil mensuração e/ou o valor pode tornar-se extremamente elevado, como é o caso do prejuízo causado por acesso de terceiros não autorizado à especificações de desenvolvimento de produto de alta tecnologia.

Enfim, conforme se pode observar são muitas as questões a serem discutidas entre os contratantes, o que inclusive pode variar de acordo com o negócio do cliente, o modelo de serviço e de implantação de computação em nuvem escolhido, além das necessidades do contratante, características e princípios de ambas partes. De qualquer maneira, a interpretação contratual deve se dar sempre de acordo com a boa fé a intenção dos envolvidos.

4 Conclusão

O “mundo digital” é uma realidade que atinge toda a sociedade, sejam as pessoas físicas ou jurídicas. Inicialmente a computação em nuvem pode ter sido mais difundida entre pessoas físicas, entretanto atualmente o seu avanço nas empresas é uma realidade.

Assim sendo, é essencial os profissionais de tecnologia da informação e do departamento jurídico das grandes companhias estarem tecnicamente preparados para negociarem e firmarem contratos de fornecimento de *cloud computing*.

Neste contexto deve-se conhecer os modelos de serviço e de implantação disponíveis no mercado, bem como as diversas soluções oferecidas pelas empresas prestadoras de tal serviço, as quais geralmente possuem abrangência mundial.

Desta maneira, os contratos de fornecimento do serviço, devem estipular cláusulas que venham de encontro com os interesses de ambas partes, como, por exemplo, segurança, integridade e confiabilidade das informações armazenadas e processadas na nuvem, questões relacionadas à propriedade industrial e intelectual e criptografia de dados.

Enfim, a computação em nuvens é uma realidade organizacional e cabe às grandes corporações se prepararem e adaptarem à esta inovação tecnológica, que lhes fornece muitas vantagens, dentre elas, foco no *core business*, redução de custos, grande disponibilidade de armazenamento e aumento da produtividade e rentabilidade da organização. Mas, para isto é essencial que sejam analisados os impactos jurídicos possíveis da adoção da computação em

nuvem e estabelecidos contratos de prestação de serviço onde estejam bem delimitados as responsabilidades e obrigações de cada uma das partes, evitando assim inconvenientes posteriores, tais como perda de informações estratégicas e sensíveis para a concorrência.

Referência

AGUILAR, Luis Joyanes. *Computación en la nube: estratégias de cloud computing en las empresas*. 1. ed. Barcelona: Alfaomega, 2012.

ATHENIENSE, Alexandre. *Você sabe o que é Cloud Computing?* Entenda como funciona e saiba dar os primeiros passos. Disponível em: < <http://www.dnt.adv.br/noticias/informatica-juridica/cloud-computing-tendenciaatheniense/>>. Acesso em 03 junho de 2012.

BERBERT, Lúcia. *Brasil precisa de lei e insumos para ter espaço no mercado de computação em nuvem*. Disponível em: <<http://telesintese.com.br/index.php/plantao/19142-brasi-precisa-de-lei-e-insumos-para-ter-espaco-no-mercado-de-computacao-em-nuvem>>. Acesso em 24 abril de 2012.

BRASIL. Constituição (1988). *Constituição da República Federativa do Brasil*. Brasília, 05/10/1988. Brasília: Senado Federal, Centro Gráfico, 1988. 292 p.

BRASIL. *Decreto-Lei n. 2.848*, de 7 de dezembro de 1940. Diário Oficial. Brasília, 07/12/1940. Código Penal.

BRASIL. *Lei n. 10.406*, de 10 de janeiro de 2002. Diário Oficial. Brasília, 11/01/2002. Institui o Código Civil.

FRANÇA, Júnia Lessa *et al.* *Manual para normatização de publicações técnico-científicas*. 8 ed. rev. e ampl. Belo Horizonte: UFMG, 2007.

GUSTIN, Miracy Barbosa de Sousa *et al.* *(Re)pensando a pesquisa jurídica: teoria e prática*. 2. ed. rev. e ampl. atual. Belo Horizonte: Del Rey, 2006.

MARCHINI, Renzo. *Cloud Computing: A Practical Introduction to the Legal Issues*. Londres: British Standards Institution, 2010.

MARTÍNEZ, Ricardo MARTÍNEZ *et al.* *Derecho y Cloud Computing*. Pamplona: Thomson Reuters, 2012.

MILAGRE, José Antônio. *Agressão à privacidade em tempos de cloud computing*. Disponível em: < <http://www.tjdft.myclipp.inf.br/default.asp?smenu=revistas&dtlh=13714&iABA=Not%EDcias&exp=>>>. Acesso em 20 de maio de 2012.

MILLARD, Christopher. *Cloud Computing Law*. Oxford: Oxford University Press, 2013.

MENKEN, Ivanka. *The Complete Cornerstone Guide to Cloud Computing: Best Practices*. Australia: Emereo, 2008.

MONTERO, Janvier Puyol. *Algunas Consideraciones sobre Cloud Computing*. Espanha: Agência Española de Protección de datos e Agência Estatal Boletín del Estado, 2013.

PINHEIRO, Mário. *Cloud Computing: 5 riscos legais antes de contratar o serviço*. Disponível em: <<http://utiletec.com/2011/05/20/cloud-computing-5-riscos-legais-antes-de-contratar-o-servio/>>. Acesso em 20 junho de 2012.

PINHEIRO, Patrícia Peck. *Aspectos Técnicos e Legais do Cloud Computing*. Disponível em: <<http://www.prodeb.ba.gov.br/modules/wfdownloads/visit.php?cid=7&lid=122>>. Acesso em 18 de fevereiro de 2014.

PINHEIRO, Patrícia Peck. *Cloud desafia o modelo jurídico atual, baseado em fronteiras físicas*. Disponível em: <<http://cio.uol.com.br/opiniao/2011/11/07/cloud-desafia-o-modelo-juridico-atual-baseado-em-fronteiras-fisicas/>>. Acesso em 06 junho de 2012.

PINHO, Débora e MELO, João Ozorio de. *Computação em nuvem é a bola da vez na era digital*. Disponível em: <<http://www.conjur.com.br/2012-mai-09/computacao-nuvem-bola-vez-mercado-advocacia>>. Acesso em 11 maio de 2012.

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS. Pró-Reitoria de Graduação. Sistema de Bibliotecas. *Padrão PUC Minas de normalização: normas da ABNT para apresentação de teses, dissertações, monografias e trabalhos acadêmicos*. 9. ed. rev. amp. atual. Belo Horizonte: PUC Minas, 2011. Disponível em: <<http://www.pucminas.br/biblioteca>>. Acesso em 10 outubro de 2012.

Projeto de Lei 2.126/2011 – Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Marco Civil). Disponível em: <<http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=517255>>. Acesso em 1º junho de 2012.

ROHRMANN, Carlos Alberto. *Curso de Direito Virtual*. Belo Horizonte: Del Rey, 2005.

SANTOS, Ana P. V. e MACHADO, Marcos. *Cloud computing: impasses legais e normativos*. Disponível em: <http://www.uniesp.edu.br/guaruja/site/revista/revista20102/PDFs/cloud%20computing_2.pdf>. Acesso em 20 junho de 2012.

SOARES, Edileusa. *Conheça os riscos legais de cloud computing: deixar claras as obrigações dos prestadores de serviços e direitos do contratante pode gerar mais segurança*. Disponível em: <<http://computerworld.uol.com.br/negocios/2011/11/17/conheca-os-riscos-legais-de-cloud-computing/>>. Acesso em 15 junho de 2012.

VALENZUELA, Daniel Peña; MONTOYA, Juan David Bazzani. *Aspectos legales de la computación en la nube*. Bogotá: Universidade Externado de Colombia, 2012.

VELTE, Anthony T; VELTE, Toby J.; ELSERPETER, Robert. *Computação em Nuvem: uma abordagem prática*. Rio de Janeiro: Alta Books, 2012.

VERAS, Manoel. *Cloud Computing: Nova Arquitetura da TI*. Rio de Janeiro: Brasport, 2013.