



Você está aqui: [Página Inicial](#) [Revista](#) [Revista Âmbito Jurídico](#) [Internet e Informática](#)

Internet e Informática

A necessidade de regulação legislativa para utilização do serviço de computação em nuvem

Luciana Vasco da Silva

Resumo: A utilização da nuvem não é uma modalidade nova, porém ganhou grande destaque na mídia em vista da manutenção do sigilo das informações. Os resultados demonstram que o modelo *Computação em nuvem* constitui uma solução economicamente viável, muito utilizada no meio empresarial, porém, desprotegida pela legislação, gerando assim, insegurança e entrave na utilização desse serviço. A possível e futura legislação deverá regular a guarda e manutenção das informações. Na atual situação, desprovido de regulamentação, permanece a cargo do contrato, firmado entre as partes, a responsabilidade pela resolução de conflitos típicos deste tipo de contratação.

Palavras chaves: Computação na Nuvem; sigilo, legislação; Internet.

Abstract: The use of the cloud is not new, but it has gained great prominence in the media concerning the confidentiality of information. The results show that the cloud computing model is an economically viable solution, widely used in business, but unprotected by law, which generates uncertainty and makes its use more difficult. Possible future legislation should regulate the safekeeping of information. As it is now, unregulated, the responsibility for solving the typical cloud computing issues is left exclusively to the contract signed between both parties.

Key words: cloud computing, confidentiality, law, internet

Sumário: *Introdução; 2 Origem de Computação em Nuvem; 3 A Necessidade de Regulamentação; 3.1 Segurança da informação em nuvem; 3.2 Localização Geográfica da nuvem; 4 Legislação em Vigor e Projetos de lei; 4.1 União Européia; 4.2 Estados Unidos da América; 4.3 Argentina, Uruguai e Chile; 4.4 Brasil; 5 Marco Civil da Internet; 6 Considerações Finais; Referências.*

INTRODUÇÃO

O Direito Digital vem se desenvolvendo graças a ampliação e constante avanço da tecnologia. Cada dia mais as transações virtuais tornam-se importantes e essenciais para a vida do cidadão e de empresas.

No diapasão do conhecimento tecnológico, a Ciência do Direito também tem o dever de tentar resguardar o direito dos usuários e cidadãos que utilizam diversos serviços. Diversas atividades tecnológicas ainda encontram-se sem proteção legislativas, sendo amplamente utilizada pelo empresário e pouco regulada pelo Direito, resultando em instabilidade e insegurança jurídica.

Dentre uma das tecnologias mais utilizadas e muitas vezes não percebidas pelo cidadão ou contratada especialmente pela pessoa jurídica a fim de diminuir gastos, fala-se em computação em nuvens. Mesmo sendo uma alternativa mais barata ao empresário, que acaba não realizando altos investimentos em infraestrutura de datacenter, o serviço requerer cuidados especiais, tendo em vista a necessidade de guarda das informações.

A problemática neste tipo de contratação é a questão de segurança da informação e local de guarda, assuntos estes, não regulamentados na lei brasileira e muitas vezes contraditória com legislações de outros lugares.

Tendo em vista que as informações são armazenadas em local, muitas vezes, não conhecido pelo contratante, não se sabe a legislação aplicável à manutenção do sigilo.

O Brasil tem diversos Projetos de Lei versando sobre o assunto, porém, nenhum deles disciplina com rigor. O Marco Civil da Internet, por exemplo, era visto como o principal texto regulatório do assunto, porém foi aprovado sem as medidas necessárias sobre computação em nuvem.

2. ORIGEM DE COMPUTAÇÃO EM NUVEM

O termo computação nas nuvens é relativamente recente, porém sua ideia de utilização não é necessariamente nova. Serviços de e-mail do gmail e Yahoo são utilizados há muito tempo. Atualmente o maior exemplo de computação em nuvem é o Dropbox, site de armazenamento e compartilhamento de fotos; Google Apps; Amazon; icloud; dentre outros.

Segundo Taurion (2009), o termo Computação em nuvem surgiu em 2006 em uma palestra de Eric Schmidt, da Google, empresa que gerenciava datacenters. O autor define computação em nuvem como "um conjunto de recursos como capacidade de processamento, armazenamento, conectividade, plataforma, aplicações e serviços disponibilizados na Internet".

A Computação em Nuvem é definida por Gartner[1] como a utilização da memória e da capacidade de armazenamento de computadores compartilhados e interligados pela internet.

Vaquero (2010) faz uma análise das definições utilizadas na literatura atual e adota a seguinte opção:

"Computação em nuvem é um conjunto de recursos virtuais facilmente usáveis e acessíveis tais como hardware, plataformas de desenvolvimento e serviços. Estes recursos podem ser dinamicamente re-configurados para se ajustarem a uma carga variável, permitindo a otimização do uso dos recursos. Este conjunto de recursos é tipicamente explorado através de um modelo pay-per-use com garantias oferecidas pelo provedor através de acordos de nível de serviço (Service Level Agreements-SLAs)."

De forma geral, Computação em nuvem é caracterizada pelo acesso e execução de programas, serviços e arquivos por meio da internet, sem a necessidade de instalação de programas ou armazenamento de arquivos no computador e em qualquer lugar, visto que as informações encontram-se disponíveis na rede.

Atualmente, há "nuvens" por toda a web e a maioria das pessoas não tem conhecimento sobre sua utilização. Conforme pesquisa divulgada em 2012 pelo NPD Group, 22% dos norte-americanos não sabiam o que o termo "computação em nuvem" significava, mas 76% dos entrevistados já tinham usado a tecnologia, isto porque é um serviço barato e que evita grandes gastos com a montagem de um datacenter.[2]

De acordo com o Jornal DCI[3], a adoção do serviço de computação em nuvem no Brasil subiu de 27% em 2010 para 37% em 2011. No mesmo ano, 28% das empresas já adotaram o uso de nuvens privadas; as nuvens públicas são utilizadas por 6%, e o uso de ambas foi assumido por 3% das companhias.

Frost & Sullivan (2014)[4] diz que o mercado brasileiro de computação em nuvem está se tornando cada vez mais maduro, com as empresas começando a perceber os benefícios em relação a custo e flexibilidade na adoção de soluções, resultando em movimentação de US\$ 328,8 milhões em solo nacional em 2013.

De acordo com a pesquisa realizada pela IBM[5], enquanto 16% dos executivos entrevistados afirmam já utilizarem funcionalidades em nuvem para promover inovações, como ingressar em novos nichos de negócio ou remodelar um segmento de mercado existente, 35% deles pretendem utilizar a nuvem, até 2015, como ferramenta de transformação de seus atuais modelos de negócios. Conforme o mesmo estudo, o número de empresas que migrarão suas infraestruturas de TI para Computação em nuvem dobrará nos próximos três anos.

No primeiro semestre de 2014, o Brasil subiu da última para 22ª posição no ranking anual sobre o mercado de computação em nuvem, elaborado pela Aliança de Negócios de Software (BSA)[6]. A entidade analisou 24 países que representam 80% da indústria de tecnologia e informação no mundo, considerando sete fatores: privacidade de dados, segurança, liberdade de comércio, proteção à propriedade intelectual, infraestrutura e suporte aos padrões da indústria.

Na Europa[7], 48% dos gestores, tanto do setor público como o privado têm consciência que a implementação da computação em nuvem pode acelerar e facilitar o trabalho. Ocorre que, mais da metade deles não aderiram ao serviço a fim de minimizar os riscos do negócio.

Computação em nuvem é um serviço fácil e econômico, que pode ser utilizado, tanto por pessoa física como pessoa jurídica, trazendo ganhos econômicos. A utilização em grande escala, depende, no momento, que o serviço apresente regulamentação e garantias a fim de conceder segurança aos usuários.

3. A NECESSIDADE DE REGULAMENTAÇÃO

A cada ano aumenta-se a complexidade de infraestrutura de TI, ocasionado pelo crescente aumento de ambientes e tecnologia ou exigência de adequação das empresas as normas e necessidades do mercado.

Neste contexto de crescimento, reduzir custos tornou-se necessidade primordial das empresas e a área de TI passa a buscar alternativas para tal objetivo. Uma das formas de economia vista pelas empresas é a adoção do modelo de computação em nuvem.

ALBERTIN e SANCHES (2008) descreve a necessidade de redução de custos, através de meios tecnológicos, como:

"Ao contratarem serviços terceirizados especializados em TI, as organizações querem agilidade, flexibilidade, qualidade e inovação na implementação de novos requisitos de negócios, buscando permanentemente uma melhor relação custo-benefício em função da produtividade e dos ganhos em escala, além de maior controle e impacto nas operações."

Muitas organizações colocam parte de sua infraestrutura na *nuvem* como forma de aumentar os recursos destinados à pesquisa e desenvolvimento. Mas, a maioria opta pelo modelo de *computação em nuvem* como forma de eliminar custos relacionados aos ativos de TI, principalmente, no que tange, ao *Data Center*, dentre outros motivos abaixo indicados:

a. Não há necessidade de sistema operacional ou hardware específico;

b. Cabe ao prestador de serviço de computação nas nuvens a realização de procedimentos de backup, controle de segurança e manutenção, ou seja, os usuários se desobrigam do ônus da manutenção de forma geral;

c. Compartilhamento de informação de forma fácil;

- d. Melhor controle de gastos, visto que muitas aplicações de computação nas nuvens são gratuito e quando oneroso, o usuário paga pelo tanto e pelo tempo que utilizar.
- e. O usuário não precisa ter conhecimento de toda a infraestrutura necessária.
- f. Redução de custos gerais com tecnologia;
- g. Liberdade de espaço físico, já que não é necessário a construção de grande datacenter.
- h. Diminuição de gasto com mão de obra em tecnologia;

TAURION (2009) cita o seguinte exemplo, a fim de justificar as vantagens de utilização do serviço de computação em nuvem:

“Imaginem uma empresa de comércio eletrônico, que vende seus produtos via internet. Ela precisa dispor de um parque computacional configurado para atender a seus picos de venda, como Natal e Dia das Mães. No restante do ano, grande parte desta capacidade computacional fica subutilizada. Com a computação em nuvem esta empresa não precisa ter esse parque de computadores instalados em seus escritórios. Ela adquire a quantidade de capacidade necessária e apenas paga por este uso.”

Frente a tantos aspectos positivos, torna-se evidente o porquê da adoção deste modelo. Ocorre que a maior preocupação dos executivos atualmente, refere-se à transferência do gerenciamento de atividades críticas a terceiros. Sem confiança no modelo adotado, sem uma legislação que guarde os direitos e deveres das partes envolvidas e mesmo o serviço sendo mais barato, a adoção do modelo é renegado pelos possíveis riscos resultantes.

Assim sendo, ao contratar este modelo de serviço, o empresário deve considerar os seguintes pontos negativos:

- a. Menos proteção à privacidade sob os aspectos legais.
- b. Frágeis sistemas de segurança são fáceis de invadir;
- c. Fácil meio de obter acesso as informações, por uma simples pesquisa por termo;
- d. Travamento de dados e controle por terceiro;
- e. Indisponibilidade do servidor
- f. Para muitos estudiosos, a computação na nuvem pode limitar a liberdade e criatividade do usuário, pelo fato de não possuir fisicamente as ferramentas, sendo permitido apenas que se faça backup dos dados.

A maior parte de empresas que não adotam o modelo de computação na nuvem argumentam que os pontos negativos são maiores do que os benefícios alcançados através da adoção, tendo em vista que a principal preocupação das empresas é a questão da *Segurança da Informação*. Segundo esses empresários, a informação na nuvem não se encontra em segurança, podendo ser acessada por pessoas desabilitadas.

Segundo relatório sobre o assunto, na União Européia[8]:

“Sublinha que, devido à incerteza existente em torno do direito aplicável e da jurisdição competente, são os contratos os principais instrumentos que definem as relações entre os operadores de serviços de computação em nuvem e seus clientes, sendo portanto claramente necessário diretrizes.”

Assim, percebemos que os aspectos *jurídicos* caminham a passos lentos e a *ausência de uma legislação específica* dificulta a disseminação do serviço e torna “inseguro” a utilização da nuvem.

3.1. Segurança da Informação na Nuvem

Os termos de privacidade dos serviços da nuvem não dão quaisquer garantias com relação à segurança das informações entregues aos prestadores do serviço. Os contratantes do serviço, principalmente, pessoas físicas, não se preocupam em disponibilizar suas informações pessoais de forma aberta na Internet e sequer procuram saber como aquele serviço que está sendo desfrutado.

Conforme explica Ulrich Beck[9], a falta de uma exata compreensão acerca de como funcionam as novas tecnologias, a rede mundial de computadores, a computação em nuvem e outros, remete à ideia de sociedade de risco.

Pelo mau uso das informações postas na Internet é correto verificar-se hoje em dia a ocorrência cada vez mais frequente de fraudes eletrônicas, estelionatos, perda de materiais, divulgação sem controle de documentos sigilosos.

A tendência é que os problemas relacionados à segurança da informação ocorram cada vez mais frequentemente nos produtos e serviços oferecidos pela nuvem.

Por não termos uma regulamentação ou padronização para Computação em nuvens, a fim de solucionar qualquer questionamento, na maior parte dos casos de fraude, faz-se necessário a realização de perícia ou até mesmo a prevenção de atos que possam causar danos.

No caso a perícia em meios digitais torna-se complicado devido à necessidade de conhecimentos técnicos para narrar os fatos e a volatilidade das informações, principalmente na computação em nuvens.

Segundo Heiser:

“Serviços de *Cloud* são especialmente difíceis de investigar, porque os *logs* e dados de vários clientes podem estar localizados conjuntamente e também estar distribuídos com uma constante mudança no conjunto de máquinas e *data centers*.”

Por sua vez, para que a auditoria seja realizada, é necessário que tenhamos o log, contendo a identificação completa do usuário: endereço de IP, login, data e horário de acesso.

Ao contrário do recomendado, segundo SANTOS e MACHADO (2010)[10]:

“Alguns prestadores de *Computação em nuvem* não vêem razões para armazenar seus *logs* fora da nuvem, mas os *riscos* deste ato devem ser levados em consideração. Suponha uma paralisação no serviço, com os *logs* armazenados em nuvem, nem mesmo a eles a empresa terá acesso. Numa invasão, dependendo do nível e controle que o invasor tiver sobre os dados, o invasor pode facilmente apagar os *logs*, eliminar possíveis provas e encobrir seus rastros; e a chance de descobrir qual foi a vulnerabilidade que possibilitou a invasão ou ataque passa a ser mínima.

A obrigatoriedade e o armazenamento dos *logs* de dados é um dos principais fatores a serem considerados na hora de regulamentar o modelo de *Computação em nuvem*.”

Um dos conselhos dos autores (2010) é que as empresas que desejam aderir a *Computação em nuvem* devem exigir de seus prestadores a garantia do armazenamento desses *logs* por alguns anos, para que crimes futuros possam ser investigados através de perícia.

Segundo Patrícia Peck (2010):

“Como toda tecnologia digital, a nuvem exige, por parte do usuário, um grau elevado de maturidade e preparo no que tange ao correto e consciente uso da mencionada tecnologia. Primeiro, porque o contrato clássico, como instrumento de papel formalizador de uma relação jurídica, servindo de garantia e segurança para as partes contraentes deixou de existir.”

Portanto, pelo que se denota facilmente, o negócio jurídico baseado na nuvem carece dos elementos tradicionais dos contratos. E aí começa a residir uma dos maiores problemas atrelados ao uso da citada tecnologia: a falta de confiança. Como qualquer negócio jurídico, o contrato a ser firmado, versando sobre computação em nuvem deve sempre se permeiar de lealdade, boa-fé, segurança, bem como abster-se de usar cláusulas abusivas e outras situações perniciosas.

Há que se analisar se a tecnologia da computação em nuvem é capaz de tutelar as legítimas expectativas do consumidor a ponto deste correr o risco de entregar seus dados confidenciais e importantes à este novo modelo tecnológico

3.2 LOCALIZAÇÃO GEOGRÁFICA DA NUVEM

Outro ponto controverso na contratação de serviços em nuvem é a localização geográfica do servidor onde as informações serão armazenadas.

O serviço pode ter sido contratado no Brasil e o servidor estar localizado do outro lado do planeta. O problema é que cada país possui sua legislação específica. Alguns com leis e normas para proteção de dados; outros com normas para serviços internacionais.

Em vistas dos riscos ocasionados por esse tipo de serviço, alguns países possuem legislação sobre o assunto, mantendo alguns pontos omissos, enquanto outras, como exemplo, o Brasil, nada possuem para regulamentar o assunto.

É fundamental saber do provedor de serviços da nuvem onde ficam armazenados os dados do ponto de vista físico[11]. Você não precisa saber o endereço do datacenter, mas precisa saber a localização geográfica do mesmo. Em caso de falha, meus dados são transferidos para fora do meu país de origem? Caso positivo, que país é esse? Por quanto tempo o dado fica localizado nesta localidade? Este ponto é importante, pois você (contratante) poderá sofrer restrições quanto ao dado sair do país de origem e com isso a decisão de adotar tal provedor já é descartada.

4 LEGISLAÇÃO EM VIGOR E PROJETOS DE LEI

O assunto de computação em nuvem é polêmico, em âmbito mundial. Nenhuma legislação ainda consegue assegurar ao usuário do serviço, proteção absoluta. Muitos países não têm sequer legislação que regule parte do assunto.

4.1 União Européia

A Comunidade Europeia tem o melhor conceito de legislação sobre computação nas nuvens. Trata a segurança das informações como Direito básico do cidadão, igual ao direito a vida privada e familiar.

Em 1995 foi aprovada a Diretiva 46/95, um verdadeiro marco regulatório de proteção de dados na rede mundial de computadores.

A Diretiva em questão - 46/95 apresenta diversas lacunas atuais, porém impõe princípios básicos de interpretação como a disponibilidade, a integridade e a confidencialidade de dados.

A principal característica da normativa é a proibição geral de exportar dados pessoais da União Europeia à países fora do Espaço Econômico Europeu, salvo se o país destinatário tenha direitos e garantias semelhantes a Diretiva 46/95.

Para os países que não apresentem normativa semelhante a Diretiva 46/95, a União Europeia impõe normas mínimas necessárias para a proteção dos dados pessoais. O primeiro exemplo de "tentativa" de adequação do país não europeu é a operacionalização do Códigos de Conduta ("*Binding Corporate Rules*"), conjunto de regra que torna o país "confiável" perante a União Europeia. Uma segunda alternativa é o chamado "acordo de porto seguro", criado no ano 2000 para possibilitar a transferência de dados mais facilitada entre a União Europeia e Estados Unidos, também considerado como país não-adequado.

Atualmente a Comunidade Europeia estuda nova legislação que flexibilize a transferência de informações para Estados não membros ou que haja um controle efetivo desses dados.

O Parlamento Europeu, em 24 de Outubro de 2013^[12] formalizou um relatório expondo as necessidades de uma legislação adequada a reger os pontos positivos e os negativos da utilização do serviço de computação em nuvens. O Relatório ressalta a redução de custos, a possibilidade de acesso de informações em qualquer lugar, a comodidade como pontos positivos para utilização do serviço.

Quanto ao ponto negativo, o relatório ressalta a questão da segurança da informação, tendo em vista que^[13]:

"A introdução de serviços em nuvem transfere a responsabilidade pela conservação da segurança da informação pertencente a cada utilizador individual para o fornecedor, levantando assim a necessidade de assegurar que os fornecedores dos serviços tenham a capacidade legal de fornecer soluções seguras e robustas de comunicação."

O primeiro passo para uma legislação adequada e garantia dos direitos dos usuários é a clara informação ao usuário sobre a utilização do serviço e suas regras. Após a informação prévia, segundo o relatório, a futura legislação deve definir um nível aceitável mínimo quanto a confidencialidade, armazenamento de dados em outros países, responsabilidade pela perda de dados.

A preocupação da União Europeia também é regulamentar a situação de nuvem constante em países não integrantes do grupo, porém com dados europeus. Além disso, a Comunidade ainda estuda a possibilidade do prestador, de outra nacionalidade, exigir a aplicação de normas aplicáveis no seu país de origem.

Havendo dúvidas, e enquanto não houver uma lei uniforme a todos os países membros, aconselha-se que as regras básicas sejam adotadas por todos os membros, bem como a celebração do contrato, a fim de garantir o sigilo das informações.

4.2 Estados Unidos da América

Os Estados Unidos da América possuem diversas legislações versando sobre a proteção de dados. Essa ampla gama de legislação esparsa prejudica a proteção ao direito de confidencialidade de dados pessoais, armazenados em nuvem.

Segundo VAZQUEZ^[14], apesar dos problemas ocasionados pela legislação esparsa e algumas vezes contraditória e desatualizada, o congresso americano é muito reticente em criar uma legislação federal única sobre proteção de dados. Como consequência direta dessa passividade, a *Federal Trade Commission* (FTC), entidade governamental que supervisiona o comércio nos Estados Unidos, acabou por incentivar a auto-regulação e o uso de tecnologias em benefício da proteção de dados, ou seja, aumenta-se a legislação esparsa e os contratos firmados são a única fonte de proteção das partes contratantes. Essa falta de regulamentação uniforme gera grandes incertezas jurídicas e acaba prejudicando a imagem do país como prestador de serviço, sem a devida credibilidade.

4.3 Argentina, Uruguai e Chile

Argentina (Lei 25.326/2000, Decreto 1528/2001), Uruguai (Código Penal Uruguaio, Lei 17.838/2004, Lei 17.930/2005, Diretivas de Governo e controle tributário, Lei 18.331/2008, Proteção de dados e Habeas Data) e Chile (Lei 25.326/2000, Decreto 1528/2001), por exemplo, buscaram adequar-se à legislação europeia e assim, permitir o fluxo de dados entre tais países, beneficiando as empresas localizadas em seus territórios, atraindo investimento de multinacionais europeias, para as quais a transferência de dados sem burocracia é altamente importante.

No caso da Argentina, há um órgão específico para defender os direitos dos cidadãos que sofrerem alguma violação de seus dados. Além disso, há previsão legal no tocante ao uso de técnica que garantam a segurança e confidencialidade dos mesmos, salvo aqueles que mantêm o banco de dados, ou seja, pessoas habilitadas ou caso de ordem judicial. Cabe, ainda, frisar, que a Argentina possui o mesmo posicionamento do que a União Europeia, permitindo o envio e guarda de informações, desde que o país tenha legislação adequada ou tratado sobre o assunto, com exceções para questões médicas, criminais, bancárias ou quando houver tratado internacional neste sentido.

O Uruguai é o que possui o sistema mais rígido de Proteção de Dados, pois, além de um órgão destinado a fiscalizar e fazer cumprir as determinações da legislação que cuida do tema, possui também conceito e legislação explícita sobre criação, guarda, transporte, disponibilidade, divulgação e tratamento de dados em geral. A legislação deste país é tão rígida que a transmissão de dados a outro país ou organização estrangeira é proibida a menos que o destinatário proporcione condições de segurança e proteção de acordo com padrões internacionais ou regionais sobre a matéria, seguindo os normas o entendimento da Comunidade Europeia^[15].

Por sua vez, a legislação chilena^[16] impõe o sigilo de autoria de informações, sempre que não houver condição que sustente seu armazenamento e também exige padrão mínimo de segurança a ser seguido. A transmissão de dados somente ocorrerá para pessoas previamente habilitadas pelo contratante do serviço de guarda.

Apesar de toda a rigidez na proteção dos dados, o Chile firmou tratado com os Estados Unidos no qual o primeiro é obrigado a fornecer informações e livre acesso aos Estados Unidos sobre empresas ou cidadãos de origem americana.

4.4 Brasil

No Brasil, não há leis específicas sobre proteção de dados. Utiliza-se apenas a analogia para questões sobre o assunto.

Questões legais para computação em nuvem tornaram-se uma preocupação dos governos. Como vimos, muitos países querem unificar as legislações a fim de que não haja divergência e concorrência entre elas.

O projeto mais relevante até o momento é o de nº 5344/13, de autoria do deputado Ruy Carneiro (PSDB-PB), que define as diretrizes para regulamentar a armazenagem e o acesso de dados em qualquer parte do mundo.

Segundo o projeto, a empresa contratada será responsável pela restituição dos dados e remoção do conteúdo do cliente de sua base, após o fim do contrato ou por um pedido do usuário, proibindo a cópia, exceto se autorizada anteriormente. No caso de perda do conteúdo do depósito, a empresa deverá indenizar o usuário com o dobro do valor recebido pelo serviço nos últimos 12 meses.

O texto reconhece a privacidade, intimidade e proteção dos dados e da propriedade intelectual, e garante a neutralidade tecnológica e de rede, proibindo privilégios para tecnologias, plataformas ou aplicativos.

A proposta também lista os tipos de informações que devem constar no contrato de serviço de uma empresa, como garantias sobre o conteúdo armazenado e sua recuperação, e os dados de pessoas autorizadas a acessar, alterar ou bloquear arquivos. Neste ponto, o projeto assemelha-se a ideia da União Europeia, sugerindo cláusulas padrões.

Não é informada explicitamente a localização geográfica dos servidores onde as informações serão armazenadas, que podem estar em qualquer parte do mundo. Com isso, há um impasse no direito digital - em caso de acesso aos dados, não há um consenso sobre qual lei deve ser aplicada. Digamos, por exemplo, que há um datacenter que é operado aqui no Brasil e ele está fornecendo um serviço para um alguém na Colômbia. Digamos que o indivíduo, na Colômbia, está acessando esse serviço e os dados estão sendo transportados por meio de um cabo que também atravessa a Venezuela. Qual lei é aplicável à proteção da informação daquele indivíduo? É a lei colombiana, porque o indivíduo vive na Colômbia? É a lei brasileira, porque o datacenter está no Brasil? Ou a lei venezuelana também será aplicável em virtude daquela fração de segundos em que a informação é movida entre o Brasil e a Colômbia?

Ninguém sabe! O projeto de lei não especifica e nenhuma outra lei conseguiu dirimir essa questão. Essa é, na verdade, uma das razões pela qual faz muito sentido para os governos trabalhem em conjunto e tentem adotar leis que sejam razoavelmente parecidas umas com as outras.

Na ausência de posicionamento legislativo brasileiro, resta ao contrato a obrigação de suprir as lacunas, contendo no documento cláusulas essenciais que garantam a qualidade do serviço, a obrigação de atualizar o software e o hardware, sempre que necessário, a obrigação de determinar o que sucederá em caso de perda de dados e a obrigação de definir o prazo para a solução de um problema ou a rapidez com que o serviço de computação em nuvem poderá retirar materiais invasivos, se o utilizador solicitar e a lei aplicável ao caso. Havendo uso indevido de dados, o instrumento deve prever aplicação de penalidade.

Conforme entende a Comunidade Europeia^[17], os contratos brasileiros de serviço de computação em nuvem devem definir, de forma clara e transparente, os direitos e deveres das partes no que se refere às atividades de tratamento de dados por parte dos operadores de serviços de computação em nuvem; assegurem a proteção contra o cancelamento arbitrário do serviço e a supressão de dados; garantam aos clientes uma possibilidade razoável de recuperar os dados armazenados em caso de cancelamento do serviço e/ou supressão de dados; realização de orientações claras aos prestadores de serviço de computação em nuvem para viabilizar uma fácil migração dos seus clientes para outros serviços.

Ensina a Dra. Patrícia Peck (2010) o contrato deve conter questões relevantes como: modelo de autenticação do usuário (senha alfanumérica. Token ou biometria); guarda de prova de acesso (logs de acesso do ambiente), quem faz e por quanto tempo; como é feita a criptografia dos dados; como é feita a disponibilidade dos dados; qual o SLA em caso de apagão digital ou parcial e como fica a proteção de dados que possam estar localizados em datacenters em outra localidade.

5 MARCO CIVIL DA INTERNET

No dia 25 de março de 2014, após quase três anos de tramitação na Câmara, o plenário da Casa aprovou o projeto de lei que é considerado a constituição da internet.

A ausência de um marco civil havia gerado incerteza jurídica quanto ao resultado de questões judiciais relacionadas ao tema.

A nova lei é considerada um avanço pois delimita pontos importantes com a neutralidade, a privacidade etc. O Marco Civil proíbe o acesso de terceiros a dados e correspondências ou comunicação pela rede. Ele também busca garantir a liberdade de expressão e a proteção da privacidade e dos dados pessoais.

Mesmo com direito a privacidade, os registros de atividade dos usuários, segundo o Marco Civil, devem ser guardados pelos provedores num prazo máximo de um ano em ambiente seguro e sigiloso. Devem ser armazenados apenas o IP do computador e data e hora inicial e final da conexão. O documento afirma ainda que essas informações podem ser guardadas anonimamente, sem qualquer dado pessoal do usuário, apenas o IP da máquina. Essa restrição pode prejudicar a segurança na utilização do serviço de computação em nuvem.

Assim, o direito a privacidade estabelecido pelo Marco Civil vai contrariar as necessidades básicas dos usuários da prestação de serviço de computação em nuvem. Como já dissemos, a guarda de log, com dados pessoais é de suma importância, e um ponto muito discutido na União Europeia.

Outro ponto importante é que o Marco Civil da Internet não regulamentou sobre qual legislação aplicar e onde deve estar localizado o Datacenter, com informações de cidadãos ou empresas brasileiras.

A legislação era uma excelente alternativa para regulamentar a atividade, porém deixou de abordar os pontos críticos, mundialmente debatidos.

Continuamos a cargo da negociação contratual para dirimir as questões, que poderiam ter sido abordadas no marco Civil. Também pode-se utilizar os normativos da União Europeia como base para melhor formalização.

De qualquer forma, permanecemos aguardando e necessitando uma legislação que regule questões controvertidas e de alto impacto na prestação de serviço.

Vale salientar que a falta de legislação desestimula os investimentos e crescimento tecnológicos, principalmente advindos de países onde a questão é amplamente debatida, como na Comunidade Europeia e até países vizinhos da América do Sul.

6 CONSIDERAÇÕES FINAIS

Mesmo com o grande volume de utilização do serviço de computação em nuvens, o Brasil ainda encontra-se defasado na regulamentação do assunto.

Muitas vezes, pela falta de legislação específica, o empresário deixa de aderir ao serviço e se beneficiar de suas vantagens.

O Brasil tem um projeto de lei a ser votado, a fim de regulamentar o referido serviço, porém encontra lacunas e problemas com questões de territorialidade.

Por sua vez, o Marco civil da Internet, texto que deveria abordar a questão, foi omissivo quanto a territorialidade dos datacenters que prestarão o serviço na nuvem. Assim sendo, permanece a discussão sobre onde e qual a responsabilidade de quem guarda a informação de terceiro.

No caso de omissão, cabe aos contratantes de serviço de computação nas nuvens, estabelecer obrigação e direitos dos provedores e contratantes. Os contratos devem ser claros e minuciosos em pontos como a responsabilidade de pagamento de energia, Telecom, rede, penalidade no caso de publicação de dados, SLA e planos de contingência, a legislação aplicável em caso de dúvidas etc.

O Brasil como exemplo, deveria seguir o modelo adotado pela União Europeia e outros países da América Latina. A União Europeia, ainda com divergência e irregularidade legislativa para executar o serviço, apresenta uma legislação mais avançada, que prevê que informações de cidadãos europeus devem estar sob a guarda de países que atendam aos requisitos legais.

A ideia de unificação das legislações é o ponto mais viável para a utilização do serviço, tendo em vista a volatilidade da informação e a desnecessidade de verificar a territorialidade do local de guarda dos dados. Devemos lembrar que estamos falando de tecnologia e este é um campo em constante evolução. Para acompanhar, é necessário termos uma legislação que possibilite a contratação e assegure os direitos dos envolvidos, independentemente do local de contratação e guarda dos dados.

Referência

Avanxo. *Quê es Computação em nuvem?* Disponível em: <<http://www.avanxo.com/cloudcomputing.html>> Acesso em: 14 mai. 2013.

Brasil Lei nº 12.527 de 2011 Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011014/2011/lei/12527.htm> Acesso em: 16 jun. 2012.

BRASIL. Lei nº 8.159, de 08 de janeiro de 1991. Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L8159.htm> Acesso em: 16 jun. 2012.

BECK, Ulrich. *La Sociedad del Riesgo Global*. Espana: Siglo Veintiuno, 2002.

CASSARRO, Antônio Carlos. *Controles internos e segurança de sistemas*. São Paulo: LTr, 1997.

CLOUD. Disponível em <<https://chapters.cloudsecurityalliance.org/brazil/2014/01/14/cloud-computing-tendencias-uma-nuvem-de-oportunidades/>>

FUTURECOM. Disponível em: <<http://www.futurecom.com.br/blog/cloud-devera-ultrapassar-us-1-bi-no-brasil-em-2017/>> . Acesso em 25/06/2014

GRECO, Marco Aurélio. *Internet e direito*. São Paulo: Dialética, 2000.

IBM. Disponível em <<https://www-03.ibm.com/press/br/pt/pressrelease/37765.wss>>

Intr@ciência: "Cloud Computing: Impasses legais e normativos". Ano 2, nº 1, p. 16-105, nov. 2010

LIMA, C. C. Preservação digital: a experiência da pesquisa Guignard. Dissertação, 2007. Disponível em: <<http://www.bibliotecadigital.ufmg.br/dspace/bitstream/1843/VPQZ6CQVW/1/preservacaodigitalpqg.pdf>> Acesso em: 28 mai. 2012.

LUCCA, Newton de; SIMÃO FILHO, Adalberto ET all. *Direito e Internet. Aspectos jurídicos relevantes*. São Paulo: Edipro, 2000.

PINHEIRO, Patricia Peck. *Direito Digital*, 4ª ed. São Paulo, Saraiva, 2010.

_____. Disponível em <<http://cio.com.br/opiniaio/2011/11/07/cloud-desafia-o-modelo-juridico-atual-baseado-em-fronteiras-fisicas>>

Revista E-Commerce Brasil, edição 06.

ROHRMANN, Carlos Alberto. *Curso de direito virtual*. Belo Horizonte, Del Rey, 2005, p. 71

SMITH, Brad. *Regulação na Internet: desafios jurídicos e oportunidades para o crescimento econômico*. Revista de Direito, Estado e Telecomunicações, v. 4, n. 1, p. 197-236 (2012)

TAURION, Cezar. *Cloud Computing: Computação em Nuvem*. Rio de Janeiro: Brasport, 2009. 22p.

VASQUEZ, Rafael Ferraz. Disponível em: <http://www.publicadireito.com.br/artigos/?cod=87682805257e619d>

Vaquero, L. M., Roderio-Merino, L., Caceres, J., and Lindner, M. (2009). A Break in the Clouds: Towards a Cloud Definition. *SIGCOMM Comput. Commun. Rev.*, 39(1):50-55.

VENTURA, Luis Henrique. *Comércio e contratos eletrônicos - aspectos jurídicos*. São Paulo: EDIPRO, 2001.

Notas:

[1] GARTNER Disponível em says Cloud Computing Will be as influential as E-Business.

[2] Disponível em <<https://chapters.cloudsecurityalliance.org/brazil/2014/01/14/cloud-computing-tendencias-uma-nuvem-de-oportunidades/>> - Acesso em 30/07/2014

[3] Edição de 22/09/2011

[4] Disponível em: <<http://www.futurecom.com.br/blog/cloud-devera-ultrapassar-us-1-bi-no-brasil-em-2017/>> . Acesso em 25/06/2014

[5] Disponível em <<https://www-03.ibm.com/press/br/pt/pressrelease/37765.wss>> - acessado em 21 de Julho de 2014. Pesquisa conduzida em âmbito mundial com mais de 500 executivos pela divisão de consultoria da IBM em parceria com o instituto de pesquisa Economist Intelligence Unit

[6] Disponível em <<http://www.globalweb.com.br/2013/03/brasil-deixa-de-ser-o-ultimo-no-ranking-anual-de-cloud-computing/>>. Acessado em 01 de Agosto de 2014

[7] Disponível em <<http://cio.com.br/opiniaio/2011/11/07/cloud-desafia-o-modelo-juridico-atual-baseado-em-fronteiras-fisicas/>>. Acessado em 17 de Julho de 2014

[8] Intr@ciência: "Cloud Computing: Impasses legais e normativos". Ano 2, nº 1, p. 16-105, nov. 2010

[9] BECK, Ulrich. *La sociedad del riesgo global*. Espana, Siglo Veintiuno, 2002.

[10] Intr@ciência: "Cloud Computing: Impasses legais e normativos". Ano 2, nº 1, p. 16-105, nov. 2010

[11] Para maiores informações sobre o Freedom of Information (FOIA) ler <http://www.state.gov/m/a/ips>

[12] Disponível em :<[HTTP://www.europarl.europa.eu/sides/getdoc.do?pubRef=-//EP//text+report+A7](http://www.europarl.europa.eu/sides/getdoc.do?pubRef=-//EP//text+report+A7)> Acesso em 05/06/2014

[13] Intr@ciência: "Cloud Computing: Impasses legais e normativos". Ano 2, nº 1, p. 16-105, nov. 2010

[14] Disponível em: <<http://www.publicadireito.com.br/artigos/?cod=87682805257e619d>> Acesso em 10/07/2014

[15] Disponível em <<http://cio.com.br/opiniaio/2011/11/07/cloud-desafia-o-modelo-juridico-atual-baseado-em-fronteiras-fisicas/>> Acesso em 17/07/2014

[16] Disponível em <<http://cio.com.br/opiniaio/2011/11/07/cloud-desafia-o-modelo-juridico-atual-baseado-em-fronteiras-fisicas/>> Acesso em 17/07/2014

[17] Intr@ciência: "Cloud Computing: Impasses legais e normativos". Ano 2, nº 1, p. 16-105, nov. 2010

Luciana Vasco da Silva

Mestranda em Direito Comercial pela Pontifícia Universidade Católica de São Paulo/SP especialista em Direito Empresarial pela Universidade Presbiteriana Mackenzie

Informações Bibliográficas

SILVA, Luciana Vasco da. A necessidade de regulação legislativa para utilização do serviço de computação em nuvem. In: *Âmbito Jurídico*, Rio Grande, XVII, n. 128, set 2014. Disponível em: <

http://www.ambitojuridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=15186&revista_caderno=17

O Âmbito Jurídico não se responsabiliza, nem de forma individual, nem de forma solidária, pelas opiniões, idéias e conceitos emitidos nos textos, por serem de inteira responsabilidade de seu(s) autor(es).