

ASPECTOS CONTRATUAIS NA CONTRATAÇÃO DE SERVIÇOS DE COMPUTAÇÃO EM NUVEM

CONTRACTUAL ASPECTS ON HIRE CLOUD COMPUTING SERVICES

TATIANA SORNAS VIGGIANI¹
WELTON RUBENS VOLPE VELLASCO²

RESUMO:

A internet tem evoluído com muita rapidez, sendo hoje utilizada como uma importante ferramenta, principalmente pelas empresas, para diminuir custos e aumentar a produtividade. Tal ferramenta exige novas perspectivas e assim deve-se criar novos paradigmas. Dentro desse quadro insere-se a Computação em Nuvem que atualizou as formas como os serviços de Tecnologia da Informação são vistos hoje. Nesse contexto, o presente trabalho tem como objetivo principal explicar de maneira simples como alguns serviços de Computação em Nuvem são prestados pela internet com toda sua caracterização jurídica e aplicabilidade das normas. Assim, o interesse deste estudo é demonstrar a importância de mantermos atualizados com a tecnologia, não esquecendo dos deveres, obrigações e responsabilidades dos contratantes, pois, apesar de tratar-se de bens incorpóreos, não deixa de ser um serviço. Para tanto, utilizou-se do método dedutivo, utilizando de pesquisa bibliográfica-documental. Conclui-se no trabalho que, embora o ordenamento jurídico não tenha acompanhado os avanços tecnológicos de nossa sociedade, pode-se utilizar das leis vigentes quando pertinentes e que ainda há muito espaço para discussão dessas novas tecnologias que fazem parte do cotidiano de tantos indivíduos.

Palavras-Chave: Computação em Nuvem. Contratos. Direito Digital. Novas tecnologias.

ABSTRACT:

The internet has evolved very quickly and today is used as an important tool, especially by companies to reduce costs and increase productivity. This tool requires new perspectives and thus must create new paradigms. Within this framework falls within Cloud Computing which updated the ways Information Technology services are seen today. In this context, the present work the main objective explain in a simple way some cloud computing services are delivered over the Internet with all their legal status and enforceability of standards. Thus, the interest of this study is to demonstrate the importance of keeping up with technology, not forgetting the duties, obligations and responsibilities of contractors, because in spite of that it was intangible, it is still a service. For this, we used a deductive method, using research literature and documentary. We conclude the work, although the law has not kept pace with the technological advances of our society, can be used when the relevant existing laws and that there is still much room for discussion of these new technologies that are part of everyday life for many individuals.

Key-words: Cloud Computing. Contracts. Digital Law. New Technologies.

¹ Mestranda em Direito na Universidade de Marília – UNIMAR.

² Mestrando em Direito na Universidade de Marília – UNIMAR.

INTRODUÇÃO

Com o advento da modernidade, muito tem se buscado, principalmente no mundo empresarial, para diminuir custos e aumentar a produtividade.

A tecnologia tem evoluído para esse fim. A internet como ferramenta importante nesse meio também deve evoluir e buscar novas alternativas para favorecer essas novas perspectivas, criando novos paradigmas.

Com o desenvolvimento da tecnologia, evolui-se do 08 bits do fim dos anos 1980 para os gigabits e de repente para os terabits, buscando-se aparelhos e dispositivos com maior capacidade de armazenamento, pois tudo está constantemente mudando, evoluindo, e consumindo mais “espaço” ao mesmo tempo que busca-se praticidade.

Com acesso à internet temos todas as informações necessárias, temos e-mails, redes sociais, nossos documentos da empresa, fotos pessoais, programas para enviar mensagens instantâneas, e tudo isso sem “travar” o dispositivo e ter que esperar horas para reiniciar como antigamente, pois não está nada na memória do dispositivo, e sim *online*.

Essa praticidade também chama a atenção de empresas, que observam aqui a oportunidade de economizar, ao mesmo tempo em que se desenvolve, pois ao utilizar a nova tecnologia disponível, da qual trataremos no presente trabalho, ela deixa de gastar com equipamentos físicos (hardwares, roteadores, etc.) já que pode ter acesso a uma estrutura mais avançada e com mais segurança do que ela sozinha poderia implantar.

Para tanto, o primeiro capítulo apresenta um breve histórico da internet e da computação em nuvem, para então introduzir e definir especificamente quais são as características dessa nova tecnologia, chamada Computação em Nuvem. O segundo capítulo versa sobre os aspectos contratuais que envolvem a contratação desses serviços. Posteriormente busca-se responder os possíveis problemas que venham a ocorrer por conta desse novo conceito e paradigma introduzido por essa nova tecnologia, ou seja, problemas referentes à jurisdição, segurança e privacidade, responsabilidades, abordando, por fim, como solucionar controvérsias relativas a essa nova modalidade de contratação.

O trabalho utilizou o método dedutivo, utilizando de pesquisa bibliográfica-documental. Foram utilizados principalmente artigos científicos da área de tecnologia da informação, artigos científicos jurídicos, trabalho de conclusão de curso jurídico, doutrinas, legislação, jurisprudência e notícias via internet. Foi inclusive pesquisadas legislações e documentos estrangeiros (Estados Unidos e Europa) para poder traçar um comparativo com a legislação brasileira.

O trabalho mostra-se relevante, pois, apresenta uma caracterização jurídica acerca desse novo tema, que é pouco abordado na área de direito, sendo mais conhecido em TI, mas que torna-se cada vez mais comum no cotidiano tanto de pessoas físicas quanto jurídicas. Assim, é importante também trazer essa discussão para o âmbito jurídico, sendo esta a meta estabelecida pelo presente trabalho ao abordar temas legais essenciais para seu bom uso, já que as questões legais têm sido retratadas como problemáticas pelos artigos de TI.

1 INTERNET E A COMPUTAÇÃO EM NUVEM

1.1 HISTÓRIA DA INTERNET

Atualmente uma grande parte dos indivíduos encontra-se *online* através da Internet, tornando assim a vida virtual uma parte essencial do cotidiano da vida real. Dificilmente pensa-se, quando *online*, na abrangência, no conceito ou na história desse meio de comunicação.

Pode-se definir a Internet, hoje, como um sistema global de rede de computadores que permite tanto a comunicação quanto a transferência de dados ou arquivos de uma máquina (ou dispositivo) a qualquer outra que esteja conectada a tal rede. Isso permite um intercâmbio de informações de maneira rápida, eficiente e sem limitações de fronteiras, sem precedentes na história, que tem como resultado a criação de novos mecanismos de relacionamento (CORRÊA, 2000, p. 08).

Em meados de 1969, a Agência de Projetos Avançados (ARPA) do Departamento de Defesa Norte-Americano, seguindo o projeto intitulado ARPANET, confiou à *Rand Corporation* a criação de um sistema de telecomunicações que garantisse que um ataque nuclear russo não interrompesse a cadeia de comando dos Estados Unidos.

Primeiramente, portanto, tal sistema era responsável pela distribuição de texto entre um pequeno número de funcionários de instituições norte-americanas destinadas à pesquisa de implantação de mecanismos de defesa militar, ou seja, foi desenvolvido como uma arma a ser utilizada na Guerra Fria.

O sistema era baseado na criação de pequenas redes locais (LAN), posicionadas em locais estratégicos do país e coligadas por meio de redes de telecomunicações geográficas (WAN). Assim, na eventualidade de uma cidade vir a ser destruída por um ataque nuclear, essa rede de redes conexas – a Internet (*Inter Networking* – coligação entre redes locais distantes) garantiria a comunicação entre as demais cidades coligadas.

No ano de 1973 ocorreu a decolagem da Internet, quando Vinton Cerf, do Departamento de Pesquisa Avançada da Universidade da Califórnia e então responsável pelo projeto, registrou o Protocolo de Controle de Transmissão / Protocolo Internet (Protocolo TCP/IP). Tal protocolo trata-se de um código que consente a diversos *networks* incompatíveis (por programas e sistemas) comunicarem-se entre si.

O elemento mais importante que permite à Internet se transformar em um instrumento comunicação em massa foi o *World Wide Web* (WWW), a rede mundial conciliada com o desenvolvimento de navegadores. O WWW nasceu em 1989 no Laboratório Europeu de Física de Altas Energias, que tem sua sede em Genebra. Ele é composto por hipertextos, ou seja, documentos cujo texto, imagens e sons são evidenciados de forma particular e podem ser relacionados com outros documentos, sem que o usuário necessite conhecer os inúmeros protocolos de acesso.

O ano de 1992 marcou o aprimoramento de tal sistema, quando um grupo de programadores desenvolvedores do *browser* WWW o tornou acessível ao domínio público, apresentando-o inclusive para um grande número de pessoas e de organizações.

Entretanto, a Internet não pode ser simplificada somente ao WWW, pois, justamente devido a sua extensão e amplitude, ela também pode significar o meio pelo qual o correio eletrônico, os servidores FTP, a WWW, o *Usenet* e outros serviços trafegam (CORRÊA, 2000, p. 09).

Portanto, a partir da década de 1990 a internet passou a ser utilizada por outros setores, não se restringindo apenas aos órgãos do governo norte-americano e a defesa de seu território. Novos programas e novos navegadores começaram a ser produzidos de maneira a tornar a Internet cada vez mais acessível, principalmente para indivíduos comuns.

Segundo alguns pesquisadores, desde o projeto ARPANET, a principal ideia era de que a Internet viesse a ser um serviço de utilidade pública, o que só foi possível com o desenvolvimento de vários navegadores e o surgimento acelerado de provedores de acesso e portais de serviços online.

A Internet se desenvolveu a tal ponto que é possível ver sua influência no mundo real, como dito, pois hoje muitas pessoas dependem dessa rede de comunicações no seu dia a dia, levando até a imaginar em como seria o mundo, hoje, sem internet.

Assim, nesse novo cenário surge a Computação em Nuvem, que será estudada no subcapítulo posterior.

1.2 A COMPUTAÇÃO EM NUVEM

A Computação em Nuvem (ou *Cloud Computing*) tem como principal funcionalidade a utilização de recursos diversos por meio da Internet, e sua ideia não é tão recente como nos aparenta ser. Ela vem sendo pensada desde o início da Internet, no fim da década de 1960, com Joseph Carl, um dos desenvolvedores do ARPANET.

Mesmo com a ideia sendo tão antiga, apenas em 1997 o termo Computação em Nuvem foi mencionado em uma palestra pelo professor de sistemas da informação Ramnath Chellappa, sendo realmente desenvolvido a partir de 1999.

A *Cloud Computing* representa uma mudança de paradigma no fornecimento de serviços computacionais, atualizando a maneira como serviços de Tecnologia da Informação (TI) são inventados, desenvolvidos e até vendidos.

Ano a ano surgem novos desafios para aqueles que atuam na área de TI relacionados principalmente com a complexidade de manutenção e gerenciamento da infraestrutura, que deve ser cada vez mais eficaz e com menos custos.

Mas não apenas as empresas são as usuárias de *Cloud Computing*. Pessoas físicas cada vez mais utilizam desse método novo de armazenagem de dados devido principalmente as novas tecnologias, já que os serviços são cada vez mais confiáveis e de melhor desempenho (com mais capacidade de armazenamento, muitas vezes, do que o dispositivo utilizado), disponíveis sempre que necessário sendo acessíveis de diferentes lugares via internet não ficando mais restrito a um único dispositivo (pode-se acessar do celular, *tablet*, notebook, computador, *e-book reader*, etc.).

Cloud Computing não possui uma definição única ou restrita. Segundo o Parecer 05/2012 relativo a computação em nuvem do Grupo de Trabalho para a Proteção de Dados Instituído pelo artigo 29º da Diretiva 95/46/CE da União Européia (que trata sobre privacidade e proteção de dados)

A computação em nuvem consiste num conjunto de tecnologias e modelos de serviços centrados na utilização e fornecimento via Internet de aplicações informáticas, de capacidade de tratamento e armazenamento e de espaço de memória. A computação em nuvem pode gerar importantes benefícios económicos, uma vez que os recursos a pedido podem ser com bastante facilidade configurados, alargados e acedidos via Internet. (UNIÃO EUROPEIA, 2012)

O Brasil ainda não tem uma definição legal para *Cloud Computing*, mas o Projeto de Lei 5.344/2013 de iniciativa do Sr. Ruy Carneiro, define

Art. 1º, § 1º - A computação em nuvem é definida como a exploração da atividade de tratamento, armazenamento, guarda e depósito virtuais, por sistemas eletrônicos ou eletromagnéticos e mediante contrato oneroso ou gratuito, no qual o depositário recebe informações, sistemas, programas, plataformas, ou qualquer espécie de dados do depositante ou titular, sejam codificados ou não, considerados conteúdos ou bens, [...] (BRASIL, CÂMARA DOS DEPUTADOS. Projeto de Lei 5.344/2013)

A definição americana proposta pelo *National Institute of Standards and Technology* (NIST) em 2011 foi a mais completa, propondo que a computação em nuvem é um modelo para permitir acesso oblíquo, sob demanda, de rede a um *pool* compartilhado de recursos computacionais configuráveis (por exemplo, redes, servidores, armazenamento, aplicações e serviços) que podem ser rapidamente provisionados e liberados com esforço de gerenciamento ou interação com o provedor de serviços mínimos (MELL; GRANCE, 2011). Este modelo de nuvem possui cinco características essenciais, a saber: *on-demand self-service*, *broad network access*, *pooling* de recursos, elasticidade rápida e serviço medido.

Cloud Computing refere-se tanto aos aplicativos entregues como serviços através da internet como hardwares e sistemas de softwares de *data centers* que providenciam esses serviços. A diferença entre os serviços é o que define os três modelos de serviço: SaaS (*Software as a Service*), PaaS (*Platform as a Service*) e IaaS (*Infrastructure as a Service*).

1.2.1 *Software as a Service* (SaaS)

O SaaS é um modelo flexível, onde a aquisição e/ou utilização de um software não está relacionado a compra de licença. Segundo Pinheiro (2013, p. 262) nesse modelo de serviço são oferecidas ao consumidor aplicações que rodam em uma infraestrutura de nuvem do provedor, acessíveis por vários dispositivos, por meio de uma interface leve como um navegador de internet. Ele permite que o usuário controle o que necessita, pagando (ou não, pois em alguns casos o serviço pode ser gratuito) apenas pelo que utilizou em determinada situação ou período.

Um exemplo de Software como serviço amplamente utilizado é o programa *Skype*, um software de comunicação com várias funções, sendo algumas gratuitas e outras tarifadas. O usuário contrata aquilo que necessita pelo próprio software, aceitando seus termos de serviço. Outros exemplos de SaaS são o *GoogleApps* e o *DropBox*.

As principais características dessa modalidade de serviço são: acesso ao aplicativo via internet, o gerenciamento do aplicativo é realizado de forma centralizada, o usuário não é

responsável por atualizações ou aplicações de correções no aplicativo e seu modelo é utilizado da forma de “um para muitos” (não é individualizado). Ou seja, aqui o usuário não gerencia a infraestrutura, somente as configurações de usuário de aplicação.

Este modelo não é a melhor opção quando há a necessidade de processamento de dados extremamente rápido ou em tempo real; ou no caso de uma legislação ou regulamentação que proíba certos dados de serem hospedados fora do país ou da empresa.

1.2.2 *Plataform as a Service (PaaS)*

O segundo segmento de serviços em computação em nuvem é a Plataforma como Serviço (PaaS), que fornece ao consumidor a capacidade de desenvolver suas próprias aplicações através de uma tecnologia adquirida (*framework*, por exemplo) para que possa funcionar em um determinado ambiente. Enquanto o consumidor é livre para desenvolver aplicativos que quiser, sua plataforma é bloqueada. Esse método de desenvolver aplicativos podem gerar baixos custos, possibilitar acesso a um maior número de ferramentas de criação como facilitar na hora de distribuir o aplicativo pronto para um maior número de pessoas.

Um dos grandes exemplos de PaaS é o *Facebook*. Desenvolvedores podem criar aplicativos específicos para a plataforma do *Facebook* e deixá-los disponível para qualquer um de seus usuários (jogos, por exemplo).

O PaaS é análogo ao SaaS, exceto que, ao invés de ser um software entregue pronto pela internet, é uma plataforma utilizada para criação, hospedagem e controle de software. Assim, suas ofertas mais comuns incluem serviços de colaboração em equipe, integração de banco de dados e gerenciamento de estado, segurança e possibilita o design, controle, testes e implantação de aplicativos. Vários usuários simultâneos podem utilizar o mesmo aplicativo, facilitando a composição de um novo aplicativo, mas nenhum irá gerenciar a infraestrutura.

1.2.3 *Infrastructure as a Service (IaaS)*

O terceiro segmento de serviço de computação em nuvem é conhecido como Infraestrutura como Serviço. Esta é a plataforma de serviço mais abrangente e é utilizada principalmente por desenvolvedores em tempo integral ou clientes empresariais em grande escala.

Enquanto o SaaS permite o uso de software em nuvens e o PaaS permite o desenvolvimento de aplicativos, o IaaS oferece toda a infraestrutura necessária para o desenvolvimento, execução e armazenamento de aplicativos e dados em ambiente de nuvem.

O benefício da IaaS é o armazenamento praticamente ilimitado (dependendo do serviço contratado) e o poder de computação disponível para desenvolvedores sem que tenham uma estrutura de hardwares físicos no seu local de trabalho, ou seja, tem como principal benefício a redução dos custos com infraestrutura, pois não é mais necessário investir em hardwares, roteadores, serviços de redes dentro da própria empresa.

Segundo Pinheiro (2013, p. 262) são oferecidos aos usuários maneiras de provisionar o processamento, o espaço em disco, redes e demais recursos essenciais em que o usuário consegue instalar softwares, incluindo sistemas operacionais e aplicações. No entanto, como os demais modelos de serviço, o usuário não gerencia a infraestrutura da nuvem, mas tem o controle dos recursos provisionados, inclusive algumas configurações de componentes de rede (como *firewalls*).

No IaaS também é utilizado o modelo *pay-per-use*, onde a cobrança é baseada no serviço e não no produto. Pode-se contratar uma quantidade determinada de servidores por um determinado período de tempo, por exemplo. O custo assim pode ser variável pelo uso ou definido de forma prévia.

Esta é uma boa opção para sites que tem a demanda muito volátil com picos significativos (por exemplo, lojas virtuais) e para novas empresas sem capital para investir em infraestrutura. No entanto, tal segmento exige profissionais com um avançado conhecimento técnico para utilizar suas ferramentas, uma vez que é mais complicado e necessita desenvolver todo o software que será utilizado.

A *Amazon*, um dos maiores serviços de comércio eletrônico do mundo, para suportar o volume de vendas no período de Natal montou uma superestrutura de processamento e armazenamento de dados, que encontra-se espalhado por todo território dos Estados Unidos. Tal superestrutura fica ociosa na maior parte do ano, assim, a empresa aluga tais recursos, oferecendo os serviços de *Simple Storage Solution* (S3) para armazenamento de dados e *Elastic Compute Cloud* (EC2) para o uso de máquinas virtuais.

O EC2 é um excelente exemplo de IaaS, pois suporta desde o menor aplicativo até sites em grande escala, fornecendo infraestrutura em nuvem para executá-los. Os usuários têm, portanto, flexibilidade para desenvolver o que desejarem utilizando uma variedade de ferramentas em ambientes como Linux ou Windows.

1.2.4 Modelos de Implantação

Ainda segundo o NIST, a Computação em Nuvem, além de possuir cinco características e três modelos de serviço, ainda tem quatro diferentes tipos de implantação, a saber:

- a) Nuvem Privada: A infraestrutura dessa nuvem é construída para o uso exclusivo de uma única organização (compreendendo talvez múltiplos consumidores, como no caso de uma unidade de negócios, por exemplo, matriz e filiais). A estrutura pertence, é gerida e operada pela organização, essa que possui total controle sobre como as aplicações são implantadas na nuvem. Geralmente uma nuvem privada é construída em um *data center* privado. Ela é feita sob medida, os provedores arcam com todos os custos e têm o comando da segurança, por isso é muito mais cara.
- b) Nuvem Pública: É quando a infraestrutura é disponível para o uso aberto do público em geral. A infraestrutura tem recursos compartilhados, padronizados e com autoatendimento pela internet. Pode pertencer, ser mantida e operada por um empresa, um organização governamental ou mesmo acadêmica, ou uma combinação delas.
- c) Nuvem Comunitária: A infraestrutura dessa nuvem é para o uso exclusivo de uma específica comunidade de consumidores de organizações que compartilham interesses em comum (por exemplo, missão, requerimento de segurança, política, etc). Esta nuvem pode pertencer, ser mantida e operada por uma ou mais organizações que fazem parte dessa comunidade, uma terceira parte, ou uma combinação entre ambas.
- d) Nuvem Híbrida: É uma combinação de duas ou mais nuvens distintas, possibilitando utilizar as melhores características de ambas para portabilidade de dados e aplicativos.

2 CONTRATOS DE SERVIÇOS

Após estudar a história da Internet e o que é a Computação em Nuvem, cabe então estudar seus aspectos legais, objeto do presente trabalho, iniciando com os contratos de prestação de serviços, pois como visto anteriormente, a Computação em Nuvem é oferecida como serviço.

Segundo o artigo publicado pela Revista USP, o *Cloud Computing* tem vários problemas de segurança, entre eles: segurança de rede, interface, segurança de dados, virtualização, governança, conformidade e questões legais.

Vários desses problemas podem ser resolvidos apenas solucionando as questões legais. No Brasil ainda não há legislação específica para tratar do assunto, e há pouco dissertado no âmbito jurídico por se tratar de um tema muito recente.

Diferente do que ocorre na União Européia, por exemplo, onde o Parecer 05/2012 relativo a computação em nuvem em seu item 3.2 define qual o direito aplicável ao tema, a saber: artigo 4º da Diretiva 95/46/CE.

No Brasil a legislação civil pouco avançou para acobertar, proteger e classificar os inúmeros contratos atípicos que estão surgindo com o advento da internet.

Contrato eletrônico é aquele celebrado por meio de programas de computador ou aparelhos com tais programas. Dispensam assinatura ou exigem assinatura codificada ou senha. A segurança de tais contratos vem sendo desenvolvida por processos de codificação secreta, chamados de criptologia ou encriptação. (GLANZ, 1998, p 72)

Contrato, primeiramente, em sua definição clássica é um acordo de vontades entre as partes. Mas no caso do contrato pela internet, nem sempre é um acordo de vontades, já que ao adquirir um software muitas vezes temos que clicar em “Li e Aceito os Termos e Condições” que o fabricante nos oferece, e no caso de não aceite, simplesmente não há a instalação ou utilização do software desejado. Muitas vezes não há como discutir cláusulas contratuais já que são feitas no modelo de “um para muitos”. Esse contrato ocorre principalmente quando tratamos de SaaS e pessoas físicas. Ou seja, não há o período pré-contratual devido a instantaneidade da internet, o que ofusca em parte o negócio jurídico e prejudica a confiança das partes.

A Lei do Software (Lei nº 9.609/98) em seu artigo 9º determina que o simples uso de um programa de computador deverá ser objeto de licença de uso, no entanto, como já dito anteriormente, no caso específico da Computação em Nuvem, seu uso não depende de licença.

Esses são os contratos-tipo, onde todas as cláusulas são impostas por uma parte à outra; e há também os contratos específicos, nos quais a elaboração é feita caso a caso, dependendo do *status* do contratante. No caso de empresas há um poder de barganha maior, mas nem sempre existente dependendo do tamanho da empresa.

No caso de contratos específicos, o Direito Digital deve-se atentar para quatro pontos importantes: a terminologia utilizada, a determinação das responsabilidades, o tipo de informação que será veiculada e o foro ou cláusula arbitral para eventual problema

(PINHEIRO, 2013). Não pode esquecer tampouco das cláusulas específicas de segurança da informação, de autenticação, de recuperação da informação (backups), guarda de provas eletrônicas, assim como um Acordo de Nível de Serviço que deve ser elaborado em conjunto com o responsável de TI.

No caso de empresas que querem economizar nos custos em sua área de TI, o contrato deve ser elaborado caso a caso, de acordo com as necessidades específicas e os direitos e obrigações que devem estar garantidos.

Pinheiro elabora um roteiro de indicadores mínimos de análise jurídica que devem ser observados pelas empresas na contratação desse tipo de serviço e deve ser usado para realização de um diagnóstico da necessidade e do risco do contrato, a saber:

- Eu preciso ter acesso aos meus dados de qualquer lugar?
- Eu preciso ter acesso a todos os dados ou só a alguns, rotineiramente?
- Só eu preciso ter acesso ou várias pessoas precisam ter acesso?
- Qual o nível de sensibilidade das informações que precisam ser acessadas?
- Qual a possibilidade de publicidade da informação a ser acessada, ela é ostensiva, confidencial ou ultrassecreta?
- Qual a segurança da informação aplicada ao ambiente pelo fornecedor do serviço de computação em nuvem, considerando que não há só uma máquina ou local a proteger e sim múltiplas máquinas e locais a proteger?
- Qual a segurança da informação aplicada para autenticar quem vai ter acesso às informações pela Internet?
- Qual a segurança da informação aplicada aos dados diretamente, que os acompanha onde eles estiverem (ex. estarão criptografados)?
- Qual a alternativa apresentada pelo fornecedor em um cenário de apagão eletrônico? Como você terá acesso aos seus dados se a Internet sair do ar? Há uma outra forma planejada (plano de contingência, redundância)?
- Qual o impacto se ocorrer um vazamento da informação acessada?
- Qual o impacto se houver indisponibilidade completa de acesso à informação?
- Quanto tempo você pode ficar sem ter acesso à informação, qual o limite (pelo menos 48h é um tempo mínimo esperado para uma recuperação da informação ou do acesso em si, calculado desde o bug do milênio)?
- Está prevista uma redundância do fornecedor, se ele ficar indisponível, vier a sofrer um incidente, tiver decretada falência, concordata, deixar de operar, passar por uma fusão e aquisição, o que ocorre com seus dados (quais os procedimentos previstos nessas situações)?

- E se o próximo bug do milênio for uma pane geral na Internet, qual o plano B?
- O que está previsto no contrato para lhe proteger técnica e juridicamente no uso da computação em nuvem?
- Há um SLA para disponibilidade dos dados, recuperação inclusive em situação de caso fortuito e força maior? Qual a responsabilidade das partes específicas de segurança da informação? Qual a penalidade (o valor é proporcional à necessidade de trazer os dados de volta)? (PINHEIRO, 2013)

Com base nas respostas às questões feitas por Pinheiro será assim possível elaborar um plano para a utilização da computação em nuvem de forma mais positiva, no entanto, nem todas as questões estão passíveis de serem respondidas dentro de um único instrumento contratual.

A atual Lei do Marco Civil da Internet (Lei nº 12.965/2014) determina em seu artigo 7º que ao usuário são assegurados os direitos:

- VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;
- VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
- VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
 - a) justifiquem sua coleta;
 - b) não sejam vedadas pela legislação; e
 - c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;
- IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;
- X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei; (BRASIL, Lei nº 12.965/2014.)

Assim, a nova Lei do Marco Civil veio de encontro a uma necessidade social de regulamentar a internet de forma a assegurar os direitos dos usuários brasileiros, mas, no entanto, como iremos observar, essa lei pode encontrar problemas no que concerne à jurisdição, já que nem sempre os dados serão armazenados em território nacional.

Torna-se conveniente, portanto, estudar qual jurisdição e quais leis que irão reger esses tipos de contratos.

3 JURISDIÇÃO

Alguns princípios do Direito devem ser repensados à luz da Internet, como o da territorialidade, já que não é mais possível definir qual território ocorreram as relações jurídicas, os fatos e seus efeitos.

No mundo tradicional, a questão da demarcação do território sempre foi definida por dois aspectos: os recursos físicos que esse território contém e o raio de abrangência de uma determinada cultura. A sociedade digital rompe essas duas barreiras: o mundo virtual constrói novo território, dificilmente demarcável, e a própria riqueza assume caráter diferente, baseada na informação, que é inesgotável e pode ser duplicada infinitamente. (PINHEIRO, 2013, p. 34)

Como visto no primeiro capítulo, é cada vez mais comum o uso da computação em nuvem tanto por empresas como por pessoas físicas. E aqui entra um problema referente a territorialidade, já que os *data centers*, locais onde os dados são armazenados, nem sempre encontram-se no Brasil.

Como dito anteriormente, a *Amazon* criou os serviços de S3 e EC2. O EC2 é amplamente utilizado como serviço de IaaS principalmente por lojas virtuais, e estas nem sempre são apenas americanas. Assim como o serviço de S3, que é utilizado pelo *DropBox*, principalmente como SaaS, por 200 milhões de usuários e armazena mais de bilhão de arquivos em sua plataforma a cada 24 horas. E os *data centers* da *Amazon* são espalhados por todo o território norte-americano.

No caso do *Facebook*, utilizado como PaaS, seus *data centers* ficam espalhados ao redor do mundo. Sua principal instalação fica nos Estados Unidos, mas também possui um *data center* na Suécia e há planos de um novo na Ásia.

Assim, é difícil para a Lei Brasileira regular algo que, mesmo utilizado por usuários brasileiros, encontra-se fora de seu território nacional.

Como a internet possibilita aos consumidores a contratação de serviços de outros países perde-se a territorialidade, desse modo o Código de Defesa do Consumidor perde sua força, havendo um confronto entre as normas de proteção nacionais e as regras estrangeiras.

A Lei de Introdução às Normas do Direito Brasileiro (Decreto-Lei nº 4.657 de 1942) tenta regulamentar situações como estas, juntamente com acordos firmados no âmbito do direito internacional.

O primeiro Projeto de Lei sobre o Marco Civil da Internet previa que os *data centers* deveriam ser localizados em território nacional, mas tal parágrafo foi retirado da Lei que foi aprovada, pois para tal necessitaria grande investimento.

As áreas para construções de *data centers*, assim como os investimentos com essas tecnologias são altos, o que vez com que fosse repensado no Marco Civil da Internet, e no Projeto de Lei nº 5.344/2013 recebesse especial atenção sua extraterritorialidade, conforme artigo 2º, incisos I a III.

A Comissão das Nações Unidas para o Direito do Comércio Internacional (UNCITRAL) elaborou e adotou em 1996 uma lei-modelo para uniformização dos problemas jurídicos envolvendo a Internet.

A lei-modelo [...] tem por objetivo facilitar o uso dos meios de comunicação e de armazenamento de informação, tais como a troca de dados eletrônicos (*eletronic data interchange [EDI]*), correio eletrônico (*e-mail*) e a telecópia, e demais ferramentas de TI. [...] A lei-modelo trata, ainda, dos seguintes aspectos: validade de dados armazenados em suporte informático como meio de prova em litígio; momento de formação dos contratos eletrônicos; lugar de envio e recebimento de mensagens de dados, entre outros. (AMARAL, 2004, p. 313)

Com base nessa lei-modelo havia o Projeto de Lei nº 672 de 1999 (arquivado), de autoria do senador Lúcio Alcântara, que estabelecia a regra do lugar que se considera enviada ou recebida a uma mensagem para contratos eletrônicos, dirimindo assim o problema de foro e também da legislação aplicável.

Assim, a alternativa para a questão da jurisdição pode ser a escolha explícita no contrato da adoção da lei brasileira. Caso contrário, se a opção for por uma lei estrangeira ou a lei do local de hospedagem, as empresas devem conhecer os riscos da hospedagem de informações fora do Brasil (no caso de ordens judiciais, quebra de sigilo, etc.).

Como no Brasil ainda não há legislação específica para regular o caso da extraterritorialidade na internet, principalmente no caso da computação em nuvem, deve-se atentar então para o estabelecido, como dito anteriormente, na Lei de Introdução às Normas do Direito Brasileiro e ao Direito Internacional. Mas a ênfase deve ser dada ao contrato que irá gerar a prestação de serviço e que irá determinar de fato como resolver possíveis problemas.

Mas não apenas a questão da territorialidade deve ser analisada ao ser estabelecido um contrato de prestação de serviço. Outros fatores também serão determinantes para que o contrato seja estabelecido de modo a favorecer e a resguardar ambas as partes.

É o caso das questões de privacidade e segurança, que podem ser diferentemente estabelecidas conforme a lei onde é prestado o serviço ou onde estão localizados os *data centers*, conforme podemos observar no capítulo que segue.

4 PRIVACIDADE E SEGURANÇA

Todo sistema computacional precisa ser protegido, porém é necessário analisar a sensibilidade dos dados que uma aplicação irá manipular para que a segurança seja adequada. Para tal, deve-se preservar propriedades básicas: confidencialidade, integridade, disponibilidade, autenticidade e não repúdio.

A segurança de sistemas computacionais envolve temas como políticas (conjunto de regras) de segurança e sua utilização em diferentes contextos – comercial, militar, doméstico, etc. e a gerência de riscos. As políticas de segurança envolvem, por exemplo, definição de regras para: proteção do nível físico; contenção, recuperação de desastres, backup, preservação (durante o uso) e destruição (após o uso) de mídias; [...] criptografia e ciclos de chaves; controle de acesso a sistemas e a recursos; não violação à leis e a ética, etc. A gerência de risco envolve a avaliação sistêmica e continuada dos níveis de segurança computacionais, avaliando os vários sistemas e aplicações de forma integrada para identificar vulnerabilidades, visando eliminá-las. Mitiga-las ou tolerá-las. (MARCON JR.; SANTIN; MAZIERO, 2011, p. 72)

Cada modelo de serviço da Computação em Nuvem (IaaS, PaaS ou SaaS) possui um nível de segurança diferente que deve ser entendido pelo adquirente do serviço, ou, no caso de empresas, pelo responsável pela área de TI, para que quando for realizado o contrato nada seja olvidado.

Quanto aos projetos de Leis que tramitam tanto no Senado quanto na Câmara dos Deputados e na Nova Lei sobre o Marco Civil da Internet, esses têm sim disposições sobre o tema.

A Nova Lei sobre o Marco Civil da Internet disciplina:

Art. 3 A disciplina do uso da Internet no Brasil tem os seguintes princípios:
I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição;
II - proteção da privacidade;
III - proteção aos dados pessoais, na forma da lei;
IV - preservação e garantia da neutralidade da rede, conforme regulamentação;
V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei; e
VII - preservação da natureza participativa da rede.
Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria, ou nos tratados internacionais em que a República Federativa do Brasil seja parte.[...]

Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.[...]

Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros. [...]

E o Projeto de Lei 5.344/2013 reconhece a privacidade, a intimidade e a proteção dos dados em seu artigo 2º, IV.

O problema da privacidade torna-se maior quando o uso dessas novas ferramentas passa a afetar o mundo corporativo, atentando contra o regime jurídico da livre iniciativa. A modalidade conhecida como espionagem a distância, ou de utilização de hackers para subtração e divulgação de informação sigilosa ou reservada, contida nos sistemas de informações ou banco de dados, quando afetar as relações entre empresas entrará em conflito com a Lei nº 9.279/96. (AMARAL, 2004, p. 314)

No entanto, a legislação brasileira determina que algumas informações sigilosas e de segurança nacional sejam processadas e guardadas dentro do país (por exemplo, dados da previdência social, sistema financeiro, consumidores de serviços públicos, dados financeiros do Banco Central, etc.), ou seja, tais informações não devem ser armazenadas em *data centers* em outros países. A principal preocupação do governo brasileiro é com a indisponibilidade das redes que impeça o acesso a dados sensíveis e a privacidade, mas principalmente com a segurança nacional após o episódio de suposta espionagem pelo governo norte-americano.

No caso da divulgação de dados da administração estatal, o agente infrator sofrerá as sanções previstas no artigo 153,§ 1º-A do Código Penal Brasileiro.

Alguns outros países também possuem legislação vigente que proíbe dados públicos de serem alojados fora do país, para assim inibir possíveis problemas quanto à privacidade.

A União Européia elaborou e aprovou a Diretiva 46/95/CE prezando pela privacidade e em 2004 criou a ENISA – *European Network and Information Security Agency* com o objetivo de melhorar a segurança das informações, desenvolvendo uma cultura de rede e segurança para seus cidadãos, consumidores e empresas.

Nos Estados Unidos, após o 11 de setembro, foi criada a TIA – *Total Information Awareness*, com o objetivo de coletar o maior número de informações sobre cidadãos norte-americanos e suas ligações com estrangeiros, o que é hoje alvo de constantes ataques por legitimar a espionagem pelo governo (prevê a segurança acima da privacidade).

No caso de problemas com relação à segurança e a privacidade, resta então saber como estarão estabelecidas as responsabilidades de cada uma das partes, tópico relevante que também deve ser abordado pelo contrato, mas que em muitos casos esse é omissivo. Em havendo omissão no contrato, resta às leis estabelecerem as responsabilidades.

5 RESPONSABILIDADES

No que tange à responsabilidade, por se tratar de um assunto tão novo e dependente de termos técnicos da área de TI ainda apresenta situações muito conflitantes.

No caso da opção pela utilização de uma nuvem fora do Brasil, é necessário sempre conhecer as obrigações do provedor e seus direitos. As responsabilidades dos prestadores de serviço devem estar sempre bem estabelecidas para que não haja riscos ou eventuais custos. Por exemplo, no caso de apagões de energia, de infrações com vazamento de dados (se a rede é criptografada), perda de dados, quais serão as penalidades impostas pela lei e pelo prestador do serviço, e se elas serão suficientes para suprir o eventual dano.

O Direito Digital, por sua necessidade de dinamismo, trouxe algumas modificações nos conceitos de responsabilidade. No âmbito jurídico adota-se a teoria da culpa e a teoria do risco, mas no direito digital apenas a teoria do risco é aplicável.

Considerando apenas a Internet, que é a mídia e veículo de comunicação, seu potencial de danos indiretos é muito maior que o de danos diretos, e a possibilidade de causar prejuízos a outrem, mesmo que sem culpa, é real. Por isso, a teoria do risco atende e soluciona de modo mais adequado as questões virtuais, devendo estar muito bem associada à determinação legal de quem é o dever de prova em cada caso. (PECK, 2012, p. 146)

O Código Civil de 2002 em seu artigo 927, parágrafo único, adota a teoria do risco, e por não haver previsão legal para internet, esse dispositivo, assim como o artigo 14 do Código de Defesa do Consumidor podem ser aplicados, dependendo do caso concreto e de acordo com o julgador.

Tem-se ainda no Brasil a completa ausência de marco regulador do uso das tecnologias via Internet, de modo que, mesmo havendo legislações que sirvam para dirimir as controvérsias, tais como a LINDB (Lei de Introdução às Normas do Direito Brasileiro – Lei nº 12.376/2010), ou ainda o Código de Defesa do Consumidor (Lei nº 8.078/90) a subsunção fato-norma nunca será perfeita, demandando assim, por parte do aplicador do direito, a utilização de mecanismos integradores da norma tais como a analogia, os usos, os costumes e a equidade. (PARCHEN, FREITAS, EFING, 2013, p. 347)

No caso da Lei do Marco Civil da Internet, ela prevê

Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa:

I - advertência, com indicação de prazo para adoção de medidas corretivas;

II - multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;

III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou

IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11.

Parágrafo único. Tratando-se de empresa estrangeira, responde solidariamente pelo pagamento da multa de que trata o **caput** sua filial, sucursal, escritório ou estabelecimento situado no País.

O Projeto de Lei nº 5.344/2013 prevê em seu artigo 4, § 1º que a guarda das informações e sigilo é de obrigação da empresa contratada que deve adotar meios de manter a informação em segurança, evitando perdas.

Entretanto, esse dispositivo se assemelha em muito ao depósito, previsto pelo Código Civil de 2002, esse que dispõe que caso o depositário não adote medidas mínimas para salvaguar sua atividade empresarial, ele deve responder pelo dano causado.

Assim, pode-se utilizar do Código Civil para que o prestador do serviço em nuvem tenha *backups* das informações para prevenir eventuais danos, ou responsabilizá-lo por falhas enquanto não há uma legislação própria.

6 SOLUÇÃO DE CONTROVÉRSIAS NOS CONTRATOS

Não são apenas as questões relativas à segurança e a privacidade e as responsabilidades que podem gerar controvérsias em um contrato de prestação de serviço.

Muitos são os casos que podem ocorrer controvérsias e, como dito anteriormente, pode-se utilizar de várias ferramentas jurídicas nesses casos.

O Código de Defesa do Consumidor é uma dessas ferramentas, pois busca equilibrar as relações de consumo, que no caso dos contratos de informática podem ser: contrato de compra e venda de *software* (sob encomenda ou não); contrato de compra e venda de *hardware* (peças ou equipamentos); contrato de assistência técnica ou contrato de prestação de serviços. (PAESANI, 2014, p. 83).

Assim, no caso de Computação em Nuvem especificamente, é um contrato de prestação de serviços, onde há os princípios normativos desse Código que devem ser

observados, tais como o dever de informar (relacionado com a finalidade ou adequação do serviço e riscos decorrentes), limitação da autonomia das partes, proibição das cláusulas abusivas e proteção legal contra os vícios e defeitos dos serviços.

Com relação ao vício ou defeito de um serviço de Computação em Nuvem, como dito, deve ser detalhado ao máximo o contrato de prestação de serviço para que não ocorra dúvidas quanto ao serviço que deve ser prestado, assim, ocorrendo falhas, busca-se no contrato se essas eram previamente “aceitáveis”.

A Lei do Marco Civil da Internet estabelece

Art. 8º A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet.

Parágrafo único. São nulas de pleno direito as cláusulas contratuais que violem o disposto no **caput**, tais como aquelas que:

I - impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela internet; ou

II - em contrato de adesão, não ofereçam como alternativa ao contratante a adoção do foro brasileiro para solução de controvérsias decorrentes de serviços prestados no Brasil.

Assim, assegura-se ao usuário brasileiro desses serviços que ele tenha a possibilidade de ter seus direitos garantidos mediante a Lei Brasileira, mesmo no caso de um *data center* localizado em outro país.

O Projeto de Lei 5.344/2013 prevê em seu artigo 12º que o prestador de serviço não seria responsável pelos casos de força maior, devendo assim prova-los. Tal artigo é amparado pelo já disposto no Código Civil referente ao depositário.

Segundo Paesani (2014, p. 87) nos Estados Unidos, segundo o “*The International Computer Lawyer*, as cláusulas que exoneram o produtor da responsabilidade por vício ou dano são admitidas de uma forma geral pelo *Uniform Commercial Code* (UCC)”. No entanto, segundo a autora, esse mesmo Código permite ao juiz americano “negar eficácia às cláusulas abusivas que resultem injustamente desfavoráveis a uma das partes”.

Outro fator importante que deve-se atentar é que muitas vezes os contratos já estipulam como foro para solução de conflitos o local onde está hospedada a empresa prestadora de serviço, que em muitos casos é em outro país, ou a arbitragem internacional. Assim, é necessário conhecer os riscos quanto aos vícios e defeitos desse contrato antes de adquirir o serviço, pois a solução de uma controvérsia pode muitas vezes ser mais cara para a empresa, ou para a pessoa física, do que a solução que o serviço previamente propunha.

Portanto, vários são os fatores a serem observados quando da celebração de um contrato de serviço de *Cloud Computing*, principalmente se esses remetem a leis diferentes das brasileiras.

CONCLUSÃO

Para aqueles que estão incluídos nesta era digital, a tecnologia da informação trouxe mudanças radicais nas estruturas intra e interorganizacionais e, evidentemente, nas transações, negócios, contratos, compras e todo o tipo de transação envolvendo as relações humanas no universo cibernético.

Contudo nosso ordenamento jurídico não acompanhou com a mesma velocidade os avanços tecnológicos ocorridos no ambiente digital. Sim, há leis, mas quando nos deparamos com certas situações sabemos que, embora essas possam alcançar o direito digital, estas, quando aplicadas, o serão por analogia, pela hermenêutica, por comparações com leis estrangeiras, entre outras hipóteses.

No consoante aos contratos desse novo tipo de tecnologia, é importante levar em conta vários aspectos, como os tratos ao longo do trabalho. Quando considera-se a contratação de um serviço como SaaS, PaaS e IaaS deve sempre pensar em onde estão os *data centers* (isso determinará a lei a ser utilizada no caso de um problema), qual a segurança, como é a privacidade, e quais as responsabilidades do provedor do serviço. O contrato, mesmo que “Li e Aceito os Termos” é muito importante ser lido e não apenas “clicado” sem ler para que se use rapidamente o serviço oferecido.

Outro fator importante é quanto à solução de controvérsias, exemplificadas quando tratadas da jurisdição, da privacidade e da segurança e da responsabilidade, que ganha um capítulo a parte para tratar dos vícios e defeitos relativos aos contratos. Nesse caso, a legislação brasileira, em especial o Código de Defesa do Consumidor, deve ser usada para resguardar a relação de consumo.

Apesar de tudo que foi demonstrado ainda caminha-se no Brasil à passos lentos no tocante à uma legislação que abarca toda essa nova realidade, apesar dos Projetos de Leis que tramitam no Senado e na Câmara dos Deputados e a recente aprovação da Lei sobre o Marco Civil da Internet. Ainda resta ao Poder Judiciário cumprir a lacuna existente com as leis já existente de forma a suprir tal deficiência.

Enquanto os mecanismos tecnológicos estão, cada vez mais, disparando em velocidade assustadora, estão, também, se desenvolvendo as ocorrências no mundo cibernético, as quais reclamam por uma regulamentação apropriada.

Desta maneira cabe a nós – operadores do direito – criarmos e darmos ênfase a discussão para que ela ganhe, dentro do âmbito jurídico, o enfoque dado em outras áreas.

REFERÊNCIAS

ALBUQUERQUE, Rafael B.; BARROS, Davi S.; FERREIRA, Anderson V. A. Serviços em Nuvem: Oportunidade para Operadoras – Parte II. Teleco. Publicado em Setembro de 2013. Disponível em: < http://www.fitec.org.br/site/wpcontent/artigos/Servicos_em_Nuvem_Oportunidade_para_Operadoras-Parte_II.pdf>. Acesso em: 03 de abril de 2014.

AMARAL, Antonio Carlos Rodrigues do. Direito do Comércio Internacional: aspectos fundamentais. São Paulo: Aduaneiras, 2004

ARMBRUST, Michael. FOX, Armando, GRIFFITH, Rean [e etc.]. A View of Cloud Computing. Communication of the ACM. April 2010. Vol. 53. N. 4. P. 50-58.

BRASIL. Câmara dos Deputados. Projeto de Lei 5.344/2013. Disponível em: < <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=570970>>. Acesso em: 03 de abril de 2014.

_____. Câmara dos Deputados. Projeto de Lei Complementar 171/2012. Disponível em: < <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=543746>>. Acesso em: 07 de abril de 2014.

_____. Código Civil. 10 de janeiro de 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm>. Acesso em: 05 de abril de 2014.

_____. Código de Defesa do Consumidor. 11 de setembro de 1990. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/18078.htm>. Acesso em: 05 de abril de 2014.

_____. Lei nº 12.965, de 23 de abril de 2014. Lei do Marco Civil da Internet.

CORRÊA, Gustavo Testa. Aspectos Jurídicos da Internet. São Paulo: Saraiva, 2000.

GARCIA JÚNIOR, Armando Alvares. Contratos via Internet. São Paulo: Aduaneiras, 2001.

GLANZ, Semy. Internet e Contrato Eletrônico. In: Revista dos Tribunais, vol. 757, nov. 1998.

GONZALES, Nelson M.; MIERS, Charles C.; REDÍGOLO, Fernando F.; ROJAS, Marco Antônio T.; CARVALHO, Tereza C. M. B. Segurança das Nuvens Computacionais: Uma visão dos Principais Problemas e Soluções. Revista USP. São Paulo. N. 97. Mar/Abr/Maio 2013. P. 27-42.

IIZUKA, André Sussumu. Aspectos tributários e contratuais do cloud computing. *ConvergeCom*. Nov. 2012. Disponível em: <<http://convergecom.com.br/tiinside/12/11/2012/aspectos-tributarios-e-contratuais-do-cloud-computing/#.Uzy1u6hdV6E>>. Acesso em: 03 de abril de 2014.

MARCON JR., Arlindo; LAUREANO, Marcos; SANTIN, Altair; MAZIERO, Carlos. Aspectos de segurança e privacidade em ambientes de Computação em Nuvem. X Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais. Minicursos. 2011. Cap. 2. P. 53-102. Disponível em: <<http://professor.ufabc.edu.br/~joao.kleinschmidt/aulas/seg2011/nuvem.pdf>>. Acesso em: 09 de abril de 2014.

MELL, Peter; GRANCE, Timothy. The NIST Definition of Cloud Computing. NIST Special Publication 800-145. U.S. Department of Commerce. National Institute of Standards and Technology. September 2011. Disponível em: <http://www.profsandhu.com/cs6393_s13/nist-SP800-145.pdf>. Acesso em: 05 de abril de 2014.

MILLER, Rich. Inside Facebook's New Lulea Data Center. *Data Center Knowledge*. June 12, 2013. Disponível em: <<http://www.datacenterknowledge.com/archives/2013/06/12/inside-facebooks-new-lulea-data-center/>>. Acesso em: 06 de abril de 2014.

PAESANI, Liliana Minardi. *Direito de Informática – Comercialização e Desenvolvimento Internacional do Software*. 9ª ed. São Paulo: Atlas, 2014.

_____. *Direito e Internet – liberdade de informação, privacidade e responsabilidade civil*. Coleção Temas Jurídicos. 3ª ed. São Paulo: Atlas, 2006.

PARCHEN, Charles E.; FREITAS, Cinthia O. A.; EFING, Antônio C. Computação em Nuvem e Aspectos Jurídicos da Segurança da Informação. *Revista Jurídica CESUMAR – Mestrado*. Vol. 13. Mar. 2013. P. 331-355.

PINHEIRO, Patricia Peck. *Direito Digital*. São Paulo: Saraiva, 2002.

_____. *Direito Digital*. 5ª ed. rev. atual. e ampliada. São Paulo: Saraiva, 2013.

SANTOS, Ana P. V.; MACHADO, Marcos. Cloud Computing: Impasses Legais e Normativos. *Revista Científica Intr@ciência*. UNIESP. Ano 2. Nº 1. Nov. 2010. P. 16-105.

SOARES, Edileuza. Conheça os riscos legais de cloud computing. *Computerworld*. Nov. 2011. Disponível em: <<http://computerworld.com.br/negocios/2011/11/17/conheca-os-riscos-legais-de-cloud-computing>>. Acesso em: 04 de abril de 2014.

STORAGE SERVERS. Dropbox uses Amazon S3 services for storage! October 25, 2013. Disponível em: <<http://storageservers.wordpress.com/2013/10/25/dropbox-uses-amazon-s3-services-for-storage/>>. Acesso em: 05 de abril de 2014.

UNIÃO EUROPÉIA. Parecer 05/2012 relativo a computação em nuvem. Adotado em 1 de julho de 2012. Disponível em: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_pt.pdf>. Acesso em: 03 de abril de 2014.