UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO DE CIÊNCIAS JURÍDICAS
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO
CURSO DE MESTRADO INTERINSTITUCIONAL UFSC/FLF

A SEGURANÇA JURÍDICA DA COMPUTAÇÃO EM NUVEM: RESPONSABILIDADE JURÍDICA NA PROTEÇÃO DE DADOS DIGITAIS POR PARTE DOS PROVEDORES DE APLICAÇÃO DE INTERNET.

FRANCISCO VICTOR VASCONCELOS

FLORIANÓPOLIS/SC
2017

Ficha de identificação da obra elaborada pelo autor, através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

VASCONCELOS, FRANCISCO VICTOR
A SEGURANÇA JURÍDICA DA COMPUTAÇÃO EM NUVEM: RESPONSABILIDADE JURÍDICA NA PROTEÇÃO DE DADOS DIGITAIS POR PARTE DOS PROVEDORES DE APLICAÇÃO DE INTERNET. / FRANCISCO VICTOR VASCONCELOS ; orientador, AIRE JOSÉ ROVER, 2017.
166 p.

Dissertação (mestrado) - Universidade Federal de Santa Catarina, Centro de Ciências Jurídicas, Programa de Pós-Graduação em Direito, Florianópolis, 2017.

Inclui referências.

1. Direito. 2. SEGURANÇA JURÍDICA. 3. COMPUTAÇÃO EM NUVEM. 4. RESPONSABILIDADE JURÍDICA. 5. MARCO CIVIL DA INTERNET. I. ROVER, AIRE JOSÉ. II. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Direito. III. Título.

Francisco Victor Vasconcelos

A SEGURANÇA JURÍDICA DA COMPUTAÇÃO EM NUVEM: RESPONSABILIDADE JURÍDICA NA PROTEÇÃO DE DADOS DIGITAIS POR PARTE DOS PROVEDORES DE APLICAÇÃO DE INTERNET.

Dissertação submetida ao Programa de Pós-Graduação em Direito da Universidade Federal de Santa Catarina, como requisito parcial para a obtenção do título de Mestre em Direito. Orientador: Prof. Dr. Aires José Rover.

FLORIANÓPOLIS/SC
2017

Francisco Victor Vasconcelos

A SEGURANÇA JURÍDICA DA COMPUTAÇÃO EM NUVEM: RESPONSABILIDADE JURÍDICA NA PROTEÇÃO DE DADOS DIGITAIS POR PARTE DOS PROVEDORES DE APLICAÇÃO DE INTERNET.

Esta dissertação foi julgada adequada para a obtenção do título de Mestre em Direito e aprovada em sua forma final pelo Programa de Pós-Graduação em Direito da Universidade Federal de Santa Catarina, na área de concentração "Direito, Estado e Sociedade", e linha de pesquisa "Direito da Sociedade da Informação e Propriedade Intelectual".

Florianópolis/SC, 06 de novembro de 2017.

_____

Prof. Arno Dal Ri Jr., PhD.
Coordenador do PPDG

Banca examinadora:

_____

Prof. Aires José Rover, Dr.
Orientador
Universidade Federal de Santa Catarina – UFSC

_____

Prof. Carlos Araújo Leonetti, Dr.
Examinador
Universidade Federal de Santa Catarina – UFSC

_____

Profª. Renata Albuquerque Lima, Dra.
Examinador
Faculdade Luciano Feijão – FLF

AGRADECIMENTOS

Dedico este árduo trabalho às pessoas que me são muito especiais, sem as quais eu não teria alcançado meus objetivos pessoal, profissional e, neste momento, acadêmico. A importância de cada uma reside em sentimento de amor, amizade e cumplicidade de forma mútua e pura. Em todo o processo de estudo, pesquisa e escrita desta obra, tive a inspiração, oriunda da torcida destas diletas e especiais pessoas. Agradeço:

À minha amada, amiga, confidente, cúmplice e esposa, Izabella Tamira, que, numa forma peculiar e corajosa, lutou ao meu lado a mais difícil das batalhas até agora por nós dois travada. Meu amor, você me trouxe um novo significado de amor, paixão e família. Agradeço a você por todo o apoio, carinho, paixão em todo este processo de crescimento que tivemos como família.

Aos meus pais, Francisco Ivo de Vasconcelos e Maria do Patrocínio de Vasconcelos, os quais, sempre demonstrando seu amor e ensinamentos, mostraram-me a realidade da vida e fizeram o melhor para a minha formação acadêmico-profissional.

Às minhas irmãs Vanessa de Vasconcelos, Raphaella de Vasconcelos e seus maridos, hoje, meus irmãos, Herbet Cunha e David Cassio, dedico-lhes toda minha admiração, respeito e fraternidade, pois com vocês amadureci muito nestes últimos anos de minha vida.

Aos meus sogros, Antonio Isael de Farias e Gorete Galdino, deixo-lhes toda a minha admiração pelo exemplo de casal que são para mim e Izabella.

Agradeço, ainda, a todos os meus professores que contribuíram para a minha formação acadêmica, em destaque aos mestres deste curso de Pós-Graduação em Direito, que, de forma muito carinhosa, ensinaram-se as profundidades científicas do Direito, o que aumentou a sede de ensino. Dentre estes grandes professores, agradeço especialmente ao meu orientador Prof. Dr. Aires José Rover, que, na sua paciência, ensinou-me a melhor maneira de produzir esta dissertação, bem como ao Prof. Dr. Arno Dal Ri Jr que ajudou na perpetuação deste sonho pessoal, que ora finalizo.

Às professoras Dra. Renata Albuquerque e Isabel Pontes, respectivamente coordenadora do curso de Direito e diretora geral da Faculdade Luciano Feijão, pelo zelo esforço hercúleo em tornar realidade o curso de mestrado interinstitucional em Direito.

Ao professor Luciano Feijão, chanceler da instituição homônima, da qual muito feliz e honrosamente integro o quadro como professor, pelo

espírito visionário de compreender que a educação assume posição central no propósito transformador da realidade social para melhor.

Aos professores doutores Arno Dal Ri Jr., Carlos Araújo Leonetti, Renata Albuquerque Lima, pela disponibilidade de examinar o trabalho, participando ativamente desta importante etapa de minha vida acadêmica.

Agradeço ainda a todos os meus amigos e alunos que, apesar de não terem participado diretamente na execução da pesquisa, torceram e incentivaram neste momento.

Por fim, e não menos importante, louvo a Deus pela força e iluminação durante todos os momentos de minha vida.

Eu não troco a justiça pela soberba. Eu não deixo o direito pela força. Eu não esqueço a fraternidade pela tolerância. Eu não substituo a fé pela superstição, a realidade pelo ídolo.

Rui Barbosa

RESUMO

O presente trabalho tem como finalidade geral proporcionar a verificação de solução jurisdicional eficiente sob o enfoque do usuário, dentro do ordenamento jurídico nacional para a responsabilização jurídica de provedores de aplicação de Internet, em sua maioria estrangeiros, que oferecem serviços de Computação em Nuvem, em razão de danos ocasionados pela quebra da lisura e da segurança dos dados digitais sob sua proteção. O pesquisador utilizou uma abordagem metodológica dedutiva, através de método monográfico e dividiu o trabalho em quatro capítulos. No primeiro, há um esmiuçamento do conceito, características e aplicabilidade da Computação em Nuvem, como um tecnologia atual, perpassando por seus modelos de implantação, vantagens e desvantagens da adoção. Por conseguinte, inicia um estudo aprofundado sobre os principais aspectos jurídicos da Internet, como uma ferramenta de interação social e econômica. Na terça parte do trabalho, o autor apresentou os principais aspectos da legislação brasileira sobre uso da Internet, sob o prisma da computação em nuvem. Neste momento, discutiu assunto como a neutralidade da rede insculpida nos artigos 3º e 9º da Lei 12.965/2014 e tributação dos serviços de nuvem computacional. O estudo investiga e analisa a informação na era digital como um bem econômico, objetivando apontar os motivos que contribuem para a sua expropriação. Por fim, no quarto e último capítulo, o estudo aborda a responsabilização jurídica dos provedores de aplicação de Internet, que ofereçam serviços em Computação em Nuvem, apontando a aplicabilidade da legislação nacional e estrangeira na ocorrência de falha na prestação do serviço, através dos elementos de conexão estipulados pela Lei de Introdução às Normas do Direito Brasileiro.

Palavras-chave: Segurança Jurídica. *Computação em Nuvem*. Internet. Marco Civil da Internet. Responsabilidade Jurídica. Elementos de conexão. LINDB.

ABSTRACT

The present work has the general purpose of providing the verification of efficient jurisdictional solution under the user's approach, within the national legal framework for the legal accountability of Internet application providers, mostly foreign, who offer Cloud Computing services in damage caused by the breach of fairness and the security of digital data under its protection. The researcher used a deductive methodological approach, using a monographic method and divided the work into four chapters. In the first one, there is a breakdown of the concept, characteristics and applicability of Cloud Computing, as a current technology, going through its implantation models, advantages and disadvantages of the adoption. Therefore, it initiates an in-depth study on the main legal aspects of the Internet, as a tool of social and economic interaction. In the third part of the paper, the author presented the main aspects of the Brazilian legislation on Internet use, under the prism of cloud computing. At the moment, he discussed the net neutrality of articles 3 and 9 of Law 12.965 / 2014 and taxation of cloud computing services. The study investigates and analyzes the information in the digital era as an economic good, aiming at pointing out the reasons that contribute to its expropriation. Finally, in the fourth and last chapter, the study addresses the legal accountability of Internet application providers offering services in Cloud Computing, pointing out the applicability of national and foreign legislation in the occurrence of failure to provide the service through the elements stipulated by the Law of Introduction to the Norms of Brazilian Law.

Keywords: Legal Security. Cloud computing. Internet. Civil Landmark of the Internet. Legal responsibility. Connecting elements. LINDB.

SUMÁRIO

INTRODUÇÃO

Hoje, a Internet, rede mundial de computadores, é a principal forma de transmissão de informação pelo mundo, mantém bilhões de pessoas conectadas entre si, por meio de dispositivos eletrônicos inteligentes. Esta interligação proporcionada pela Internet não se restringe somente às pessoas, mas também entre estas e seus bens jurídicos, uma vez que a informação possui um valor imensurável na sociedade de informação.

A rede mundial de computadores trouxe grandes e variados benefícios para seus usuários, quais passaram a produzir novas ideias, produtos e serviços, consolidando, assim, novas formas de relacionamento, de comércio, de negócios e, até mesmo, de governos.

Destarte, a Internet firmou a existência da sociedade tecnológica, oriunda da Terceira Revolução Industrial ou Revolução Tecnocientífica, qual a partir da segunda metade do século XX, iniciou-se esta nova fase de processos tecnológicos, decorrentes de uma integração física entre ciência e produção.

A sociedade tecnológica é caracterizada pelo imediatismo e pela quebra das barreiras geográficas na transmissão da informação, porque busca, por meio da Internet, uma fluidez imediata de informação, oriunda de diversas fontes nacionais ou internacionais. As características da sociedade tecnológica só são possíveis por causa da constante inovação na tecnologia de informação de *hardware* (componentes concretos da máquina) e de *software* (programas).

No mundo, o processo evolutivo da *Internet* não se deu uniformemente entre os países, em virtude de diversas variáveis, como cultura, economia, religião. Até mesmo, em plena metade da segunda década do Século XXI, há países, como Irã e Coreia do Norte, que controlam a utilização da Internet por parte de seus habitantes. Outros países, por fatores econômicos, não possuem meios de disseminar a utilização da rede mundial de computadores entre sua população.

Outra consequência advinda da Internet é a internacionalização de relações jurídicas interpessoais, posto que se permita a comunicação imediata e instantânea entre pessoas, localizadas em partes diferentes do mundo, quais poderão firmar avenças entre si.

Esta internacionalização permitiu que a liberdade, quase anárquica, do ciberespaço, pois se projeta uma cibersociedade mutuamente sustentada em princípios éticos e morais culturalmente divergentes entre si. Essa “anarquia” facilitaria as relações entre os membros do ciberespaço e constituiria micronações e culturas

engendradas dentro desse espaço, como é o caso dos *hackers*, *crackers*, *geeks*, por exemplo.

A internacionalização não se restringe somente a relação entre pessoas, mas também, no liame jurídico entre as pessoas e seus bens jurídicos, pois os dados digitais que contém informações importantes são objetos juridicamente relevantes. Por exemplo: o indivíduo registra fotograficamente com sua câmera digital o momento em que seu tenro filho começa a dar os primeiros passos e salva este arquivo em um servidor situado em país diverso. Os dados informáticos constantes no servidor têm o mesmo valor jurídico, que o registro fotográfico impresso e guardado em um cofre de um banco local.

Com o escopo de aumentar a mobilidade e a independência da interligação entre o indivíduo e seus dados digitais, criou-se o sistema de computação em nuvem (do inglês *clouding computing*), pois é uma ferramenta-meio para o acesso de dados digitais armazenados em servidores, através de qualquer dispositivo inteligente, como *notebook's, ultrabook's, tablet's, smartphone's* etc. Deste modo, a computação em nuvem se propõe a delegar a tarefa de armazenamento e gerenciamento de dados de seus usuários a terceiros em servidores localizados em pontos diversos do globo.

Então, é possível a indagação: Como será garantida a lisura, a higidez e, sobretudo, a segurança da informação depositada em sistema de nuvem computacional? Em casos de falhas na segurança dos dados, como proceder a tutela dos direitos dos usuários/consumidores do serviço, haja vista a insuficiente legislação acerca da Internet?

O Direito, em apertada síntese, é o conjunto de normas imposta pelo Estado, Democrático ou não, com a finalidade de regular o convívio pacífico entre as pessoas em seu território, atribuindo-se um valor normativo a cada fato social relevante. Com base no conceito básico de Direito, podemos destacar que o ordenamento jurídico de um Estado não subjuga a de outro. Entretanto, a paz social mantida entre os entes internacionais deve ser mantida através de tratados e convenções internacionais, que são criadas para alinhavar os parâmetros legislativos, em razão de um interesse comum internacional.

Numa visão teleológica, é possível afirmar que a Internet permite que seus usuários participem igualmente de possíveis discussões dentro de um espaço democrático de direito. Para Rover (2012, p.3):

> Embora o processo democrático contemporâneo se apresente como um sistema teleológico, de cima para baixo, onde as formas de exercício da

> cidadania estão definidas nos limites da Constituição Federal, a internet, por sua vez, surge como um sistema emergente, de baixo para cima, um ambiente democrático e descentralizado que permite a participação direta de todos os que estiverem conectados e interessados em participar da política e ajudar a construir esta nova sociedade em rede.

Há vários tratados e convenções internacionais, mas, para a presente pesquisa, destaca-se a Convenção de Budapeste que tipifica os principais crimes cometidos na Internet. Foi criada em 2001, na Húngria, pelo Conselho da Europa e está em vigor desde 2004, englobando atualmente mais de vinte países. Este documento prioriza uma política criminal comum, com o objetivo de proteger a sociedade contra a criminalidade no ciberespaço, designadamente, através da adoção de legislação adequada e da melhoria da cooperação internacional e reconhece a necessidade de uma cooperação entre os Estados e a indústria privada. Por conseguinte, destaca como obrigatório o respeito à Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais do Conselho da Europa (1950); ao Pacto Internacional sobre os Direitos Civis e Políticos da ONU (1966); à Convenção das Nações Unidas sobre os Direitos da Criança (1989); e à Convenção da Organização Internacional do Trabalho sobre as Piores Formas do Trabalho Infantil (1999).

Infelizmente, o Brasil não foi signatário da Convenção de Budapeste. Aliás, frente a ampla generalidade da substância legal, os legisladores pátrios não consideravam a necessidade da regulamentação da Internet, até a criação da Lei nº. 12.965/2014, conhecida como Marco Civil da Internet.

No Brasil, o tema deste trabalho é pouco investigado, tanto pela ausência de legislação pertinente ao tema, quanto pela complexidade que a envolve, uma vez que se deve analisar a proteção jurídica de dados digitais sob a ótica da legislação nacional, bem como da legislação alienígena.

A Lei nº. 12.965/2014 não traz especificamente a proteção da lisura dos dados armazenados em nuvem computacional, porém a norma do artigo 11 da Lei nº. 12.965/2014[1] tem como finalidade a proteção dos

[1] Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e

dados digitais se as operações de informáticas forem atribuídas a um dispositivo localizado no Brasil. Infelizmente, esta norma não é suficientemente coerente, haja vista a internacionalização da Internet, limitando a utilização do usuário ao território nacional.

A relevância jurídica deste tema surgiu de questionamentos acerca da responsabilização jurídica de provedores de computação em nuvem, em sua maioria situados em outros países, por falhas da segurança de dados digitais armazenados em nuvem computacional, tendo em vista que o Estado brasileiro não faz parte da Convenção de Budapeste e possui parca legislação sobre o ciberespaço. Esta vulnerabilidade jurídica deve ser sanada por nosso Poder Judiciário, haja vista a possibilidade de invocação da lei estrangeira, nos termos do artigo 14 da Lei de Introdução ao Código Civil: "Não conhecendo a lei estrangeira, poderá o juiz exigir de quem a invoca prova do texto e da vigência." (BRASIL. Decreto-Lei Nº 4.657, de 4 de setembro de 1942)

Por outro lado, não poderá o magistrado nacional invocar de ofício a lei estrangeira, cabendo ao usuário prejudicado manifestar-se espontaneamente, pois a aplicabilidade da norma alienígena dependerá da sua vigência no Estado de origem, devendo, ainda, o juiz interpretá-la em conformidade com regras de interpretação do direito estrangeiro invocado.

---

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.

§1º O disposto no caput aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.

§2º O disposto no caput aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.

§3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.

§4º Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo.

Conforme o dispositivo legal apontado, podemos inferir que o usuário brasileiro somente poderá buscar sua tutela após o seu dispositivo chegar a território nacional. Então, se o seu dispositivo móvel nunca chegar ao Brasil, por qualquer motivo alheio a sua vontade, nunca poderá o brasileiro obter tutela de proteção judicial, haja vista a corrupção dos dados armazenados, pois o terminal que enviara os dados não está localizado no território nacional.

A problemática central da Computação em Nuvem reside sobre sua segurança e confiabilidade. Arlindo Marcon Jr. (2010, p.55), em seu estudo intitulado "Aspectos de segurança e privacidade em ambientes de Computação em Nuvem" afirma que o "esquema de segurança computacional necessita preservar as propriedades básicas: confidencialidade, integridade, disponibilidade, autenticidade e não repúdio."

Inobstante, todo a sistema de segurança proporcionado pelo servidor ao oferecer o serviço de armazenamento em nuvem computacional, não pode o usuário ser submetido a este produto sem garantias mínimas, seja legal ou contratual. Deve haver por parte do usuário, um grau elevado de maturidade e preparo no que tange ao correto e consciente uso da mencionada tecnologia.

No Brasil, como já explanado, a legislação não acompanhou devidamente a evolução da Internet e de suas implicações sociais, restando ao legislador produzir normas sem muita eficácia, quais, consequentemente, imporão à jurisprudência o mister de solver as lacunas legislativas, atribuindo ao usuário prejudicado a melhor tutela que lhe for possível, sem se restringir à aplicação exclusiva da Lei nº. 12.965/2014. A restrição à aplicação do Marco Civil da Internet causa muitas intempéries ao usuário prejudicado, bem como dificulta uma razoável reprimenda judicial pelos danos ocasionados em razão da falha na segurança computacional. Deve o magistrado, invocando as regras de direito internacional, aplicar no que couber a legislação alienígena, no qual se insere o servidor causador do dano.

Aparentemente, a aplicação da lei estrangeira por juiz nacional poderia ferir a soberania nacional, pois um magistrado estaria reconhecendo a competência legal de legislador estrangeiro como produtor de norma jurídica. Todavia, não há qualquer ferimento a soberania nacional, pois o juiz, ao buscar a aplicabilidade da norma internacional, deverá aplicar o direito estrangeiro interpretando-o na conformidade das regras de interpretação de nosso ordenamento jurídico.

Com efeito, a Lei de Introdução às Normas do Direito Brasileiro (LINDB) previu, em seu artigo 14, que o magistrado poderá utilizar-se da

lei estrangeira, cabendo a quem lhe invoca o ônus de comprovar sua vigência e integridade textual. Desta forma, em razão da fragilidade legislativa nacional acerca da segurança jurídica no ambiente digital, o magistrado poderá utilizar-se da legislação estrangeira, com escopo de proporcionar um julgamento eficaz na tutela dos direitos dos usuários de serviços de computação em nuvem.

CAPÍTULO 1 – SISTEMA DE COMPUTAÇÃO EM NUVEM

Evolutivamente, a capacidade do homem de calcular quantidades dos mais variados modos foi um dos fatores que possibilitaram o desenvolvimento da matemática, da lógica e consequentemente da computação. Nos primórdios da matemática e da álgebra, utilizavam-se os dedos das mãos para efetuar cálculos. A mais antiga ferramenta conhecida para uso em computação foi o ábaco, e foi inventado na Babilônia por volta de 2400 a.C. O ábaco dos romanos, por sua vez, consistia de bolinhas de mármore que deslizavam numa placa de bronze cheia de sulcos.

Cléuzio Fonseca Filho (2007), em sua obra "História da Computação: O Caminho do Pensamento e da Tecnologia" afirma que a primeira máquina capaz de somar, subtrair, multiplicar e dividir foi construída por Wilhelm Schickard (1592-1635). Todavia, durante muitos anos nada se soube sobre essa máquina, por isso, atribuía-se a Blaise Pascal (1623-1662) a construção da primeira máquina calculadora, que fazia apenas somas e subtrações. Esta calculadora usava engrenagens que a faziam funcionar de maneira similar a um odômetro. A máquina Pascal foi criada com objetivo de ajudar seu pai a computar os impostos em Rouen, França.

No Século XIX, o francês, Charles Xavier Thomas, conhecido como Thomas de Colmar, projetou e construiu uma máquina capaz de efetuar as 4 operações aritméticas básicas: a Arithmomet. Esta foi a primeira calculadora realmente comercializada com sucesso. Ela fazia multiplicações com o mesmo princípio da calculadora de Leibniz e efetuava as divisões com a assistência do usuário. Apesar da capacidade de calcular, todas essas máquinas estavam longe de serem consideradas um computador, uma vez que lhes faltavam programação.

Conforme Fonseca Filho (2007), a era da computação nasceu quando o homem procurou ultrapassar os limites práticos da aritmética. A ideia de uma programação surgiu nos anos 1830 com inglês Charles Babbage, um século antes do período tradicionalmente atribuído ao nascimento do computador. O primeiro computador eletromecânico foi construído por Konrad Zuse (1910-1995). Em 1936, esse engenheiro alemão construiu, a partir de relés que executavam os cálculos e dados lidos em fitas perfuradas, o Z1.

Posteriormente, os computadores eletrônicos modernos que surgiram durante a Segunda Guerra Mundial, como o ENIAC (Eletronic Numeric Integrator And Calculator) criado pelo Exército americano, deram origem à noção de um computador universal, que seria uma

máquina capaz de processar qualquer tipo de informação, inclusive manipular os próprios programas. Esses são os computadores que movem o mundo atual. E embora pareça que a tecnologia da computação tenha amadurecido a ponto de se tornar onipresente e aparentemente ilimitada, pesquisadores buscam inspiração na mente, em sistemas biológicos e na física quântica para criar tipos completamente novos de máquinas cada vez mais potentes.

O constante avanço tecnológico da sociedade humana moderna proporcionou a efetivação de uma entrega transparente de serviços básicos e essenciais de utilidade pública como água, eletricidade, telefone e gás, os quais se tornaram fundamentais para nossa vida diária e são explorados por meio do modelo de pagamento baseado no uso e suas infraestruturas desenvolvidas permitem entregá-los em qualquer lugar e a qualquer hora, de forma que possamos simplesmente acender a luz, abrir a torneira ou usar o fogão. Seu uso é, então, cobrado de acordo com as diferentes políticas de tarifação para o usuário final.

Recentemente, a mesma ideia de utilidade e essencialidade tem sido aplicada no contexto da informática, através do *Cloud Computing* ou Computação em Nuvem. Esta nova ideia é uma tendência tecnológica cujo objetivo é proporcionar serviços de Tecnologia da Informação (TI) sob demanda com pagamento baseado no uso.

Aymerich et al. (2008) afirmam que a expressão "computação em nuvem" foi empregada pela primeira vez em 2006 pelo *Chief Executive Officer*, CEO do *Google*, Eric Schmidt, para referenciar a computação empregando os recursos da Internet. De fato, não há registro na literatura acadêmica desta expressão antes de 2006. Assim, sendo ou não Schmidt o responsável por cunhar a expressão, de fato é que ela parece não ter sido referenciada em período anterior.

A Computação em Nuvem pretende alcançar índices globais e proporcionar serviços, que atingem desde o usuário final que armazena seus arquivos pessoais na Internet até empresas que terceirizam toda infraestrutura de Tecnologia da Informação (TI) para outras. Com isso, os usuários estão movendo seus dados e aplicações para a nuvem computacional e assim acessá-los de forma simples e de qualquer local.

Em geral, os recursos físicos de computação são propensos a obsolescência rapidamente e a utilização de plataformas computacionais de terceiros é uma solução inteligente para os usuários lidarem com esta problemática, uma vez que não despenderão de recursos financeiros constantemente para a aquisição de novos *hardwares*, com a finalidade de acompanhar a evolução das novas tecnologias.

A Computação em Nuvem, dentre várias vantagens, sobre a computação tradicional, oferece ao usuário serviços "gratuitos", livres para uso, gerando economia em aquisições de *hardware, software* e outros serviços. O armazenamento de dados fica a cargo do provedor, responsável pela aquisição e manutenção da estrutura necessária à operação da nuvem computacional. Para Cesar Taurion (2009, p. 3):

> As pequenas empresas, em particular, estão recorrendo a estes serviços para fugir da dor de cabeça que é manter seus próprios *data centers*. Como a empresa não paga por recursos desnecessários e nem tem gastos com os espaços físicos e de infraestrutura do *data center*, como energia e refrigeração, ela tem gastos menores com sua operação de TI e pode repassar esta eficiência operacional aos seus clientes, tornando-se mais competitiva no mercado.

Na Computação em Nuvem, os recursos tecnológicos são fornecidos como um serviço, permitindo aos usuários o acesso sem a necessidade de conhecimento sobre a tecnologia utilizada. Assim, os usuários e as empresas passaram a acessar os serviços sob demanda independentemente de localização, o que aumentou a quantidade de serviços disponíveis. Para utilizarem os serviços, os usuários necessitam minimamente ter em suas máquinas um sistema operacional, um navegador e acesso à Internet. Todos os recursos computacionais estão disponíveis na nuvem e as máquinas dos usuários não necessitam ter altos recursos computacionais, diminuindo o custo na aquisição de máquinas.

1.1 Conceito, características e modelos da Computação em Nuvem

Em um conceito técnico informacional, os computadores são dispositivos eletrônicos que executam operações lógicas e matemáticas a partir de uma sequência de instruções gravadas como sinais elétricos em substrato semicondutor, usualmente denominado *RAM*, do inglês *Random Access Memory*. A unidade básica de armazenamento é um *bit*, um sinal elétrico que varia 0 Volts, significando o valor binário 0, a 5 Volts, significando o valor binário 1. Cada instrução é uma sequência de bits (4, 8, 16, 32, 64 ou mais bits) cada qual com um significado específico, que são lidas, entendidas e executadas pela *CPU*, *Central Processing Unit*.

O conjunto das diferentes instruções inteligíveis e executáveis pela *CPU* é denominado linguagem de máquina. O conjunto dos subsistemas

construídos em semicondutores que auxiliam e possibilitam o funcionamento da *CPU* é chamado de microprocessador ou simplesmente processador. Uma sequência de instruções concebida por um programador é denominada código-executável. Só existe uma linguagem de máquina para um certo tipo de processador, mas podem existir vários códigos executáveis, concebidos por diferentes programadores, para um certo tipo de processador. Estes códigos executáveis serão executados da mesma maneira pelos diversos exemplares do dito processador.

O *hardware* é um equipamento ou dispositivo que, embora mais complexo, é semelhante a outros dispositivos eletrônicos, com a diferença principal de ser inteiramente dependente do software para cumprir algum papel, cuja natureza jurídica é de bem móvel fungível, conforme disposto no Código Civil, Art. 82[2] e Art. 85[3].

O *software,* por sua vez, é algo intangível, consubstanciado numa sequência de zeros e uns, armazenada na memória RAM do *hardware* e por este executada. No Brasil, a Lei 9.609/98 dispõe sobre a proteção da propriedade intelectual de programa de computador e define o *software* como um propriedade intelectual protegida por direito de autor:

> Art. 1º Programa de computador é a expressão de um conjunto organizado de instruções em linguagem natural ou codificada, contida em suporte físico de qualquer natureza, de emprego necessário em máquinas automáticas de tratamento da informação, dispositivos, instrumentos ou equipamentos periféricos, baseados em técnica digital ou análoga, para fazê-los funcionar de modo e para fins determinados.
>
> Art. 2º O regime de proteção à propriedade intelectual de programa de computador é o conferido às obras literárias pela legislação de direitos autorais e conexos vigentes no País, observado o disposto nesta Lei.

[2] Art. 82. São móveis os bens suscetíveis de movimento próprio, ou de remoção por força alheia, sem alteração da substância ou da destinação econômico-social.

[3] Art. 85. São fungíveis os móveis que podem substituir-se por outros da mesma espécie, qualidade e quantidade.

Por sua vez, a nuvem é uma metáfora para a Internet ou infraestrutura de comunicação entre os componentes tecnológicos. Cada parte desta infraestrutura é provida como um serviço e, estes são normalmente alocados em Centros de Dados (*Data Center*), utilizando hardware compartilhado interligado pela rede mundial.

É adequado mencionar a definição proposta pelo *National Institute of Standards and Technology* (NIST), entidade federal americana não regulatória vinculada ao Departamento de Comércio do Governo dos Estados Unidos e responsável por promover a inovação e a competitividade industriais em âmbito nacional naquele país. Para o NIST (2009):

> Computação em nuvem é um modelo que viabiliza o acesso oportuno e sob demanda a um pacote compartilhável de recursos computacionais configuráveis (por exemplo, redes, servidores, áreas para armazenagem, aplicativos e serviços) que podem ser rapidamente provisionados e liberados com um esforço mínimo de gestão ou de interação com o provedor dos serviços.[4]

Pelo conceito acima exposto, a computação em nuvem é um modelo computacional que serve para criar um acesso irrestrito a serviços baseados em rede de computadores (de preferência a rede mundial) que servem a possibilitar ao seu usuário, rápido e fácil uso de suas aplicações, que podem ser desde servidores de armazenamento de dados, passando por aplicações (softwares) e serviços.

A *Cloud Security Alliance*[5] assevera que:

> Computação em nuvem ("Nuvem") é um termo em evolução que descreve o desenvolvimento de muitas das tecnologias e abordagens existentes em computação para algo distinto. A nuvem separa as aplicações e os recursos de informação de sua infraestrutura básica, e os mecanismos utilizados

[4] Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

[5] Organização privada norte-americana, sem fins lucrativos, que visa oferecer as melhores práticas para a segurança dentro da computação em nuvem, bem como a educação necessária para o uso desta tecnologia.

> para entregá-los. A nuvem realça a colaboração, agilidade, escalabilidade e disponibilidade, e oferece o potencial para redução de custos através de computação eficiente e otimizada. Mais especificamente, a nuvem descreve o uso de uma coleção de serviços, aplicações, informação e infraestrutura composta por pools de recursos computacionais, de rede, de informação e de armazenamento. Estes componentes podem ser rapidamente organizados, provisionados, implementados, desativados, e escalados para cima ou para baixo, provendo um modelo de alocação e consumo baseado na demanda de recursos.

Neste conceito, a computação em nuvem é a tecnologia focada na acessibilidade móvel e confortável a uma rede de recursos computacionais existentes, conforme a necessidade e o gosto do usuário, que pode ser acessada rapidamente e usada com um mínimo de interação com o provedor de serviços, permitindo a troca de informações em velocidade instantânea.

Armbrust et al. (2009) propõem a seguinte definição: “A computação em nuvem é um conjunto de serviços de rede ativados, proporcionando escalabilidade, qualidade de serviço, infraestrutura barata de computação sob demanda e que pode ser acessada de uma forma simples e pervasiva”.

1.2 Características técnicas

Para este trabalho, considerou-se a visão do NIST, que descreve que o modelo de computação em nuvem é composto por cinco características essenciais, três modelos de serviço e quatro modelos de implantação.

O modelo de Computação em Nuvem foi desenvolvido com o objetivo de fornecer serviços de fácil acesso, baixo custo e com garantias de disponibilidade e escalabilidade. Este modelo visa fornecer, basicamente, três benefícios.

O primeiro benefício é a redução do custo na aquisição e composição de toda infraestrutura requerida para atender as necessidades das empresas, podendo essa infraestrutura ser composta sob demanda e com recursos heterogêneos e de menor custo. O segundo é a flexibilidade, pois diz respeito à adição e substituição de recursos computacionais, podendo escalar tanto em nível de recursos de hardware quanto software para atender às necessidades das empresas e usuários. O último benefício é prover uma abstração e facilidade de acesso aos usuários destes serviços. Desta maneira, os usuários dos serviços não precisam conhecer profundamente os aspectos tecnológicos sobre a utilização e os resultados destes serviços.

A Computação em Nuvem é uma tecnologia baseada na Internet, necessita, para seu perfeito funcionamento, tanto de uma parte física (hardware) quanto de abstração lógica (softwares), que trabalhem em conjunto de modo a oferecer os serviços baseados neste tipo de computação.

De acordo com a NIST, a computação em nuvem possui as seguintes características:

a) Serviço sob demanda: é o consumidor que determina as capacidades dos serviços que deseja usar, de forma automática, sem necessidade, em regra, de interação humana direta com o prestador do serviço;

b) Amplo acesso à rede: os recursos disponíveis oferecidos e utilizados através da rede mundial e podem ser acessados por quaisquer meios ou mecanismos de interação tais como celulares, *tablets*, *smartphones*, *desktops*, *notebooks* e etc;

c) Armazenamento de recursos (*Pooling*): os recursos da computação em nuvem estão todos agrupados em um *pool*, alocados de forma a esperar a demanda do consumidor. Os recursos computacionais do provedor são organizados em um pool para servir múltiplos usuários usando um modelo de multi-inquilino, com diferentes recursos físicos e

virtuais, dinamicamente atribuídos e ajustados de acordo com a demanda dos usuários, que não precisam ter conhecimento da localização física dos recursos computacionais;

d) Elasticidade e escalabilidade: Recursos podem ser adquiridos de forma rápida e elástica, em alguns casos automaticamente, caso haja a necessidade de escalar com o aumento da demanda, e liberados, na retração dessa demanda. Adequa-se à demanda do consumidor, que tem a sensação de ausência de limites e de conformação a qualquer quantidade e momento da demanda. Escalabilidade ou escalonamento é característica corolário da elasticidade, e consubstancia-se na capacidade da nuvem computacional crescer de forma praticamente infinita, passando ao usuário/consumidor a sensação ou ilusão de capacidade infindável de armazenamentos, aplicações e recursos, na medida em que o *pool* de serviços pode ser livremente ampliado ou manejado conforme a demanda incide sobre a nuvem com o passar do tempo.

Com efeito, a "nuvem" não é estanque: uma das suas primordiais características é a da elasticidade, que se constitui no fato de tal tecnologia moldar-se à necessidade demandada por seu usuário/consumidor, sem que tal variação cause interrupções ou transtornos à fruição dos serviços postos à disposição deste.

e) Mensuração constante do serviço: sistemas em nuvem automaticamente controlam e otimizam o uso de recursos por meio de uma capacidade de medição. São automaticamente controlados e otimizados utilizando sua capacidade de medição e abstração apropriadas para o tipo de serviço escolhido, o que permite oferecer ao consumidor, transparência, além de total e efetivo controle do serviço utilizado.

1.3 Modelos de serviço da Computação em Nuvem

Após a apresentação das características técnicas da Computação em Nuvem, há necessidade de se conhecer seus modelos de aplicação.

De acordo com o NSIT, a Computação em Nuvem está cravada em três modelos de serviço e quatro modelos de entrega conhecidos.

Os modelos de serviço são:

a) *Software as a Service* (SaaS): o consumidor acessa os serviços que estão em um provedor que oferece aplicações em nuvem. Os sistemas de software são acessíveis a partir de vários dispositivos do usuário por meio de uma interface *thin client* como um navegador *Web*, mas o usuário final não gerencia nem controla a infraestrutura da nuvem, tais como a rede, os servidores, os sistemas operacionais, com exceção das possibilidades limitadas de configuração que os serviços disponibilizam de forma a tornar a experiência mais agradável.

Desta maneira, os desenvolvedores se concentram em inovação e não na infraestrutura, promovendo um desenvolvimento célere de novos sistemas e recursos, os quais podem ser incorporados automaticamente aos *softwares* sem que os usuários percebam, tornando transparente a evolução e atualização dos sistemas, reduzindo os custos ao consumidor, uma vez que é dispensada a aquisição de licenças de sistemas de *softwares*. Como exemplos de SaaS podemos destacar *Google Docs*.

b) *Platform as a Service* (PaaS): é ofertado ao usuário a possibilidade de criar e implantar na nuvem aplicações (usando linguagem de programação de computador) ou ainda, adquirir infraestrutura. Aqui, o usuário, como no modelo SaaS, não controla a infraestrutura da nuvem, mas tem controle sobre os aplicativos por ele desenvolvidos e implementados e suas configurações. A PaaS proporciona um sistema operacional, linguagens de programação e/ou ambientes de desenvolvimento para as aplicações, auxiliando a implementação de sistemas de software, uma vez que contém ferramentas de desenvolvimento e colaboração entre desenvolvedores.

Sob o prisma econômico, a PaaS permitirá aos usuários a utilização de serviços de terceiros, aumentando o uso do modelo de suporte no qual os usuários se inscrevem para solicitações de serviços de TI ou para resoluções de problemas pela Web. Com isso, pode-se melhorar o gerenciamento do trabalho e as responsabilidades das equipes de TI das empresas. É possível destacar, como PaaS, Google App Engine, Microsoft® Windows® Azure.

c) *Infrastructure as a Service* (IaaS): O termo IaaS se refere a uma infraestrutura computacional baseada em técnicas de virtualização de

recursos de computação. Isto é, refere-se à parte responsável por prover toda a infraestrutura necessária para a PaaS e o SaaS. Seu principal é facilitar o acesso ao o fornecimento de recursos, tais como servidores, rede, armazenamento e outros recursos de computação fundamentais para construir um ambiente sob demanda, que podem incluir sistemas operacionais e aplicativos.

Desta forma, é entregue ao usuário a capacidade de fornecer processamento, armazenamento e redes e outros recursos de *hardware* que poderão ser utilizados para executar qualquer programa de computador que deseje, tal qual um sistema operacional ou ainda, aplicativos. Em geral, o usuário não administra ou controla a infraestrutura da nuvem, mas tem controle sobre os sistemas operacionais, armazenamento e aplicativos implantados, e, eventualmente, seleciona componentes de rede, tais como *firewalls*.

Por fim, analisando os modelos de serviço, é possível observar que o ponto em comum entre eles reside no fato de que, em nenhum momento, o usuário tem controle sobre a infraestrutura da nuvem, em razão da necessidade de minorar os custos do usuário como características basilar da Computação em Nuvem.

Pelo conceito estipulado no presente estudo, vê-se a peculiaridade da Computação em Nuvem reside na delegação da capacidade de armazenamento a um terceiro prestador de serviços. E é justamente aqui que reside uma das maiores problemáticas da Computação em Nuvem, qual seja, a questão da segurança da informação entregue a tal tipo de tecnologia.

1.4 Modelos de implantação da Computação em Nuvem

Considerando o acesso e disponibilidade de ambientes de computação em nuvem, é possível distinguir diferentes tipos de modelos de implantação. A maneira de acesso depende do negócio, do tipo de informação e do nível de visão do usuário. Certas empresas não desejam que todos os usuários possam acessar e utilizar determinados recursos no seu ambiente de computação em nuvem, surgindo, neste sentido, a necessidade de ambientes mais restritos, em que somente alguns usuários devidamente autorizados possam utilizar os serviços providos.

Os modelos de implantação repercutem junto ao usuário de forma bastante incisiva, o que possibilita à computação em nuvem ser a tecnologia que permite a mudança de paradigmas na relação humano-máquina.

Os modelos de implantação da computação em nuvem podem ser divididos em nuvem pública, privada, comunidade e híbrida

a) Nuvem Privada: a infraestrutura da nuvem é de uso exclusivo de uma única organização, proprietária ou não da nuvem, que pode compreender vários usuários, com diferentes níveis de gerenciamento. Neste modelo, são empregados políticas de acesso aos serviços, promovendo diferentes níveis de gerenciamento de redes; de configurações dos provedores de serviços; e de utilização de tecnologias de autenticação e autorização.

b) Nuvem Comunitária: neste modelo há um compartilhamento por diversas empresas e/ou usuários de um sistema de nuvem, sendo esta suportada por uma comunidade específica que partilhou seus interesses. Este tipo de modelo de implantação pode existir local ou remotamente e, em regra, é gerenciado por alguma empresa da comunidade ou por terceiros.

c) Nuvem Pública: a infraestrutura é disponível para uso aberto do público em geral, sendo acessado por qualquer usuário que conheça a localização do serviço. Neste modelo, não podem ser aplicadas restrições de acesso quanto ao gerenciamento de redes, nem utilizar técnicas para autenticação e autorização.

d) Nuvem Híbrida: neste modelo existe uma composição de dois ou mais modelos de implantação de nuvens, que podem ser privadas, comunidade ou pública e que permanecem como entidades únicas, ligadas por uma tecnologia padronizada ou proprietária que permite a portabilidade de dados e aplicações.

1.5 Vantagens associadas à adoção da Computação em Nuvem

Desde a criação dos computadores portáteis (*notebooks*), a forma clássica de projetá-los e fabricá-los permanece basicamente a mesma, pois se refere a junção de peças e instrumentos, que viabilizam ao seu usuário a interação com a máquina por meio de um processo eletrônico, consubstanciado no teclado, touchpad ou no monitor. Dentre os componentes integrados à estrutura do computadores, destacam-se a memória RAM (*Randon Access Memory*) ou o disco rígido (*Hard Disk Drive*), que são responsáveis pelo armazenamento e backup das informações neles produzidas e/ou salvas, respectivamente.

A Computação em Nuvem busca justamente romper o paradigma clássico de fabricação e existência de um dispositivo tecnológico para o armazenamento de dados, haja vista que retira deste a função de armazenar e efetuar cópias de segurança da informação, deixando-os precipuamente com a incumbência de proporcionar acesso à rede, com o fito de buscar a informação armazenada no servidor.

Assim, como se denota da definição e características da nuvem computacional, toda a tarefa de armazenamento e *backup* da informação é delegada a servidores geralmente situados nas sedes das empresas prestadoras de serviços de *Cloud Computing*.

Outrossim, a computação em nuvem é tecnologia que amplia a possibilidade de fabricação de dispositivos eletrônicos cada vez menores e confortáveis ao usuário, haja vista que tais aparatos não precisam mais conter, em sua estrutura física, pesados e grandes componentes de armazenamento. Concomitantemente aos fatores expostos, existe a tendência de mercado de que quanto mais o dispositivo demandar componentes para poder existir, e quanto maior for a *expertise* empregadas nestes, maior será o custo de sua fabricação. Dessa maneira, o custo será repassado ao usuário/consumidor, que precisará pagar mais caro para ter um produto com alta tecnologia embutida.

Através da Computação em Nuvem, ao consumidor é possibilitada a aquisição de um produto potencialmente mais barato, justamente porque necessita de um menor número de componentes estruturais para existir. O aparelho é otimizado ao ponto de proporcionar acesso aos meios digitais e não mais a armazenar informações, as quais ficarão armazenadas na "nuvem", que é a estrutura física e lógica encarregada de proporcionar alocação de conteúdo e torná-lo disponível para acesso via *smartphones*, *tablets*, *ultrabooks*, entre outros. Assim, o consumidor solicita a tecnologia da computação em nuvem, pagando pela demanda. É o sistema pague por uso (*pay per use*) disponibilizado pela já

mencionado modelo *software as a service* (SaaS). Em tal sistema, o recurso baseado nesta é entregue na exata medida em que demandado, sem que o consumidor acabe arcando com o custo de um serviço superdimensionado ou demasiado à sua necessidade. Sobre tal característica da "nuvem", preleciona Hans Alberto Franke (2010, p.38):

> Nos últimos anos, com Cloud Computing emergindo, a computação teve seu cenário de arquiteturas de serviço modificado. Cloud Computing é baseado na visão de prover serviços como utilidades (e.g. agua, luz), onde consumidores podem acessar os serviços em qualquer lugar do mundo e, por demanda, pagar apenas pela quantidade que consomem.

Ademais, alguns estudiosos, como Arlindo Marcon Jr (2010, p.10), ressaltam a economia de materiais proporcionada pela tecnologia desenvolvida pela Computação em Nuvem:

> A migração de sistemas tradicionais para os serviços fornecidos pela nuvem pretende reduzir os custos de manutenção da infraestrutura de TI (Tecnologia da Informação) do consumidor, oferecendo as seguintes vantagens [Zhang et al. 2010]: economia em servidores, armazenamento, rede, licenças de software, energia, resfriamento e bens materiais; redução de trabalho na administração de sistemas; redução do tempo de configuração; diminuição de equipes de trabalho; desenvolvimento de aplicações com ciclo de vida mais curto e consequente redução do tempo de disponibilização de novos produtos e serviços no mercado; maior confiabilidade com custos menores e redução de gastos com manutenção, redução de custos com atualizações de hardware/infraestrutura.

Em contrapartida, diversas empresas do setor de tecnologia da informação elaboraram estudos para tentar concluir se a tecnologia da computação em nuvem é realmente barata.

A tecnologia da Computação em Nuvem traz inerente a si a razão de baratear os dispositivos tecnológicos e dos serviços nela baseados. Principalmente se for levado em consideração o axioma mercadológico

da oferta e da procura, onde quanto mais tal forma de computação se popularizar e disseminar, maior será a redução de custos ao consumidor, que, por sua vez, poderá optar pela contratação de serviços em "nuvem", balizando-se na concorrência entre fornecedores e o preço praticado por estes.

Tal tecnologia permite que as empresas possam mais facilmente escalar seus serviços de acordo com a demanda de seus clientes, uma vez que os recursos computacionais são manuseados via *software*, que podem ser disponibilizados rapidamente à medida que novos equipamentos são adicionados à rede, podendo, assim, minorar mais ainda os custos de manutenção. Na realidade, o objetivo da computação em nuvem é possibilitar que os recursos sejam escalados dinamicamente, para mais ou para menos, por meio de software, dependendo da carga dos clientes, com a mínima interação possível com os provedores.

Outra questão mormente aos benefícios proporcionados pela Computação em Nuvem relaciona-se com a como possibilidade de redução do uso de matérias-primas não renováveis na fabricação de dispositivos tecnológicos. Com a sociedade interconectada houve aumento exponencial do consumo de dispositivos eletrônicos que, como qualquer outro bem de consumo, ainda utilizam-se de métodos fabris expropriadores da natureza, ocasionando a produção poluentes. O lixo eletrônico é todo resíduo material produzido pelo descarte de equipamentos eletrônicos. Com o elevado uso de equipamentos eletrônicos no mundo moderno, este tipo de lixo tem se tornado um grande problema ambiental quando não descartado em locais adequados.

O perigo do lixo eletrônico reside no fato de que ele é altamente prejudicial à saúde humana, por possuir muitos elementos químicos, inclusive alguns deles, comprovadamente cancerígenos, como chumbo e mercúrio.

A problemática ambiental oriunda da produção, comercialização e do uso dos dispositivos tecnológicos se mostra patente, sobretudo, na seara ambiental, pois os problemas afetos ao crescente uso de aparatos tecnológicos, bem como ao continuo gasto de energia para fabricá-los tendem a consumir rapidamente recursos ambientais, como, por exemplo, o silício, utilizado largamente para a fabricação de aparatos tecnológicos.

O desenvolvimento da tecnologia da Computação em Nuvem com relação ao meio ambiente proporciona uma economia de energia e de recursos ambientais na fabricação de dispositivos eletrônicos, pois a redução de insumos escassos e não renováveis, como silício e petróleo, está diretamente relacionada ao tamanho cada vez menor do dispositivo fabricado. Logo, é plausível afirmar que tanto a preservação ambiental

quanto a redução de custos ao consumidor pode ser analisadas sob o prisma da computação em nuvem, como meio a proporcionar a redução do uso de matéria prima não renovável na produção de dispositivos como *tablets*, *smartphones* e *notebooks*.

Ademais, a tecnologia da computação em nuvem tem potencial para reduzir as barreiras que a TI impõe à inovação, o que é visivelmente demonstrado observando-se as inúmeras novas empresas que têm surgido, servindo-se de recursos computacionais em nuvem e que, em pouco tempo de atuação, são excepcionalmente bem sucedidas. Nesta situação, podem ser citadas como exemplo *YouTube, Facebook*.

Em um contexto econômico, em 2012, por causa de convênio firmando com o Ministério da Ciência, Tecnologia e Inovação, a Brasscom contratou junto à *Frost & Sullivan*, um estudo de mercado de Análise Competitiva do Mercado Brasileiro de *Datacenters*.[6] O estudo, entre outros itens, avaliou a composição dos custos de investimento (*capex*) e custos operacionais (*opex*) de *datacenter*s no Brasil. No estudo estimou um potencial de R$ 47 bilhões de investimentos em novos *datacenters* no período de 2013 à 2017.

A análise dos custos de investimento (*capex*), baseada na construção de um *datacenter* com investimento total de US$ 60,9 milhões, revela a seguinte distribuição dos investimentos: 58,5% em *software* e *hardware*, sendo US$ 7,6 milhões em *software* e segurança; 20,4% em sistemas de energia e refrigeração; 16.9% em espaço físico e 4,2% em infraestrutura de telecomunicações. A análise de custos operacionais (*opex*) aponta para um custo mensal de US$ 950.000, com a seguinte distribuição: 33,0% com energia; 28,4% com manutenção; 26% com mão de obra; e 12,6% com telecomunicações. O gráfico abaixo melhor representa os números informados:

[6] Fonte: Frost & Sullivan, Análise Competitiva do Mercado Brasileiro de Datacenters, dezembro de 2012. Desenvolvido para MCTI, Ministério de Ciência Tecnologia e Inovação e Brasscom, Associação Brasileira de Empresas de Tecnologia da Informação e Comunicação.

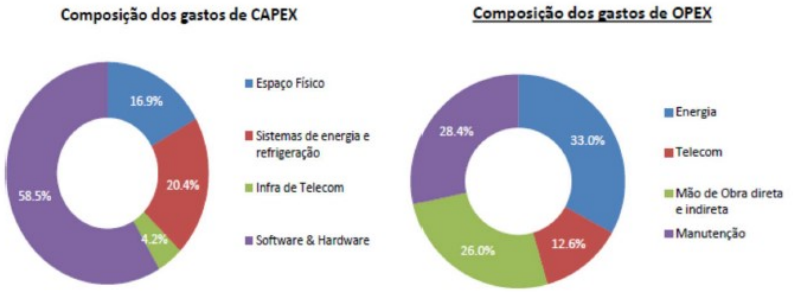

Gráfico 1 – Investimentos (*capex*) e custos operacionais (*opex*) em datacenters.

O mercado brasileiro de *datacenter* apresentou elevação de 14,3% no de 2016, com destaque para as áreas de evolução de *hosting* dedicado e serviços de armazenamento. Os dados da consultoria *Frost & Sullivan*[7] indicam ainda uma previsão otimista até 2017, com alta de ao menos 10% por ano. De acordo com o relatório, um dos mais importantes impulsionadores da Computação em Nuvem no Brasil é a disponibilidade de infraestrutura de TI, segundo 84,6% das empresas entrevistadas. Para 81,3% dos executivos de TI dessas organizações, a redução de custos é o principal fator para migrarem sua infraestrutura para a nuvem.

Atualmente, o Brasil ocupa o 22º lugar em um ranking de 24 países no uso de Computação em Nuvem, conforme estudo feito pela *Business Software Alliance* (BSA)[8], entidade que representa os pesos pesados da indústria norte-americana, entre elas, a Microsoft.

1.6 Desvantagens associadas à adoção da Computação em Nuvem

Após análise acerca das vantagens, percebeu-se que os referenciais bibliográficos adotados pouco mencionam a respeito das desvantagens que possam servir de impedimento à contratação de serviços de Computação em Nuvem. Miller (2008) apresenta uma lista de potenciais obstáculos que inibem a migração de usuários para estes ambientes. Estes obstáculos são:

1 - Falta de recursos: a implementação de um sistema de computação em nuvem é um grande desafio técnico, pois centenas ou

[7] Disponível em: http://www.frost.com/sublib/display-report.do?id=N807-01-00-00-00

[8] Estudo disponível no site: http://cloudscorecard.bsa.org/2016, acesso em 30 de julho de 2017.

milhares de computadores e servidores devem ser adquiridos e instalados com alto grau de interação entre eles, a fim de proporcionar um gerenciamento integral de todo o sistema durante o funcionamento. Tudo isto requer um investimento massivo de recursos financeiros e não é qualquer empresa de tecnologia que consegue viabilizar adequadamente;

2 – Demorado retorno de investimento: Em razão do volume de investimento necessário para implementar um ambiente de computação em nuvem, o retorno do capital investido, bem como a geração de lucro são demorados, o que inibem interessados em prestar este tipo de serviços.

3 – Desconfiança na segurança do serviço: Este fator se relaciona à segurança dos dados mantidos pelas aplicações executadas em nuvens, pois, como já houveram tantos os casos de violação de segurança computacional, até mesmo em ambientes com menor grau de vulnerabilidade, os usuários/consumidores questionam se, de fato, os fornecedores têm condições de garantir a segurança nas nuvens. Ademais, o fato de os acervos de informação estarem armazenados em locais distantes ou mesmo desconhecidos proporciona, em muitos consumidores, uma sensação de perda, o que aumenta a desconfiança na Computação em Nuvem. Logo, uma mudança de atitude para com relação a esta sensação exige novo comportamento por parte dos consumidores e dos fornecedores.

Pensando a desconfiança dos consumidores**,** os autores Marks e Lozano (2010, p.107/108) destacam que a adoção de métodos, ferramentas e/ou mecanismos de segurança por parte dos fornecedores do Serviço de Computação em Nuvem são essenciais para a satisfazer os usuários:

> A segurança da nuvem e as preocupações de privacidade associadas, fazem com que muitas organizações pausem enquanto pensam em suas preocupações particulares de computação em nuvem. As preocupações de segurança e privacidade incluem segurança física e acesso simples a instalações e equipamentos, bem como segurança lógica, requisitos de conformidade da indústria, auditabilidade, e mais. Há também duas perspectivas: (1) onde o vidro de segurança está meio cheio e (2) onde está meio vazio. A perspectiva do Halffull de vidro acredita que as preocupações com a segurança da nuvem são gerenciáveis e de fato são melhores quando tratadas por um provedor de serviços da terceira

> parte da nuvem. O ponto de vista meio vazio de vidro exibe todos os desafios de segurança como obstáculos que são imóveis e não podem ser mitigados ou superados, independentemente do perfil de negócios que merece internamento em uma nuvem. Tal como acontece com os desafios de segurança que acompanharam a SOA e os serviços da Web, a arquitetura de segurança e os modelos associados à nuvem serão debatidos de forma semelhante, e silenciosamente superados com soluções de segurança à medida que a indústria evolua. [9]

A segurança e a privacidade são quesitos importantes para a adoção dos ambientes de computação em nuvem e a perspectiva de existência de potenciais falhas de segurança e violação da privacidade faz com que consumidores se questionem sobre a adoção desses ambientes. Portanto, as empresas devem proporcionar aos usuários mecanismos ou ferramentas de segurança virtual eficazes contra possíveis violações. Os consumidores esperam que os sistemas de Computação em Nuvem sejam confiáveis e que a disponibilidade dos serviços e recursos oferecidos atenda integralmente às suas necessidades.

A Computação em Nuvem depende fundamentalmente de confiabilidade, portanto, se os usuários/consumidores sentem que não podem tê-la na plenitude, relutam em aderir a este modelo de tecnologia.

---

[9] Tradução livre de: The security of cloud, and associated privacy concerns, give many organizations pause as they think through their particular cloud computing concerns Security and privacy concerns include physical security and simple access to facilities and equipment, as well as logical security, industry compliance requirements, auditability, and more. There are also two perspectives: (1) where the security glass is half-full and (2) where it is half-empty. The glass halffull perspective believes that the cloud security concerns are manageable and in fact are better when handled by a thirdparty cloud service provider. The glass half-empty point of view views all security challenges as hurdles that are immovable and cannot be mitigated or overcome, regardless of the business profile that merits onboarding into a cloud. As with the security challenges that attended SOA and web services, the security architecture and models associated with cloud will similarly be stridently debated, and quietly overcome with security solutions as the industry evolves.

1.7 Descrição, descoberta, composição de serviços e licenciamento de *software*

Na Computação em Nuvem, vários modelos desenvolvidos evoluíram rapidamente para aproveitar as tecnologias de *software*, plataformas de programação, armazenamento de dados ou infraestrutura de *hardware*. Ao passo que estes modelos se referem ao núcleo dos serviços de Computação em Nuvem, a interoperabilidade têm sido pouco falha e a sua viabilidade, muitas vezes, é questionável.

Cada serviço da nuvem tem interfaces e protocolos próprios e é complexo para os usuários encontrarem e comporem serviços que necessitem, uma vez que há uma grande diversidade de serviços dispersos na Internet. Por exemplo, suponha que um usuário necessite de dois serviços da nuvem, um de processamento e outro de armazenamento para guardar os dados processados. Para tanto, seria necessário, compor os serviços de processamento e armazenamento, o que é outra dificuldade para os desenvolvedores.

Dessa forma, o desafio é desenvolver técnicas eficazes para descrever, descobrir e compor serviços na nuvem de forma a auxiliar os usuários em suas tarefas de forma completa. Modelos de Dados, conhecido como Ontologia da Tecnologia de Informação, podem ser utilizadas para a organização do domínio de conhecimento de computação em nuvem, ajudando na descrição e descoberta de serviços em nuvem, assim como na composição de novos serviços a partir dos serviços existentes, promovendo um aumento da interoperabilidade entre diferentes provedores e, consequentemente, proporcionando melhorias na qualidade dos serviços.

Por outro lado, a Computação em Nuvem ainda necessita de elementos integradores que possibilitem ao usuário a utilização de serviços pouco complexos, uma vez que não há uma padronização entre os serviços ofertados. Neste sentido, Souza et al (2010, p. 34):

> Contudo, não existem padrões de integração de sistemas de computação em nuvem [OpenCloud 2010]. O formato XML pode ser uma alternativa para mover dados entre ambientes em nuvem, mas os sistemas também precisam gerenciar dados localmente. A utilização de APIs pode auxiliar neste processo de integração. Por exemplo, as APIs da Amazon estão se tornando um padrão de fato para serviços sob demanda. Contudo, a quantidade de tecnologias envolvidas é muito grande,

> tornando-se um desafio padronizar as diversas interfaces e serviços, bem como fornecer interoperabilidade entre recursos heterogêneos.[10]

É possível concluir que serviços da nuvem computacional podem, por não conseguirem ainda interagir entre si em razão da falta de padronização, carecer de elementos de interoperabilidade. Pode aquele que busca os benefícios da computação em nuvem, por ausência de padrão ou de elementos básicos sobre o funcionamento, vir a se confundir facilmente e acabar contratando algo que não precise, ou que possa ser, ainda, sub ou hiperdimensionado às suas necessidades.

A falta de uma composição maior de serviços, ocasionada pela divergência de sistemas, que não são capazes, ainda, de perfeitamente integrarem-se entre si, podem gerar problemas afetos ao licenciamento de *software*, ou seja, aos modelos de cobrança ao usuário do serviço prestado

Neste sentido, Souza et. al (2010, p.35):

> Assim, a computação em nuvem apresenta diversos modelos de preço, sendo estes organizados em três grupos: preço diferenciado, preços por unidade e assinatura de serviços básicos. Preço diferenciado é o modelo adotado pela Amazon, onde os serviços são oferecidos em vários níveis de especificações, tais como alocação de memória e tipo de CPU, informações de SLA e o valor cobrado é um preço específico por unidade de tempo. Preço por unidade é normalmente aplicado a dados transferidos ou ao uso de memória. Este modelo é mais flexível do que o de preço diferenciado, já que permite aos usuários personalizarem a alocação de memória de seus sistemas baseados nas necessidades de aplicações específicas. O modelo de assinatura de serviços básicos é o modelo de preços mais amplamente utilizado, permitindo aos usuários preverem suas despesas previamente na utilização de um serviço. Contudo, este modelo não tem a precisão em cobrar dos usuários o que eles têm realmente utilizado.

[10] SOUZA, Flávio R.C; MOREIRA, Leonardo O; MACEDO, José Antônio F. de; MACHADO, Javam C. Gerenciamento de Dados em Nuvem: Conceitos, Sistemas e Desafios. Publicado no SWIB 2010. Disponível em:< >. Acesso em 15 de abril de 2017.

Desta maneira, é possível vislumbrar que os esquemas de cobrança praticados pelos desenvolvedores de software para licenciar seus produtos não têm se mostrado compatíveis com a maneira pela qual estão sendo compostas as ofertas de serviços em nuvens, o que, por vezes, leva a situações que inviabilizam o uso de determinados software em função do custo para os consumidores. Aos desenvolvedores da tecnologia da Computação em Nuvem é imposto o dever de trilhar os caminhos necessários rumo à solução destas contradições ou controvérsias, possibilitando a fruição mais apurada e vantajosa das potencialidades da nuvem. Isso porque, somente a constituição de uma plena tecnologia de nuvem computacional apta a satisfazer os anseios do consumidor é que possibilitará a este, bem avaliar os serviços em "nuvem".

É difícil falar em possibilidade de auditoria pelo usuário quando o assunto é Computação em Nuvem. Afinal, como uma pessoa física irá facilmente auditar um servidor que está localizado em outro país, por exemplo? Portanto, aquele que utiliza os serviços na nuvem computacional fica limitado, muitas vezes, pela ausência de recursos de fácil aferição, valendo-se, portanto, de elementos empíricos para constatação da qualidade na prestação de serviços, quando na verdade, deveria esperar uma verdadeira relação consumerista baseada nos elementos da boa-fé objetiva e nos deveres anexos ao contrato, tais como cooperação, cuidado, segurança e outros. Assim, o desenvolvedor ou fornecedor do serviço baseado em Computação em Nuvem deve adotar mecanismos transparentes e de fácil detecção da qualidade dos recursos contratados pelo usuário.

Um dos aspectos mais relevantes inerente à avaliação dos serviços de Computação em Nuvem é a segurança dos serviços de dados, pois, afinal, somente poderá ser bem avaliado um serviço seguro e confiável.

E neste sentido, e diante de tudo o que foi tratado até o presente momento, há que se considerar que dentre os desafios da computação em nuvem, aquele afeto ao gerenciamento e segurança dos serviços de dados foi identificado como sendo o principal entrave à integral assunção pelos usuários da referida tecnologia. Por se tratar o tema, o ponto fulcral do estudo, exigindo, portanto, maiores detalhes e aprofundamentos, o mesmo será abordado mais à frente.

CAPÍTULO 2 – ASPECTOS JURÍDICOS DA INTERNET

As transformações provocadas pela Internet na vida do ser humano são evidentes e se solidificam dia a dia, com interferência em todos os campos sociais: na cultura; na economia; na educação e, por conseguinte, atinge o campo do direito. Estamos diante de uma nova realidade – o mundo virtual convivendo com o mundo real. Hoje, o computador é um equipamento essencial para a própria sobrevivência do homem em sociedade. Atualmente, o Direito possui o grande desafio de compreender as inovações tecnológicas, visando a garantia da pacificação social, o desenvolvimento sustentável e da manutenção do próprio Estado Democrático de Direito. Para Gustavo Corrêa (2000, p.8):

> A Internet é um sistema global de rede de computadores que possibilita a comunicação e a transferência de arquivos de uma máquina a qualquer outra máquina conectada na rede, possibilitando, assim, um intercâmbio de informações sem precedentes na história, de maneira rápida, eficiente e sem limitação de fronteiras, culminando na criação de novos mecanismos de relacionamento.

O Direito sempre buscou regular relações decorrentes da realidade fática e de âmbito material. Ao regular a arte, a propriedade intelectual, para protegê-las juridicamente, o Direito partiu do momento em que a ideia, a criação se exteriorizou no mundo concreto, isto é, quando a obra intelectual e artística se materializou no mundo fático. Agora, principalmente em relação à Internet, o Direito se vê diante de um mundo virtual, que não precisa exteriorizar-se materialmente para gerar efeitos jurídicos no mundo fático.

O problema decorrente das relações produzidas pela Ciência do Direito e da Informática deve ser amplamente conhecido e avaliado pela comunidade jurídica e pelo legislador nacional. Este, depois da ampla discussão jurídica e legislativa que já seguiu à problemática levantada, precisa apresentar soluções legais aptas a permitirem o reconhecimento e a segurança jurídica que os negócios e as relações jurídicas concretizadas pela internet necessitam para sua eficácia e validade plena no mundo do Direito.

2.1 – Internet, mais que uma ferramenta democrática de integração, um direito fundamental

A rede mundial de computadores surgiu num forma embrionária durante o período da Guerra Fria. Primordialmente, foi desenvolvida com objetivos exclusivamente militares, porque seria uma das formas das forças armadas norte-americanas de manter as comunicações rápidas e confiáveis, em caso de ataques inimigos que lhes destruíssem os meios convencionais de telecomunicações, como telégrafo e telefone.

No final dos anos 1980, o pesquisador britânico do CERN – *Conseil Européen pour la Recherche Nucléaire* (Conselho Europeu para a Pesquisa Nuclear) – Sir Tim Berners-Lee escreveu sobre uma possível e viável proposta de interconectar redes de computadores numa única e gigantesca rede: a rede mundial de computadores. Desta forma, foi criada a *World Wide Web*.

O processo evolutivo da *Internet* vem sendo escalonado por várias etapas, que perpassam pelo uso institucionalizado de Estados soberanos, os quais possuem o poder legiferante para a produção de normas mínimas acerca do uso da Internet, dentro de seu âmbito territorial. Entretanto, a interligação rápida de informação entre computadores, propiciada pela rede mundial de computadores, desafia as soberanias modernas, mitigando as fronteiras internacionais.

A Internet possui como características primordiais a velocidade, que permite a execução imediata de tarefas, gastando um tempo infinitamente menor que na via comum; a hipertextualidade, que se refere a conexão entre sítios eletrônicos; a multimídia, qual está relacionada à união de imagens, sons e vídeos numa só mídia informativa; a interatividade, como forma de comunicação mais rápida, a Internet proporciona a interação social, mesmo à distância; e, por último, a personalização, que é a adaptação de um produto aos anseios ou preferências do usuário.

Inobstante a presença nítida desta características, a utilização da rede mundial de computadores é diferente para cada Estado-Nação, por causa da ausência de uma regulamentação mínima internacional.

Atualmente, a rede mundial de computadores é considerada por parte da maioria dos Estados como uma ferramenta interativa e rápida de comunicação e de transmissão de dados digitais. Todavia, este paradigma está se modificando, uma vez que a rede mundial de computadores, diante da pungente Revolução Tecnocientífica, qualifica-se como uma das formas dos exercício de democracia.

O primeiro passo para a modificação do paradigma da rede mundial de computadores foi dado pela Organização das Nações Unidas (ONU), na sua publicação *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*, de 16 de maio de 2011. Neste relatório, a ONU afirmou, em síntese, que o acesso à Internet é um direito humano e que desconectar a população da *web* viola esta política. Logo, impedir o acesso à informação pela *web* infringe, segundo a ONU, o artigo 19, parágrafo 3, do Pacto Internacional de Direitos Civis e Políticos, de 1966:

> ARTIGO 19
>
> 1. Ninguém poderá ser molestado por suas opiniões.
> 2. **Toda pessoa terá direito à liberdade de expressão; esse direito incluirá a liberdade de procurar, receber e difundir informações e idéias de qualquer natureza, independentemente de considerações de fronteiras, verbalmente ou por escrito, em forma impressa ou artística, ou por qualquer outro meio de sua escolha.**
> 3**. O exercício do direito previsto no parágrafo 2 do presente artigo implicará deveres e responsabilidades especiais. Consequentemente, poderá estar sujeito a certas restrições, que devem, entretanto, ser expressamente previstas em lei e que se façam necessárias** para:
> a) assegurar o respeito dos direitos e da reputação das demais pessoas;
> b) proteger a segurança nacional, a ordem, a saúde ou a moral públicas. (destaque nosso)

Em seu relatório, a Organização das Nações Unidas reconhece a grandiosidade da rede mundial de computadores, bem como suas características, ao aduzir que:

> Muito poucos, se quaisquer desenvolvimentos nas tecnologias de informação têm tido um efeito tão revolucionário quanto a criação da Internet. Diferente de qualquer outro meio de comunicação, como rádio, televisão e publicações impressas baseada na transmissão de um título de informação,

a Internet representa um salto significativo para a frente como na mídia interativa. De fato, com o advento de serviços de Web 2.0, ou plataformas intermediárias que facilitam participativa compartilhamento de informações e colaboração na criação de conteúdos, os indivíduos já não são receptores passivos, mas também editores ativos de informação. Essas plataformas são particularmente valiosas em países onde não há meios de comunicação independentes, uma vez que permitem aos indivíduos para compartilhar pontos de vista críticos e obter a informação objetiva. Além disso, os produtores de mídia tradicional também pode usar a internet para expandir as suas audiências a um custo nominal. De modo mais geral, ao permitir que os indivíduos para trocar informações e ideias instantaneamente e barata através das fronteiras nacionais, a Internet permite o acesso à informação e conhecimento que antes era inatingível. Este, por sua vez, contribui para a descoberta da verdade e progresso da sociedade como um todo.

Na verdade, a Internet tornou-se um dos principais meios pelos quais os indivíduos podem exercer o seu direito à liberdade de opinião e de expressão, garantido pelo artigo 19 da Declaração Universal dos Direitos Humanos e no Pacto Internacional sobre os Direitos Civis e Políticos. Este último prevê que:

(A) Todas as pessoas têm o direito de ter opiniões sem interferência;

(B) Toda a pessoa tem direito à liberdade de expressão; este direito inclui a liberdade de procurar, receber e transmitir informações e idéias de todos os tipos, independentemente de fronteiras, seja oralmente, por escrito ou na cópia, em forma de arte, ou através de qualquer outro meio à sua escolha;

(C) O exercício dos direitos previstos no n.º 2 do presente artigo implicará deveres e responsabilidades especiais. Por conseguinte, pode estar sujeito a certas restrições, que serão unicamente as previstas pela lei e consideradas necessárias:

> (D) para o respeito dos direitos e da reputação de outrem;
> (E) para a proteção da segurança nacional ou da ordem pública (ordem pública), ou da saúde ou da moral públicas. [11]

O artigo 19, parágrafo 3, do Pacto Internacional de Direitos Civis e Políticos, de 1966 considera a hipótese de aqueles que tiverem transgredido algum tipo de lei, envolvendo meios de comunicação, possam sofrer restrições específicas, no entanto, não totais e apenas se as

[11]Tradução Livre: Very few if any developments in information technologies have had such a revolutionary effect as the creation of the Internet. Unlike any other medium of communication, such as radio, television and printed publications based on one-way transmission of information, the Internet represents a significant leap forward as na interactive medium. Indeed, with the advent of Web 2.0 services, or intermediary platforms that facilitate participatory information sharing and collaboration in the creation of content, individuals are no longer passive recipients, but also active publishers of information. Such platforms are particularly valuable in countries where there is no independent media, as they enable individuals to share critical views and to find objective information. Furthermore, producers of traditional media can also use the Internet to greatly expand their audiences at nominal cost. More generally, by enabling individuals to exchange information and ideas instantaneously and inexpensively across national borders, the Internet allows access to information and knowledge that was previously unattainable. This, in turn, contributes to the discovery of the truth and progress of society as a whole.
Indeed, the Internet has become a key means by which individuals can exercise their right to freedom of opinion and expression, as guaranteed by article 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights. The latter provides that:
(a) Everyone shall have the right to hold opinions without interference;
(b) Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice;
(c) The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
(d) for respect of the rights or reputations of others;
(e) for the protection of national security or of public order (ordre public), or of public health or morals. (destaque nosso)

transgressões colocarem em risco os direitos e reputações de outras pessoas ou a segurança nacional.

O relatório expõe que alguns países bloqueiam alguns conteúdos específicos na rede para seus cidadãos. Porém, para a ONU, não importa se houve violação de direitos autorais ou intelectuais, todo ser humano deve ter o direito de continuar com acesso à informação e à Internet. Por fim, a ONU pede aos países que revejam suas leis contra pessoas que tiverem cometidos violações de direitos autorais ou intelectuais e as punições adotadas, para que elas não contrariem as diretrizes contidas no Pacto Internacional de Direitos Civis e Políticos.

A Organização das Nações Unidas possui a competência e a legitimidade para atuar em conflitos entre os países, por meio da Carta das Nações Unidas, que também reconheceu a obrigação dos Estados de manter a segurança internacional, a paz e a praticar a tolerância e o respeito. Logo, a ONU passou a ser vista como o órgão central da nova ordem mundial.

Inobstante a ONU ser um organismo internacional formada por vários países, esta instituição possui uma personalidade jurídica própria que lhe possibilita a atuação no cenário internacional como entidade distinta do Estados membros, assim considerado individualmente. Com fundamento nesta lógica, em 1949, a Corte Internacional de Justiça (CIJ) estabeleceu que a personalidade jurídica da ONU está pautada na doutrina dos poderes implícitos, por meio da qual entende-se que o tratado constitutivo da organização confere-lhe os poderes ali acordados.

Trata-se, assim, de uma personalidade jurídica derivada, distinta daquela dos Estados, mas que, no entanto, visa o alcance do propósito para o qual foi criada a organização. Em outras palavras, os poderes implícitos e inerentes decorrem automaticamente do tratado que institui a organização, não se tratando de mera competência legislativa.

Por fim, é possível concluir que a personalidade jurídica da ONU se estende também ao âmbito interno, no momento em que exerce o poder de estabelecer um sistema jurídico próprio e independente dos ordenamentos estatais, a fim de reger condições de trabalho e funcionalismo.

A ONU é composta por distintos órgãos estatutários e subsidiários, sendo seus principais órgãos estatutários: a Assembleia Geral, o Conselho de Segurança, a Corte Internacional de Justiça, o Conselho de Tutela, o Secretariado e o Conselho Econômico e Social, os quais estão previstos no artigo 7° da Carta de São Francisco.

A Assembleia Geral é o órgão central e o pleno da ONU, tendo o caráter mais democrático, pois prevalece em seu processo de votação a

perspectiva de um voto único por Estado-membro, independentemente de seu poder político. Ademais, os processos de votação obedecem à maioria simples de presentes, salvo quando as questões em debate dizem respeito a segurança, paz ou assuntos financeiros, para os quais se exige maioria de dois terços, conforme o normatizado no artigo 18.2 da Carta de São Francisco.

De acordo com o artigo 10 da Carta da ONU, a Assembleia Geral pode discutir quaisquer questões que se insiram nas finalidades do documento ou que digam respeito a funções e atribuições dos órgãos criados a partir dela. Nesta esteira institucional de caráter internacional, a Organização das Nações Unidas pode deliberar sobre assuntos de direitos humanos, com a finalidade de proporcionar um melhor desenvolvimento no planeta.

As decisões proferidas pela Assembleia Geral da ONU são consideradas como recomendações, em razão do eminente caráter político, oriundo de debate dentro do órgão, tal como um Parlamento Nacional. No entanto, distintamente das normas materializadas em sede de legislativos nacionais, as decisões da Assembleia Geral não vinculam os Estados membros a adotá-las, razão pela qual são chamadas de recomendatórias, constituindo parte do *soft law* do direito internacional.

A título de exemplificação, há em tramitação no Brasil a Proposta de Emenda à Constituição nº 479/2010, que pugna pelo acréscimo do inciso LXXIX ao art. 5º da Constituição Federal, para incluir o acesso à Internet em alta velocidade entre os direitos fundamentais do cidadão. Há também a Lei 12.965/2014, conhecida como Marco Civil da Internet.

Com o contínuo desenvolvimento das Tecnologias de Informação e Comunicação, como a Internet, permitiu-se uma criação de novos institutos democráticos ou adaptação dos velhos modelos, em face do exercício de uma democracia eletrônica. Numa visão teleológica, podemos afirmar que a Internet permite que seus usuários participem igualmente de possíveis discussões. Para Rover (2012, p. 3):

> Embora o processo democrático contemporâneo se apresente como um sistema teleológico, de cima para baixo, onde as formas de exercício da cidadania estão definidas nos limites da Constituição Federal, **a internet, por sua vez, surge como um sistema emergente, de baixo para cima, um ambiente democrático e descentralizado que permite a participação direta de todos os que estiverem conectados e interessados em participar da política e ajudar**

> **a construir esta nova sociedade em rede. (grifo nosso)**

Em seguida, o autor (2012, p. 4) complementa:

> No que concerne especificamente à democracia eletrônica, o que interessa é o fortalecimento da relação entre o governo e o cidadão, e, dentro desta iniciativa, percebe-se que a falta de acesso à informação impede o pleno exercício da cidadania, pois a cidadania somente pode ser exercida de forma plena se for assegurado ao cidadão o acesso às novas tecnologias e à informação democrática e instantânea que no presente momento somente existe no ciberespaço.

É possível inferir que, atualmente, a *Internet* ultrapassa o viés de uma ferramenta de comunicação ou de integração entre pessoas e empresas, pois alterou toda a estrutura de interação dos cidadãos com seus respectivos governos, uma vez que permite àqueles o acesso rápido e transparente de informações.

2.2 – A transnacionalidade da *Internet* e a necessidade de uma proteção jurídica mínima

A alteração paradigmática influenciada pela Organização das Nações Unidas concede à Internet um novo *status* jurídico, deixando de ser uma simples ferramenta e passa a ser um meio inviolável de exercício dos direitos humanos, dentre eles, a cidadania. Contudo, faz-se necessário discutir-se a natureza jurídica da Internet, como um direito humano, frente à soberania dos Estados, considerando sua transnacionalidade, bem como a existência de um meio institucionalizado ou não para promover uma proteção jurídica mínima.

É cediço que a existência da sociedade internacional não ofende a soberania do Estado Constitucional Moderno. A progressiva inter-relação, interdependência entre Estados e a consolidação de uma ordem jurídica internacional, em razão da interação cultural, impulsionam o fenômeno da globalização, promovendo uma reformulação do próprio conceito de soberania absoluta.

O poder supremo estatal e a soberania estão sendo paulatinamente relativizados por causa do desenvolvimento de organizações transnacionais ou supranacionais, diante das quais muitos Estados se

viram impelidos a, por exemplo, firmar acordos comerciais ou militares com outros ou a mitigar sua independência jurídica para uma organizações estatal, como ocorre na União Europeia.

Como consequência do processo globalizante, o poder centralizado estatal vai se esvaziando, pois o Estado está transferindo suas atribuições jurídicas e administrativas, como se observa, por exemplo, quando o Estado Constitucional Moderno contrai obrigações externas na forma de Tratados Internacionais, permitindo o controle de seus atos por organismos externos, como a Convenção Americana de Direitos Humanos.

O modelo contemporâneo de territorialidade e de soberania é caracterizado pela insurgência de um espaço público democrático fundamentado na solidariedade e cooperação entre as nações, pondo de lado qualquer entrave de ideias e interesses antagônicos. Por isso, é imperioso repensar o Estado Constitucional Moderno a partir da concepção de uma nova ordem pública transnacional, em que exista solidariedade democrática entre povos, devendo-se ultrapassar as barreiras econômicas, sociais, raciais e culturais que dividem os Estados Modernos.

Nas palavras de Ulrich Beck (1999, p. 192), os "estados transnacionais são portanto Estados fortes, cujos poderes de conformação política nascem a partir de resposta cooperativas à globalização."

No entendimento do autor deste trabalho, a Internet, em razão de suas características, trouxe grandes e variados benefícios para o mundo moderno, onde se passou a produzir novas ideias, tecnologias, produtos e serviços, consolidando, assim, novas formas de relacionamento, de comércio, de negócios, mitigando o espaço físico existente entre povos e nações.

A sociedade tecnológica é caracterizada pelo imediatismo e pela quebra das barreiras geográficas na transmissão da informação, porque busca, por meio da Internet, uma fluidez imediata de informação, oriunda de diversas fontes nacionais ou internacionais. As características da sociedade tecnológica só são possíveis por causa da constante inovação na tecnologia de informação de hardware (componentes concretos da máquina) e de software (programas).

No mundo, o processo evolutivo da Internet não se deu uniformemente entre os países, em virtude de diversas variáveis, como cultura, economia, religião. Até mesmo, em plena metade da segunda década do Século XXI, há países, como Irã e Coreia do Norte, que controlam fortemente a utilização da Internet por parte de seus habitantes.

Outros países, por fatores econômicos, não possuem meios de disseminar a utilização da rede mundial de computadores entre sua população.

Outra consequência advinda da Internet é a internacionalização de relações jurídicas interpessoais, posto que se permita a comunicação imediata e instantânea entre pessoas, localizadas em partes diferentes do mundo, quais poderão firmar avenças entre si. Esta internacionalização permitiu uma liberdade, quase anárquica, do ciberespaço, pois se projeta uma cibersociedade sustentada em princípios éticos e morais culturalmente divergentes.

O Estado Moderno, delineado por Maquiavel, está se enfraquecendo paulatinamente, sobretudo pela sua impotência e incapacidade de impor sua soberania às novas demandas trazidas pelo fenômeno da globalização, cujo o catalisador primordial e atual é a Internet.

Para Gonçalves e Stelzer (2009, p.6):

> O Estado não desapareceu, mas relativizou-se de tal modo que em determinadas dimensões legais, não se reconhece mais o ente político-jurídico em suas características elementares: no embate público, a exemplo do Estado-membro europeu; no embate privado, com o Estado marginalizado do campo legal intra-firmas. Esse é o contexto na qual se insere a transnacionalidade, ou seja, "o desmanche da unidade do Estado e da sociedade nacional, novas relações de poder e de concorrência, novos conflitos e incompatibilidade entre atores e unidades do Estado nacional por um lado e, pelo outro, atores, identidades, espaços sociais e processos sociais transnacionais.

Nesta senda, podemos caracterizar a Internet como um fenômeno globalizante-transnacional, uma vez que não respeita os limites fronteiriços das soberanias estatais, e, em razão da forte e iminente interação social, promove diuturnamente a criação de novas relações jurídicas comerciais, sociais etc.

A ideia de transnacionalismo remete à existência de uma grande corporação multinacional, que promove sua atuação além das fronteiras dos Estados soberanos. Para Gonçalves e Stelzer (2009, p.13), "sob tal ponto de vista, não se trata do Direito transnacional, mas de adjetivação que se esforça em demonstrar a capacidade econômica que a mega corporação possui". Os autores complementam:

> As Corporações Transnacionais representam o que há de mais fetichizado no emergente cenário transnacional. Trata-se de unidades de capital privado, que condensam tecnologias e alta capacidade de produção, sob ritmo de produção em escala mundial, verdadeiro símbolo do capitalismo moderno. Assiste-se, nas operações de produção ou de prestação de serviço, à realização plena do capital, superando fronteiras, rumo à absoluta expansão mundial. No âmbito do fenômeno da transnacionalização, o Estado se vê frágil diante desses emergentes centros de decisão econômicos e políticos que comandam o sistema. "Dentro dos limites impostos pelas legislações locais, a empresa transnacional tenta configurar mercado internacional, englobando vários mercados nacionais. Para tanto, apóia-se no fato de que a tecnologia e a organização moderna empresarial permitem planejar sua produção, global e independentemente de fronteiras nacionais." (Gonçalves e Stelzer. 2009, p.13)

A exemplo destas grandes corporações mundiais, as quais prestam serviços de Internet ou se dele se beneficiam, temos *Google*, *Windows*, *Apple*, *Samsung*. É inegável que as condutas praticadas na Internet têm característica da transnacionalidade, porém é necessário se ponderar acerca da forma de combate de possíveis abusos e/ou crimes cometidos através da rede mundial de computadores. Para o combate de manifestações e ou abusos transnacionais, impõe-se a necessidade de cooperação entre os países, cujas necessidade acentua-se na mesma proporção do avanço da Tecnologia da Informação.

Inobstante o avanço tecnológico proporcionado pela Internet, em âmbito mundial, há somente a Convenção de Budapeste que foi o primeiro tratado internacional elaborado buscando tipificar os principais crimes cometidos na Internet, harmonizar leis, aperfeiçoar as técnicas de investigação e aumentar a cooperação entre as nações. Engloba mais de 30 países signatários, entre eles: Albânia, Armênia, Áustria, Bélgica, Bulgária, Croácia, Ilha de Chipre, Estônia, Finlândia, França, Alemanha, Grécia, Hungria, Itália, Letônia, Moldova, Holanda, Noruega, Polônia, Portugal, Romênia, Espanha, Suíça, República Iugoslava da Macedônia, Ucrânia e Inglaterra. De países não-membros do Conselho Europeu, houve a adesão do Canadá, Japão, África do Sul e dos Estados Unidos da América.

Segundo o texto, a Convenção prioriza "uma política criminal comum, com o objetivo de proteger a sociedade contra a criminalidade no ciberespaço, designadamente, através da adoção de legislação adequada e da melhoria da cooperação internacional" e reconhece "a necessidade de uma cooperação entre os Estados e a indústria privada". Em 2006, foi incluído mais um protocolo sobre a criminalização de atos de natureza racista e xenofóbicos. A Convenção de Budapeste é o principal acordo internacional regulador de uma legislação para crimes na Internet. Dá diretrizes gerais, mas não fere a autonomia dos países signatários de criarem suas próprias leis para criminalizar os cibercrimes.

Uma outra norma de nível internacional, a *ACTA* (Anti-Counterfeiting Trade Agreement - em tradução livre, "Acordo de Comércio Contra a Pirataria") é um acordo, assinado em outubro de 2011, pela Austrália, Canadá, Japão, Marrocos, Nova Zelândia, Cingapura, Coréia do Sul e Estados Unidos, visando a criação de leis mais rígidas para defesa de direitos autorais e combate à pirataria. O *ACTA* estipula que os países signatários criem leis nacionais que garantam a retirada de conteúdo ilegal da internet.

Para isso, a privacidade de usuários pode ser invadida e o infrator pode se ver obrigado a ressarcir parcelas de lucro, além de receber multas e penas legais. Além da propriedade intelectual, este acordo também aumenta a gravidade de crimes como a gravação de imagens a partir de telas de cinema, ou a falsificação de medicamentos. A vigilância na distribuição física de conteúdo pirateado também seria intensificada. Atualmente, a União Europeia estuda a adesão ao ACTA.

A Convenção de Budapeste e o *ACTA* são duas normas, a nível internacional, com um pequeno viés transnacional, pois os Estados signatários, apesar de não mitigarem suas respectivas soberanias, buscam uma cooperação mínima e eficaz em razão de um direito ou interesse maior e comum entre eles.

Considerando o caráter transnacional da Internet, o relatório de 2011 (*Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*), oriundo da Assembleia Geral das Nações Unidas, ao seu fim, propõe várias recomendações, dentre elas, a de considerar o acesso à Internet como um direito humano fundamental a nível mundial. Como já aduzido anteriormente, as decisões proferidas, através de Relatórios, pela Assembleia Geral da ONU tendem a serem chamadas de recomendações, pois possuem caráter político, oriundo de um intenso debate dentro da instituição. Desta forma, distintamente das normas tipificadas, as decisões da Assembleia Geral não impõem juridicamente a vinculação por parte

dos Estados membros, razão pela qual se constitui uma verdadeira *soft law* do direito internacional.

A nova qualificação jurídica da Internet demonstra a importância de uma proteção legal mínima e uniforme à Internet, uma vez que ultrapassa o conceito de uma mera ferramenta de comunicação social limitada a um grupo social, passando a ser um meio eletrônico de exercício à democracia, ante o efetivo fortalecimento da relação entre o governo e o cidadão, haja vista que a falta de acesso à informação impede o pleno exercício da cidadania.

Não há organismo internacional, interestatal ou não, que promova uma proteção jurídica mínima à Internet e, em razão deste fato, a Organização das Nações Unidas avocou para si esta competência e declarou que a Internet é um direito humano fundamental, necessário para a democracia.

É deveras difícil a criação de uma legislação mínima internacional (*hard law*) sobre a tônica da Internet, uma vez que a rede mundial de computadores, apesar da uniformidade de suas características, é utilizada diferentemente em cada Estado, com fundamento em suas peculiaridades.

Inobstante tal dificuldade, é possível a criação de organismos internacionais, intergovernamentais ou não, para atender a necessidade de uma evidente e imperiosa cooperação internacional sobre a temática da Internet, a exemplo como a Organização Mundial de Saúde, Organização Internacional do Trabalho, Greenpeace, dentre outros, os quais promovem uma política mínima de proteção e fomento ao direito à saúde, ao trabalho digno e ao meio ambiente.

Tais organismos intergovernamentais são uma associação voluntária de Estados, criada por um convênio constitutivo (Tratados e/ou Convenções) e com finalidades pré-determinadas, regida pelas normas de Direito Internacional, dotados de personalidade distinta da dos seus Estados-membros, que se encerram em um organismo próprio, dotados de autonomia e especificidade, possuindo ordenamento jurídico interno e órgãos auxiliares, por meio dos quais realiza os propósitos comuns de seus membros, mediante os poderes próprios que lhes são atribuídos por estes.

Inicialmente, é possível trazer à baila o questionamento acerca da necessidade da criação deste organismo internacional. A Internet é uma rede sem fronteiras, cabendo a cada Estado resguardar-se juridicamente contra possíveis abusos de direito por usuários internos ou estrangeiros. Entretanto, tal proteção jurídica pode ser exagerada ou leniente demais a depender da situação, uma vez que o exercício dos direitos humanos,

inobstante de aplicabilidade plena e imediata, possui restrições mínimas, por vezes a nível ético ou moral.

Por exemplo, há a Primavera Árabe, caracterizada pelas manifestações e protestos contra os governos do Egito, Líbia, Síria e Tunísia, quais foram organizadas através das redes sociais como *Facebook, Twitter e Youtube*, para organizar, comunicar e sensibilizar a população e a comunidade internacional em face de tentativas de repressão e censura na Internet por partes dos Estados.

É imperioso frisar que este organismo intergovernamental não teria o condão de limitar a utilização da Internet, mas tão-somente, propor ou recomendar políticas públicas internacionais de cooperação acerca da utilização da grande rede, a fim de promover um maior desenvolvimento social mundial. É uma consequência direta do fenômeno da internacionalização das relações jurídicas, qual pode ser claramente vista na interação social difundida na rede mundial de computadores.

Para Gonçalves e Stelzer (2009, p.3):

> A idéia de internacionalização traz em si o relacionamento predominante entre países, ausente percepção de alcance global. Na internacionalização as relações político-jurídicas desenvolvem-se de forma bilateral ou multilateral, mas sem que tal circunstância esteja envolvida com a multiplicação de enlaces decorrentes das transformações tecnológicas, de comunicação ou de transporte em escala planetária. Desse ponto de vista, o fenômeno da internacionalização está firmemente escorado na idéia de relações entre soberanias. A cooperação entre Estados é a característica dominante e a relação que se estabelece caracteriza-se por ser abreviada entre as partes. Entre os Estados vigora o respeito mútuo e a idéia de soberanias em semelhante plano.

Com a criação deste organismo internacional, não haverá uma transferência da soberania estatal para determinado ente jurídico, com a finalidade de decidir sobre determinado viés jurídico. Funda-se mais na transnacionalidade das relações jurídicas, uma vez que proporciona uma "desterritorialização dos relacionamentos político-sociais, fomentado por sistema econômico capitalista ultra-valorizado, que articula ordenamento jurídico mundial à margem das soberanias dos Estados" (Gonçalves, Stelzer, 2009, p.2).

As organizações internacionais não têm soberania, que é atributo exclusivo dos Estados, e seus poderes são apenas mediatos, já que são criadas pelos próprios Estados, através de acordos de cooperação. As Organizações Internacionais distinguem-se das Organizações Não-Governamentais, enquanto aquelas são criadas por tratados constitutivos concluídos entre Estados soberanos, o que lhes confere personalidade jurídica internacional, estas, por sua vez, são criadas pela vontade de particulares, sendo regidas pelo direito interno do Estado onde foram instituídos, sendo por estas normas regidas, e não pelas normas de Direito Internacional Público. Acrescente-se também que a criação destes organismos internacionais, interestatais ou não, promoveria uma democratização uniforme do uso da rede mundial, buscando primar pela proteção jurídica mínima dos usuários, haja vista seu caráter de direito humano fundamental, uma vez que concede ao indivíduo sua participação no processo democrático de seu país.

2.3 – A valoração mercantil da informação digital no contexto da sociedade tecnológica

Os produtos e serviços baseados em Tecnologia da Informação surgiram como formas de respostas aos anseios da sociedade tecnológica pela necessidade da ampla e imediata geração e troca de informações. Com a abertura deste meio de troca de informações para a sociedade civil, a disseminação do acesso à informação de forma instantânea passou a ser prioridade dos governos e empresas, uma vez que os outros meios digitais, assim como *fax modem*, não possuiam a caracteristicas da imediatidade. Para, *International Service of the Swiss Broadcasting*:

> A conexão de computadores em redes fechadas já havia começado em 1969, com a Arpanet, que interligava instituições de pesquisa dos EUA. Mas Tim Berners-Lee deu uma dimensão mundial à tecnologia. Sua proposta mostrava como as informações poderiam ser facilmente transferidas através da internet, utilizando hipertexto, hoje conhecido como sistema de ponto-e-clique de navegação através da informação. No ano seguinte, o engenheiro de sistemas do Cern Robert Cailliau tornou-se o primeiro usuário da web e um de seus defensores. A idéia era ligar hipertexto com a internet e computadores pessoais e, assim, formar uma única rede que ajudasse os físicos do Cern a partilhar todas as informações armazenadas em computador nos laboratórios da instituição.

A criação e o desenvolvimento de um meio de comunicação que ultrapassasse as barreiras geográficas que separam as pessoas, vieram possibilitar a diminuição dos custos da comunicação, bem como o maior controle sobre a troca de informações, em contraposição ao moroso processo tradicional de envio de cartas manuscritas e encomendas que os serviços de correios proporcionam até hoje. Por exemplo, a criação do correio eletrônico (*e-mail*) alterou a forma de troca de informações, principalmente porque passou a permitir a criação de uma cópia dos dados trocados, bem como o controle e catálogo, por data e hora, de mensagens enviadas e recebidas.

Assim, com a evolução tecnológica, surgiram posteriormente outros serviços baseados na rede mundial de computadores, como a

Computação em Nuvem, que permitiu a ampliação e consolidação do conceito de mobilidade da informação digital, através de dispositivos tecnológicos portáteis como *tablets*, *smartphones*.

Inobstante desse cenário tecnológico em franco desenvolvimento, é importante ressaltar que a informação nunca esteve totalmente segura, porque desde logo se percebeu o seu valor, uma vez que seu uso, posse ou domínio por aquele que não seja seu proprietário ou detentor, pode propiciar-lhe alguma vantagem econômica, política ou de poder, ainda que indevidamente.

A dinâmica da produção capitalista da era digital trata a informação como um verdadeiro produto diferenciado no mercado, buscando seu máximo lucro, haja vista que a informação está submetida à lei da oferta e da procura, adquirindo, assim, um autêntico *status* de mercadoria valiosa nos dias atuais. Logo, a ausência de educação tecnológica impulsiona a criação de problemas de segurança informacional.

Neste sentido, Manuel Castells (1999) afirma que quem detém a informação, detém o poder. Para este autor (1999, p.411), na era da informação, isso significa que "as lutas pelo poder são lutas culturais". A respeito de tal ilação, há vários exemplos na história da Humanidade: na Idade Média, era comum a interceptação e tortura dos mensageiros dos reinos, para obtenção de informações.

No Século XX, com a derrota na Primeira Grande Guerra, os alemães criaram uma máquina de criptografia chamada de Enigma, com a finalidade de codificar suas ordens e mensagens de guerra, impossibilitando o conhecimento e interpretação dos dados pelo inimigo. Todavia, o Terceiro Reich não esperava que o segredo da máquina Enigma caísse nas mãos dos Aliados, fazendo com que a inteligência alemã ruísse por completo.

É importante ressaltar que em seus primórdios, a imprensa tinha, em seu campo jornalístico, um poder fiscalizatório, que supervisionava a atuação do Estado em todos os momentos, apontando fato comprovados. Atualmente, a credibilidade destes meios nos contextos democráticos está cada vez mais sendo posto em dúvida devido às disposições da audiência. Ramonet *apud* Marques (2004, p.22), em suas considerações não otimistas quanto a credibilidade dos conteúdos divulgados nos meios de comunicação, afirma:

> Ceticismo. Desconfiança. Descrença. Eis os sentimentos dominantes dos cidadãos em relação à mídia. [...] Ninguém nega a indispensável

> função da comunicação de massa numa democracia, pelo contrário. A informação continua sendo essencial ao bom andamento da sociedade, e sabe-se que não há democracia possível sem uma boa rede de comunicação e sem o máximo de informações livres. [...] E, não obstante, a suspeita pesa sobre a mídia. [...] Se o público sente muito bem de que uma informação de qualidade depende sua maior ou menor participação na vida cívica – e consequentemente a qualidade da democracia – nem por isso deixou embalar pela lisonja da televisão que lhe prometia informa-lo divertindo-o e apresentando-lhe um espetáculo cheio de ressaltos, apaixonante como um filme de aventuras. Esta contradição inicial se resolve finalmente pela consciência atual que esses cidadãos têm do perigo induzido por uma informação sedutora, que segue, até o paroxismo, a lógica do suspense e do espetáculo. Eles descobrem que informar-se é cansativo e que este é o preço da democracia.

Entretanto, mesmo com tais discussões sobre a ética e validade quanto à credibilidade das informações disseminadas n**o**s meios de comunicação em massa, é importante notar que a Internet traz um diferencial, em relação aos meios de comunicações tradicionais. Sobre o tema, Marques (2004, p. 23) aduz que:

> O diferencial em relação aos meios de comunicação convencionais é que a Internet oferece, através de visita a sites, recebimento de informativos, participação em salas de bate-papo ou assinatura de listas de discussão, acesso direto ao agente e não apenas aos intermediários informativos (usos permitidos pelas diferentes plataformas), ou seja, a capacidade de não mais se estar preso a determinada cobertura, a dado enfoque predominante. Este fenômeno seria possível graças à horizontalidade natural de um sistema de comunicação disposto em rede.

Corroborando a citação acima, Castells (2005, p. 566/567), dispõe que:

> [...] um novo sistema de comunicação que fala cada vez mais uma língua universal digital tanto está promovendo a integração global da produção e distribuição das palavras, som e imagens de nossa cultura como personalizando-as ao gosto da identidades e humores dos indivíduos. As redes interativas de computadores estão crescendo, exponencialmente, criando novas formas e canais de comunicação moldando a vida, e ao mesmo tempo, sendo moldadas por ela.

Portanto, pode-se dizer que a Internet tem força para influenciar a economia e a cultura, passando a ser considerada uma nova morfologia social das sociedades. Castells (2005, p. 566/567) continua:

> [...] Mas a morfologia da rede também é uma fonte de drástica reorganização das relações de poder. As conexões que ligam as redes (por exemplo, fluxos financeiros assumindo o controle de impérios da mídia que influenciam os processos políticos) representam os instrumentos privilegiados do poder. Assim, os conectores são os detentores do poder. Uma vez que as redes são múltiplas, os códigos interoperacionais e as conexões entre as redes tornam-se as fontes fundamentais da formação, orientação e desorientação das sociedades.

Modernamente, o valor da informação escalanou de forma geométrica e a proteção da informação digital, atualmente, é a razão principal pela qual se desenvolvem tantos mecanismos de controle, registro, identificação, como antivírus e *firewall*, por exemplo. Com a Computação em Nuvem não pode ser diferente, pois os desenvolvedores cada vez mais se investem em segurança e sigilo dos dados postos na "nuvem", como forma de proteger o consumidor.

A produção, o sigilo e o armazenamento da informação estão nos centros de estudos, pois há o fenômeno de superdimensionamento da importância e valor da informação, causado, essencialmente, pelo atual estágio tecnológico em que se encontra a sociedade. Com efeito, este superdimensionamento do valor da informação se deu com o surgimento do computador pessoal, que trouxe a necessidade de ofertar produtos e serviços que possibilitassem o acesso e a disseminação de informações. Como exemplo, é importante salientar que foram criados e difundidos

os disquetes, que eram dispositivos que, por seu tamanho e peso diminutos, permitiam a mobilidade e armazenamento da informação neles inserida, fomentando a difusão de conteúdo através de diversos computadores.

Os primeiros *softwares,* que precisavam de mudanças contínuas para tornar a sua fruição satisfatória, traziam aplicações pouco complexas e criadas para um fim específico, como editor de texto. Nesse momento do desenvolvimento da informática, era o usuário do produto que tinha que se adaptar ao computador, procurando estudar os manuais de instrução e apreender a lógica daquela programação, afim de utilizar o computador. Entretanto, com a disseminação e consolidação dos meios informáticos, os produtos e serviços da era digital entraram em um processo de crescente aperfeiçoamento, tornando-se cada vez mais fáceis e intuitivos ao usuário, que, em pouco tempo, saberá manejar o dispostivo ou o programa.

Insta salientar que a personalização dos produtos e serviços da era digital substitui o ultrapassado conceito de generalidade, em que o intuito passa a ser o da conformação daqueles aos gostos e necessidades específicas de seus usuários. Ou seja, o dispositivo ou programa está primeiramente sendo adaptado ao usuário e não este a aquele. Desta maneira, está havendo uma abolição dos produtos pouco complexos na sua forma de fabricação e dos que exigem alta abstração do seu usuário, haja vista que os desenvolvedores de *hardwares e softwares* conseguiram vislumbrar que quanto mais intuitivo e transparente o produto ou serviço ofertado, melhor.

E cada vez mais, as aplicações surgem para ajudar e alavancar outras. Exemplo disto é a tecnologia *Java*[12], da empresa Oracle, que sendo um *software*, permite a fruição de funcionalidades dentro de outros *softwares* tais como os sistemas operacionais IoS (*Apple*), *Android* (Google) e *Windows* (Microsoft). E a computação em nuvem insere-se justamente no já mencionado contexto de tecnologia auxiliada pela tecnologia, ou seja, TAT (*Technology-Aided Technology*).

A personalização da informática promoveu a quebra de um

[12] O Java permite executar jogos, fazer upload de fotos, bater papo on-line, fazer tours virtuais e usar serviços, como treinamento on-line, transações bancárias on-line e mapas interativos. Se você não tiver o Java, muitas aplicações e websites simplesmente não funcionarão." Disponível em: <http://www.java.com/pt_BR/download/whatis_java.jsp>. Acesso em 21 de maio de 2017.

paradigma, e justamente neste movimento de rompimento é que reside o aludido e atual superdimensionamento da informação, como fenômeno intrínseco daquilo que Gilles Lipovestky (2004, p. 53) costuma chamar de "hipermodernidade ou pós do pós-moderno". O citado autor questiona esta exacerbação que atualmente domina os mais diversos aspectos da sociedade: "Hipercapitalismo, hiperclasse, hiperpotência, hiperterrorismo, hiperindividualismo, hipermercado, hipertexto – o que mais não é hiper? O que mais não expõe uma modernidade elevada à potencia superlativa?" (Lipovestky, p. 53)

Jeremy Rifkin (2001, p.25) aponta a transformação social causada pela quebra do paradigma, ao asseverar que:

> A economia física está encolhendo. Se a Era Industrial foi caracterizada pelo acúmulo de capital e de propriedade, a nova era valoriza as formas intangíveis de poder vinculadas a conjuntos de informações e ativos intelectuais. O fato é que os produtos tangíveis, que durante muito tempo foram uma medida da riqueza no mundo industrial, estão se desmaterializando.

A tecnologia da Computação em Nuvem, por evidente, acompanha esta quebra de paradigma, porém, não há um produto ou serviço desta plataforma disponibilizado ao usuário, que não contenha inúmeras opções predefinidas, que existem para facilitar a *interface* homem-máquina (princípio da transparência), bem como para permitir as alterações das configurações da plataforma da Computação em Nuvem, tornando-a uma extensão da personalidade humana.

As tecnologias desenvolvidas como a da Computação em Nuvem são o expoente deste novo patamar que alcançou a sociedade tecnológica, justamente porque foram criadas totalmente inseridas neste contexto de personalização, sendo voltadas à atender de forma flexível e personalizadas a maior gama possível de necessidades de seus usuários. Conforme asseverado por Charles Emmanuel Parchen, Cinthia O. A Freitas e Antônio Carlos Efing (2003, p 158): "O processo capitalista enxergou no uso dos computadores e na evolução da informática, uma ampliação do seu modo de acumulação de riquezas e de poder através do domínio da informação." A informação passou a ser objeto de valoração tal qual uma mercadoria, diga-se de passagem, bastante cara e valiosa.

No livro *O filtro invisível: o que a internet está escondendo de*

você, Eli Pariser (2012) demonstra a existência de uma ideia ilusória e aponta uma trajetória cheia de exemplos para apresentar como a personalização que ocorre na rede por parte de diversos *sites*, como *Google*, *Facebook* e *Amazon*, tem deixado os usuários presos numa bolha invisível, fazendo com que essas empresas exibam apenas aquilo que acham que o navegador deseja ver.

Tem-se que, seja através da venda dos hábitos do consumidor para publicidade dirigida feita por anunciantes que pagam ao provedor de serviços da "nuvem", seja pelo uso das informações em prol da elaboração de produtos e serviços individualizados a um determinado grupo de pessoas ou, ainda, seja até mesmo - em casos de fornecedores mal intencionados - para o uso das informações no cometimento de fraudes e crimes, as informações personalizadas interessam fortemente a prestadores de serviços e comerciantes que, para poderem potencializar seus ganhos, precisam conhecer minúcias dos hábitos e preferências de seus consumidores.

Portanto, não é de estranhar que empresas como o *Google* ou *Facebook* tornaram-se veneradas e seus proprietários, ricos e influentes. Isso porque sob os auspícios da gratuidade dos serviços ofertados, (por exemplo, com o aplicativo de *e- mails* baseado em tecnologia da Computação em Nuvem: *Gmail*) dados de seus consumidores são coletados e vendidos a anunciantes, que fazem ofertas de produtos de forma dirigida, segmentada e extremamente personalizada ao público que utiliza esses serviços, graças à análise das informações pessoais e das predileções constatadas no perfil de cada usuário. A resposta destacada por Pariser está na publicidade, que consiste na maior fonte de renda dessas empresas. Segundo o autor, a questão reside em qual empresa irá retornar mais o investimento realizado:

> As massas de dados acumulados pelo Facebook e pelo Google têm dois propósitos: para os usuários, são a chave para a oferta de notícias e resultados pessoalmente relevantes; para os anunciantes, os dados são a chave para encontrar possíveis compradores. A empresa que tiver a maior quantidade de informações e souber usá-las melhor ganhará os dólares da publicidade. (Pariser. 2012, p. 41)

Neste sentido, assevera Don Tapscott (2000, p.183):

> Quase todas as transações que efetuamos deixam

> um registro eletrônico, criando vastos depósitos de informações sobre nossos padrões de despesas, nossas preferências em termos de produtos, nosso poder de compra e até mesmo dados pessoais como estado civil ou crença religiosa. Um novo negócio de *database marketing* está surgindo deste enorme acúmulo de informações sobre os consumidores – e estes dados são investigados, refinados e analisados com ferramentas tecnológicas poderosas e com técnicas de analise cada vez mais sofisticadas para produzir um quadro surpreendentemente detalhado de cada consumidor.

Prova disso reside na política de uso de dados do *Facebook*, onde se vislumbra que a captação e venda de informações é uma das medidas lucrativas do serviço, conforme consta no termo de utilização do serviço:

> Usamos as informações que temos para melhorar nossos sistemas de publicidade e medição; assim, podemos mostrar anúncios relevantes a você dentro e fora dos nossos Serviços, além de medir a eficácia e o alcance dos anúncios e serviços. Saiba mais sobre a publicidade em nossos Serviços e como controlar a maneira como suas informações são usadas para personalizar os anúncios que você vê.
> …
> **Aplicativos, sites e integrações de terceiros que usam ou são integrados aos nossos Serviços.**
> Quando você usa aplicativos, sites ou outros serviços de terceiros que utilizam ou são integrados aos nossos Serviços, eles podem receber informações sobre suas publicações ou compartilhamentos. Por exemplo, quando você joga com seus amigos do Facebook ou usa os botões Curtir ou Compartilhar em um site, o desenvolvedor do jogo ou o site pode coletar informações sobre as suas atividades no jogo, ou receber o comentário ou link do site compartilhado por você no Facebook. Além disso, quando você baixa ou usa serviços de terceiros, eles podem acessar seu Perfil Público, que inclui seu nome ou número de identificação

> de usuário, faixa etária e país/idioma, lista de amigos, bem como as informações que você compartilha com eles. As informações coletadas por esses aplicativos, sites ou serviços integrados está sujeita aos seus próprios termos e políticas.

O *Facebook* é um serviço baseado em Computação em Nuvem e notabilizou-se por abusar da possibilidade de coletar dados para oferecê-los a anunciantes, tanto que no ano de 2011 foi obrigado a compor com o Governo dos Estados Unidos[13] para poder readequar-se e comprometer-se com práticas mais transparentes e profundas de proteção da privacidade de seus usuários.

Portanto, considerando a importância da informação no contexto da sociedade tecnológica atual, insta salientar que há uma evidente necessidade de fomenter a preservação dos direitos e do equilibrio no pacto contratual do consumidor pessoa física com os fornecedores e investidores da tecnologia da Computação em Nuvem.

No Brasil, com escopo generalístico, visando a proteção do consumidor, foram criadas as políticas públicas do Sistema Nacional de Proteção do Consumo, bem como a Lei 8.078/1990 – Código de Defesa do Consumidor. Não se permite olvidar os progressos alcançados pelo Código de Defesa do Consumidor (Lei Nº 8.078/1990) e pelo Sistema Nacional de Proteção do Consumo (SNPC) que possibilita congregar diferentes entidades estatais e públicas voltadas à análise de questões que tenham repercussão nacional e interesse geral, além de ações relacionadas à Política Nacional de Defesa do Consumidor. Os órgãos componentes deste Sistema, como Procon, são importantes ferramentas de fiscalização e verificação do mercado da computação em nuvem, sendo mecanismos de resposta do Estado, que não pode se furtar à intervenção e regulamentação de tão relevante meio de contratação eletrônica.

---

[13] Facebook and the Federal Trade Commission are nearing a settlement over deceptive practices related to several Facebook features, including its privacy settings, according to two people briefed on the settlement. Under the agreement, Facebook would agree to privacy audits for 20 years, one of the people said. It would also prohibit Facebook from making public a piece of information that a user had originally shared privately on the site without express permission, the person said. MILLER, Claire Cain. F.T.C. Said to Be Near Facebook Privacy Deal. The New York Times. November, 10,2011. Disponível em: <http://www.nytimes.com/2011/11/11/technology/facebook-is-said-to-be-near-ftc-settlement-on privacy.html?_r=0>. Acesso em: 15 de maio de 2017.

A Lei 12.965/2014, conhecida como *Marco Civil E Regulatório Da Internet*, pretende ser o aparato legal a proteger a pessoa interconectada aos meios digitais e que lança mão dos aparatos eletrônicos para os mais diversos aspectos de sua vida. Especificamente não traz a proteção dos dados armazenados em nuvem computacional, porém assevera que "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."

A norma do artigo 11 da Lei nº. 12.965/2014 tem como finalidade a proteção dos dados digitais se as operações de informáticas forem atribuídas a um dispositivo localizado no Brasil. Infelizmente, esta norma não é suficientemente coerente, haja vista a internacionalização da Internet, limitando a utilização do usuário ao território nacional. Um problema que será discutido posteriormente. Se tal cenário persistir, a subsunção fato-norma nunca será perfeita, demandando, por parte do aplicador do direito, a utilização de mecanismos integradores da norma tais como a analogia, os usos, os costumes e a equidade.

CAPÍTULO 3 – PRINCIPAIS ASPECTOS DA LEGISLAÇÃO BRASILEIRA SOBRE USO DA INTERNET E SEUS REFLEXOS NA COMPUTAÇÃO EM NUVEM

A Lei Nº 12.965, de 23 de abril de 2014, conhecida no Brasil como Marco Civil da Internet e, internacionalmente, alcunhada como *The Internet Bill of Rights*, representa uma importante proposta legislativa, sob o aparente enfoque econômico e social da rede mundial de computadores, que se tornou essencial ferramenta de comunicação para os cidadãos, os Estados, em função do seu alcance geográfico, vocação de universalidade.

O Marco Civil da Internet é visceralmente atrelado aos grandes ramos do Direito, quando se trata da proteção dos direitos dos usuários, tanto de viés consumerista quanto relativamente à privacidade; responsabilidade civil dos usuários e dos atores envolvidos com o provimento de serviços, conexões ou aplicações, nos casos de usos indevidos causadores de danos a terceiros ou de perpetração de condutas ilícitas, por exemplo. Logo, temas mais técnicos, como estabilidade e neutralidade de rede, sobressaem-se por causa dos efeitos protetivos dos usuários. Na medida em que o Marco Civil da Internet começa a produzir seus efeitos no mundo jurídico e sobre os atores sociais que operam neste complexo ecossistema no âmbito pátrio, aumenta a necessidade de aprofundar-se a exegese do diploma.

O texto legal é dividido em cinco capítulos, sendo reservado o primeiro aos princípios que devem ser observados no uso da Internet por todos os agentes envolvidos, como a garantia de liberdade de expressão, a proteção da privacidade, por exemplo. O segundo capítulo trata dos direitos e garantias desses usuários, tais como o direito à inviolabilidade da intimidade e ao sigilo das comunicações privadas, entre outros, além do direito à indenização pelo uso indevido. Já, o terceiro capítulo encontra-se dividido em quatro seções, que tratam da neutralidade da rede, da proteção e guarda dos registros, dados pessoais e das comunicações privadas, da responsabilidade pelos danos decorrentes de conteúdo gerado por terceiros, além da requisição judicial de registros.

A atuação do Poder Público, com o estabelecimento de diretrizes para seus entes, restou prevista no quarto capítulo, a eles incumbindo promover o desenvolvimento da internet no país através de mecanismos de governança multiparticipativa, buscando sempre a racionalização da gestão, da expansão e uso da internet, além de garantir a interoperabilidade tecnológica dos serviços de governo eletrônico entre os diversos setores públicos. O quinto capítulo destinou-se às disposições

finais, tais como o controle parental de conteúdo, a inclusão digital, a forma de exercício em juízo dos direitos e interesses estabelecidos nessa lei, além da *vacatio legis*, fixada em sessenta dias após sua publicação.

Os princípios fundamentais do Marco Civil da Internet são enunciados no Art. 2º e seus seis incisos[14]. Já a redação do Parágrafo Único do Art. 3º[15] adverte que os princípios legalmente enumerados ali não se constituem uma lista exaustiva, tendo em vista que não excluem outros princípios previstos no ordenamento ou em tratados internacionais pertinentes.

A ausência de taxatividade principiológica não conduz a uma insegurança jurídica, pois a generalidade traz um maior alcance da cobertura normativa da relações jurídicas e negociais tratadas na Internet, perfazendo-se a um análise sistêmica de um conjunto harmônico e funcional de acordo com as técnicas jurídicas mais apropriadas.

Os princípios fundantes do Marco Civil da Internet são norteadores de conduta tanto no âmbito doméstico quanto no internacional, aplicáveis a todos os atores sociais envolvidos com a Internet.

O primeiro fundamento do Marco Civil da Internet, liberdade de expressão, é lastreado no Art. 5º, IV da Constituição Federal, sendo por ele disciplinado quanto à vedação ao anonimato. Outros incisos do Artigo 2º da Lei 12.965 são transcrições idênticas dos princípios constitucionais, a saber: cidadania (Art. 1º, II, CF); direitos humanos (Art. 4º, II, CF); livre iniciativa (Art. 1º, IV, CF); livre concorrência e defesa do consumidor (Art. 170, IV e V, CF). Esta reiteração de princípios constitucionais tem o condão de sujeitar as relações e a conduta dos atores sociais na Internet a vários ramos do direito, sem maiores questionamentos, destacando-se destes os Direitos Humanos; Direitos do Consumidor e Direito da Ordem Econômica e Financeira.

---

[14] Art. 2º A disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como:
I - o reconhecimento da escala mundial da rede;
II - os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais;
III - a pluralidade e a diversidade;
IV - a abertura e a colaboração;
V - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
VI - a finalidade social da rede.

[15] Art. 3º - 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.

Dentre os princípios do artigo 2º da Lei 12.965, é necessário destacar o que consta do inciso I, que introduz o princípio do "reconhecimento da escala mundial da rede", decorrente da própria natureza da Internet, que congrega atualmente cerca de 3,7 bilhões de usuários, a saber 50% (cinquenta por cento) da população mundial, com potencial de atingir todos os povos, nações, idiomas, dialetos e culturas na medida em que o acesso segue se massificando.[16] O reconhecimento da natureza global da Internet proporciona substantivamente maior extensão aos demais princípios enumerados no Art. 2º, notadamente aos enunciados nos incisos III e IV: pluralidade, diversidade, abertura e colaboração. O reconhecimento na natureza global da rede e de sua governança não deve ser considerado como uma afronta à soberania nacional, mas um necessário e saudável exercício de ponderação, realizado no melhor interesse do País.

No que tange às garantias, o Marco Civil da Internet não faz uma estrita entre os direitos e garantias, todavia, pela sua dicção, é possível considerar que o Art. 3º enumera as garantias providas pelo Estado Brasileiro aos atores sociais. Sem embargo da distinção, direitos e garantias fundamentais têm natureza de princípios jurídicos.

O Art. 3º, I estabelece que a liberdade de expressão é garantida nos termos da Carta Magna, que, implica vedação ao anonimato. O inciso II garante a proteção da privacidade, cuja violação é ato ilícito nos termos dos Arts. 186 e 187 do Código Civil, ensejando reparação de danos. O inciso III garante a proteção de dados pessoais, que atribui aos provedores pertinentes a responsabilidade no tocante aos registros de conexão e acesso às aplicações, aos dados pessoais e ao conteúdo das comunicações, conforme se vê na Seção II do diploma legal. O inciso IV dispõe sobre a preservação e garantia da neutralidade de rede.

O inciso V determina a preservação da estabilidade, segurança e funcionalidade da rede. No Brasil, a Internet deve ser entendinda como um esforço coletivo e colaborativo empreendido por fornecedores de telecomunicações, provedores de acesso e a Anatel - Agência Nacional de Telecomunicações. Em razão desta faina coletiva e interdependente, entende-se que o disposto neste inciso trata especificamente da rede, pois se entende por estabilidade o funcionamento contínuo dentro dos padrões de desempenho esperados. A segurança da rede relaciona-se com a

[16] Estudo feito pela instituição *We Are Social* e *Hootsuite* que revela dados interessantes: o Digital in 2017 Global Overview, disponível em <https://wearesocial.com/special-reports/digital-in-2017-global-overview>, acesso em 20 de julho de 2017.

inviolabilidade das informações transmitidas e que sejam imunes a tentativas de invasão e de ataques externos que provoquem interrupção do serviço. A inviolabilidade dos dados não é uma característica originária da grande rede, mas a sua proteção pode ser implementada com protocolos seguros que empregam técnicas de criptografia, tais como, IPSec e SSL. A funcionalidade da rede consiste na transmissão de pacotes de dados desde o terminal originador até o destino final, passando por pontos intermediários de roteamento. O inciso V estabelece o modo pelo qual deve-se preservar a estabilidade, a segurança e a funcionalidade da rede, destacando-se a referência aos padrões internacionais.

A preservação da estabilidade, segurança e funcionalidade da rede é um trabalho coletivo e colaborativo, desempenhado por atores públicos e privados. É necessário que este sistema seja fortalecido e que se evite que a regulamentação do diploma legal se constitua em um fator inibidor da evolução tecnológica, em função de serem intimamente relacionadas com a adoção de novos padrões e práticas internacionais. Desta maneira, o Comitê Gestor da Internet (CGI) e a Anatel devem se esmerar no esforço de acompanhar a dinâmica de introdução de novas tecnologias e de fiscalizar a adoção, por parte dos atores envolvidos, de arquitetura de rede aberta e distribuída e de padrões internacionais abertos que garantam a interoperabilidade e a livre circulação das comunicações.

Os incisos VI e VII referem-se responsabilização dos agentes de acordo com suas atividades e preservação da natureza participativa da rede, respectivamente. A exegese destes dispositivos não detém maiores questões, porém é importante frisar que a lei se limita a estabelecer penalidades exclusivamente civis, não abrangendo a responsabilização penal dos agentes, os quais serão responsabilizados por atividade exercida, ou seja, o usuário será punido como usuário; o provedor como provedor.

A liberdade dos modelos de negócio promovidos na Internet preconizada no Inciso VIII do Art. 3º do Marco Civil da Internet dá enfoque na constante mutabilidade dos modelos de negócios proporcionada pela rede mundial, a fim de impulsionar a continuidade da inovação e da difusão de novas tecnologias. É cediço que a Internet proporcionou significativos avanços em novos modelos de negócio, pois em um passado recente, o mercado de *software* era lastreado na comercialização de licenças perpétuas. E, hoje, observa-se que o provimento de *software* está sendo comercializados mediante mensalidades, ou por provimento de aplicações gratuitas *on line*, subsidiadas por receitas de propaganda e *marketing*.

Os princípios enunciados no Art. 4º[17] do Marco Civil da Internet possuem um viés finalístico, sendo, portanto, altamente convergentes com a natureza de mandamentos de otimização propugnada pelo jurista e filósofo Robert Alexy. A distinção entre regras e princípios está no âmbito das diferenciações teorético-estruturais, sendo a mais importante para a resolução de problemas que envolvem restrições de direitos fundamentais:

> O ponto decisivo na distinção entre regras e princípios é que *princípios* são normas de ordenam que algo seja realizado na maior medida possível dentro das possibilidades jurídicas e fáticas existentes. Princípios são, por conseguinte, *mandamentos de otimização*, que são caracterizados por poderem ser satisfeitos em graus variados e pelo fato de que a medida devida de satisfação não depende somente das possibilidades fáticas, mas também das possibilidades jurídicas. O âmbito das possibilidades jurídicas é o determinando pelos princípios e regras colidentes. Já as regras são normas que são sempre ou satisfeitas ou não satisfeitas. Se uma regra vale, então, deve se fazer exatamente aquilo que ela exige; nem mais, nem menos. [...] Isso significa que a distinção entre regras e princípios é uma distinção qualitativa e não uma distinção em grau. Toda norma é ou uma regra ou um princípio. (ALEXY, 2015, p. 90/91)

Além de serem princípios em sua própria natureza, os incisos do Art. 4º consubstanciam-se, também, como critérios a serem empregados no sopesamento de princípios, tanto na atividade jurisdicional, quanto de forma ex ante em atividade legiferante.

Resta evidente que, no âmbito do Marco Civil da Internet, o critério teleológico é prestigiado com quatro princípios de disciplina de uso, que,

---

[17] Art. 4º A disciplina do uso da internet no Brasil tem por objetivo a promoção:
I - do direito de acesso à internet a todos;
II - do acesso à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos;
III - da inovação e do fomento à ampla difusão de novas tecnologias e modelos de uso e acesso; e
IV - da adesão a padrões tecnológicos abertos que permitam a comunicação, a acessibilidade e a interoperabilidade entre aplicações e bases de dados.

para além da relevância ínsita per se, os quatro princípios enunciados no Art. 4º materializam critério adequado para discernir o peso relativo entre os vários princípios colidentes observados no seio do diploma da grande rede.

A promoção do direito de acesso à Internet a todos enunciado no Inciso I do Art. 4 pode se desdobrar em dois aspectos: (i) o aspecto formal do direito de acesso, que veda qualquer prática discriminatória, seja por qualquer pretenso fundamento, e (ii) o aspecto material da viabilização econômica do acesso, oferecido no seio de uma sociedade marcada por significativas diferenças de poder aquisitivo entre as classes.

Com efeito, a rede mundial tem grande função social, uma vez que é essencial que seja acessada por todos. Quanto maior a massificação da Internet, não apenas a sua disponibilização potencial, mas do efetivo uso e fruição por parte de todos os brasileiros, maior o benefício em termos de desenvolvimento social e consequentemente econômico, o que implica o acesso à rede e disponibilidade de dispositivo para dela fazer uso.

O inciso II assevera que a regulamentação legal deve impor o livre e irrestrito acesso aos conteúdos disponibilizados através da rede mundial, de forma completa e desimpedida, quando relacionados à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos.

No que tange ao inciso III, é possível inferir que a promoção da inovação e do fomento à ampla difusão de novidades tem um condão principiológico de direito econômico por excelência, com características inovadoras e de universalização de serviço público. Primeiramente, em se tratando de um objetivo promocional e de fomento, o princípio se constitui em um mandamento positivo, determinando que o Estado busque ativamente a consecução de objetivos através de instrumentos de ação, com desdobramentos na esfera social. Por outro lado, este princípio se posiciona como um critério de limitação a ser considerado em face a outros princípios, pois coíbe normativos que possam ter a finalidade de inibir a inovação ou de restringir a difusão de novos modelos de uso e de acesso.

Quanto ao Art. 4º, Inciso IV, que dispõe sobre a adesão a padrões tecnológicos abertos que permitam a comunicação, a acessibilidade e a interoperabilidade entre aplicações e bases de dados, é clara a finalidade de impulsionar acessibilidade no tocante ao uso de tecnologias que viabilizam a conexão de Internet, de pessoas com deficiência, por exemplo, que pode ser visto como um importante instrumento viabilizador de inserção no mercado de trabalho, pot que permite que este seja feito remotamente, a partir da própria residência do empregado com

deficiência, proporcionando realização pessoal e profissional, bem como melhoria da condição financeira do individuo. Ademais, há menção à interoperabilidade, que surgiu da necessidade de ligar operacionalmente ambientes com redes heterogêneas, como uma necessidade de articulação sistêmica para o usuário.

3.1 – Princípio da Neutralidade da Rede (Art. 3º, IV e Art. 9º da Lei 12.965/2014)

Historicamente, a problemática da neutralidade da rede emergiu nos Estados Unidos da América, na década de 1990, quando ocorreram várias denúncias sobre bloqueios ou atrasos propositais de fluxo de dados de forma indiscriminatória realizados por operadores de telecomunicação contra certos provedores de Internet. No Brasil, a neutralidade polarizou o debate durante a tramitação do projeto de Lei do Marco Civil da Internet, terminando por ser positivado nos artigos 3º e 9º.

O Marco Civil da Internet conceitua Neutralidade de Rede, no Art. 9º, de uma forma técnica restritiva, o que se demonstra, na prática, um importante desafio ao intérprete do direito, quando confrontado com a constante evolução tecnológica:

> Art. 9º **O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação**. (destaque do autor)

Possíveis exegeses jurídicas estritas têm o condão de inibir a inovação tecnológica da Internet. É precisamente em relação à tais riscos interpretativos que a hermenêutica com base no sopesamento de princípios se apresenta como poderosa ferramenta.

A redação do *caput* do Art. 9º ao informar que se deve "tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação", aparenta ser inspirada nas famosas características do protocolo IP, que são a base do serviço de Internet atualmente disponibilizado ao público em geral.

O protocolo de comunicação IP foi criado em 1980 com duas políticas essenciais de transmissão de pacotes: (a) o encaminhamento do pacote pela rota mais favorável e (b) a entrega de pacotes baseada em melhores esforços (*best effort*), porém sem garantia de entrega ao

destinatário. Os pacotes são tratados pelo protocolo IP sem distinção de conteúdo ou priorização relativa. Em 1999, foi publicada a primeira versão do protocolo MPLS, que, operando em conjunto com o protocolo IP, permite a criação de Classes de Serviço, diferenciando pacotes e possibilitando a alocação específica de banda para cada classe, de modo a obter Qualidade de Serviço (QoS) adequada aos requisitos das diversas aplicações que se comunicam através da rede.

Em 2002, os protocolos IntServ[18] e DiffServ[19] foram introduzidos, aumentando as possibilidades para implementação de QoS. Os serviços empregando MPLS foram amplamente disponibilizados pelas operadoras de telecomunicações e se tornaram dominantes nas redes empresariais. Entretanto, a implementação de QoS não foi estendida à Internet. O aumento do poder de processamento dos *hardwares* de rede trouxe novas técnicas de desenvolvimento para a priorização de pacotes, algumas com base no exame do conteúdo para escolha do tipo de aplicação trafegada.

A exegese sistêmica dos parágrafos 1º e 2º do Art. 9º traz a ideia de que os pacotes devem ser tratados igualitariamente, porém é pacífico em direito que só há isonomia material quando os desiguais são tratados desigualmente visando a justiça.

O Princípio da Neutralidade de Rede impõe que a rede deve se apresentar neutra, isto é, não interferente, perante o usuário e suas escolhas. Em sua essência, este princípio é um norteador da relação dos provedores, que, isolada ou agregadamente, materializam o serviço de Internet, com todos os demais atores sociais, que a utilizam para realizar uma atividade específica de seu interesse. Assim, não é possível afirmar que o Princípio da Neutralidade de Rede seja um dispositivo jurídico de natureza técnica exclusivamente, pois, em razão de sua importância, deve ser considerado como um parâmetro de condutas imponíveis aos atores envolvidos com a rede, ou seja, àqueles que têm alguma participação no provimento da infraestrutura e dos serviços que viabilizam a troca de informações, notadamente, os prestadores de serviço de Internet devem minimamente respeitar a neutralidade da rede.

---

[18] O modelo de Serviços Integrados (*Integrated Services – IntServ* Este modelo de qualidade de serviço é caracterizado essencialmente pela reserva de recursos (largura de banda, atraso e jitter), antes do estabelecimento da comunicação. (Alves Jr., Nilton. 2000, p.4);

[19] É baseado no tratamento diferenciado de classes, podendo manipular diferentes tipos de classes de varias maneiras dentro da rede. (Alves Jr., Nilton. 2000, p.4)

Compreender os desdobramentos do Princípio da Neutralidade da Rede, inclusive à luz de outros princípios do Marco Civil da Internet, inicia-se pela conscientização das múltiplas naturezas da Internet, relevantes para o direito. Para Sérgio Paulo Galindo (2016, p. 49/50), a Internet possui as múltiplas naturezas de:

> a. **Natureza de Ecossistema:** A Internet é um ecossistema de atores sociais conectados, incluindo, usuários, provedores de Internet, provedores de aplicação, provedores de serviço, provedores de conteúdo e provedores de mercadoras por intermédio de comércio eletrônico. Com o advento da nova onda tecnológica denominada Internet da Coisas, dispositivos inteligentes conectados, incluindo sensores e atuadores, passam a ser parte relativamente autônoma do ecossistema.
> b. **Natureza de Espaço Público:** A Internet é um espaço público, no qual usuários e provedores de aplicação, de conteúdo, de serviços ou de mercadorias estabelecem relações jurídicas com os provedores de Internet para "adentrar" à rede e exercer os seus direitos.
> c. **Natureza de Rede de Comunicação:** A Internet é uma rede de comunicação, que transporta pacotes de dados de acordo com certas características técnicas e de modo não discriminatório. Neste espaço se materializa o Princípio da Neutralidade e os Princípios da Economia da Inovação da Internet.
> d. **Natureza de Espaço Mercantil:** A Internet é um mercado no qual os atores sociais conectados estabelecem, entre si, relações jurídicas visando a fruição da utilidade econômica pretendida.

Após a compreensão da multiplicidade de naturezas da Internet, em que em todas há o elemento mínimo de liberdade, é possível extrair da norma legal do Marco Civil da Internet algumas características insítas ao Princípio da Neutralidade da Rede, no que concerne à relação entre os provedores de Internet e os contratantes do serviço. As características são: a) Transparência dos termos e condições do serviço de Internet; b) Isonomia nos termos e condições ofertados; c) Liberdade de escolha do contratante; d) Não interferência do provedor de serviço de Internet na efetiva prestação do serviço; e) Não prejudicialidade em relação às

características do serviço de qualquer contratante; f) Inviolabilidade das comunicações circulantes na Internet, por parte dos provedores.

Transparência dos termos e condições do serviço de Internet: é o pressuposto principal da sua neutralidade, na medida em que qualquer possível obscuridade sobre os termos, condições ou características pelas quais se dá a prestação do serviço de Internet a macula e desnatura. A máxima em tela está positivada no diploma da rede nas garantias enumeradas nos incisos VI e VIII do Art. 7º da Lei 12.965/2014.

Isonomia nos termos e condições ofertados: Esta característica não significa igualdade, mas sim tratamento desigual aos desiguais, pois os serviços ofertados por um certo prestador de Internet podem ter diferentes características técnicas e comerciais, e podem também estabelecer pré-requisitos específicos e distintos. Logo, é legítimo que um serviço de maior velocidade tenha um preço superior a um outro de menor banda. Entretanto, uma vez liberada ao público em geral, uma certa oferta deve necessariamente ser acessível a todo e qualquer pretendente a contratante, exceto se a prestação do serviço for impossibilitada pelas condições de infraestrutura da localidade na qual o contratante pretenda instalar ou usar o serviço, por exemplo.

Liberdade de escolha do contratante: Possui duas facetas correlatas, mas distintas. A primeira é a efetiva concretização da proposta do fornecedor, no tocante às características do serviço contratado, frente ao efetivamente prestado, uma decorrência natural do princípio *pacta sunt servanda*. O prestador do serviço de Internet não pode inovar os serviços, afastando-se das condições acordadas com o contratante, sem a aquiescência deste. Desta maneira, o prestador não está adstrito a se manter prestando o serviço previamente contratado, mas tampouco pode alterar as suas características sem antes informar o contratante e obter dele a autorização para mudar a efetiva prestação. Poder-se-ia inferir que alterações contratuais realizadas em benefício do consumidor/usuário, por exemplo, como aumento da velocidade de concexão, prescindiriam de sua aprovação. Entretanto, tal conduta não é lícita, pois a informação clara e detalhada, corolário da transparência, deve ser instrumentalizada pelo fornecedor. É por intermédio da transparência e do respeito às escolhas do contratante da Internet que a confiança entre os atores sociais da Internet existe, numa verdadeira prova de boa-fé mútua. A segunda faceta da liberdade de escolha diz respeito ao uso do serviço contratado, pois nem sempre o usuário da Internet é o contratante do plano. Em ambiente familiar, por exemplo, um plano de Internet é contratado pelo ente familiar e é usado de forma compartilhada pelos membros da família, ou, em casos de planos móveis, que compartilham franquias de dados.

Assim, a liberdade de escolha dos diversos usuários que compartilham um plano de serviço de Internet está vinculada e adstrita às necessidades definidas pelo contratante, uma vez que os pais podem contratar ferramentas de controle parental, restringindo o acesso de seus filhos civilmente incapazes a certos portais e tipos de conteúdo, por exemplo.

Assim, dentro das fronteiras estabelecidas pelas restrições contratadas, deve o usuário, mesmo restritoa alguns *sites* ou portais, gozar de plena liberdade no tocante à informação que desejar acessar, uma vez que firmada a contratação, mediante o livre exercício das escolhas do contratante com base na informação transparentemente prestada pelo provedor, o serviço deve ser fielmente prestado.

Não interferência do provedor de serviço de Internet na efetiva prestação do serviço: A não interferência é a consubstanciação da neutralidade de rede no cotidiano da prestação do serviço que deve ser livre de práticas discriminatórias, como, por exemplo: bloqueio de acesso a páginas ou aplicações, degradação injustificada de tráfego ou de outros aspectos de desempenho da rede e outras condutas congêneres. Todavia, é seguro afirmar que, em razão da inteligência do Art. 9º, §1º, a degradação de desempenho da conexão é aceitável em certas circunstâncias, que se justificam pelo princípio da preservação da estabilidade, segurança e funcionalidade da rede, estatuído no Art. 3º, V. Dessa forma, o que fere a neutralidade da rede é a interferência arbitrária e injustificável no serviço prestado, que o faça destoar das características esperadas pelo usuário.

Não prejudicialidade em relação às características do serviço de qualquer contratante: implica que as escolhas de um contratante não devem influenciar as escolhas dos demais contratantes do mesmo serviço de Internet ou prejudicar o serviço usufruído por nenhum outro contratante. O prestador de serviço de acesso à Internet deve garantir que o serviço seja prestado tal como contratado, não podendo escudar-se em alegações fundadas em limitação de infraestrutura. Por exemplo, um prestador introduz uma nova oferta com velocidade máxima de 10 Mbps em certa vizinhança na qual seus assinantes contrataram acessos com a antiga velocidade máxima de 2 Mbps. Este prestador tem a obrigação de preparar a infraestrutura de tal sorte que o aumento de velocidade daqueles que venham optar pelo serviço mais veloz, não degrade o desempenho daqueles que decidirem permanecer com a velocidade mais baixa. A observância da não prejudicialidade possibilita ao provedor ampla liberdade de desenvolvimento e oferta de novos planos de serviços, em consonância com o que se espera da dinâmica da própria Internet.

Inviolabilidade das comunicações circulantes na Internet, por parte dos provedores: Ao prestador do serviço Internet é vedado, como regra geral, exercer atividade cognoscente sobre os dados trafegados na Internet. A inviolabilidade da informação circulada na Internet é obrigação de não fazer imponível ao prestador do serviço de Internet, qual seria de abster-se de analisar os dados trafegados, visando extrair informação, obrigação. Está tipificada no Art. 7º, incisos I, II e III do Marco Civil da Internet, *in verbis:*

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
> I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
> II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
> III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial.

Por outro lado, a inviolabilidade não deve ser considerada como um conceito absoluto, mas sim um direito disponível do contratante, passível de relativização, sempre que em seu benefício e por intermédio de sua decisão plenamente informada. Exemplo da possibilidade de mitigação da inviolabilidade consta das aplicações de antivírus e *antispam*, os quais, na medida em que examinam todas as mensagens endereçadas ao usuário, analisam e varrem todo o conteúdo das mensagens, executam atividade cognoscente específica de identificação de códigos maliciosos, com a finalidade de proteger o usuário. Desde que devidamente autorizadas pelo contratante, no pleno e informado exercício de sua liberdade de escolha o afastamento da inviolabilidade é não somente justificável, mas também desejável para evitar danos.

Por fim, diante das características da Neutralidade da Rede, é possível estabelecer que esta regra é um limite mínimo a ser observado por todos os provedores de Internet. O disposto no Art. 9º estabelece um padrão de serviço mínimo, cuja execução abaixo do contratado gera uma violação irremediável do Princípio da Neutralidade de Rede estatuído no Art. 3º, IV, do Marco Civil da Internet. Todavia, este padrão básico pode ser violado em favor dos contratantes, respeitadas as características e desdobramentos exegéticos do Princípio da Neutralidade de Rede.

3.2 – A incidência tributária dos Serviços em Nuvem

A rede mundial de computadores oferece os mais diversos produtos, como compra de bens móveis com entrega domiciliar, bem como os variados serviços, como *e-mail*, armazenamento de dados em nuvem, transmissão audiovisual, transações bancárias etc. O potencial de crescimento da utilização da Internet para anunciar, vender e entregar bens e serviços obriga tributaristas de todo o mundo a considerarem todas as ramificações desses novos métodos de negociação e suas repercussões na esfera tributária.

Nos Estados Unidos da América, as autoridades tributárias de vários Estados consideram os provedores de serviços da internet como prestadores de serviços, tais como serviços de informação; processamento de dados, telecomunicações, *marketing*. Atualmente, existiu uma norma jurídica chamada de *Internet Tax Freedom Act (*Ato de Isenção de Impostos na Internet), que foi implementada em 1º de outubro de 1998 até 21 de outubro de 2001, por decisão do Congresso americano, que alcança os consumidores e comerciantes envolvidos em transações vinculadas à internet, protegendo-os de eventual taxação incidente sobre comércio e serviços efetivados exclusivamente via internet, os quais não tenham equivalente *off line*. Tal moratória também declarou, por certo tempo, que a internet deveria se caracterizar como zona não-tributável.

Este Ato de Isenção de Impostos na Internet foi criado porque o Congresso entendeu haver necessidade de uma pausa que conferisse à internet oportunidade para crescer e, ao mesmo tempo, propiciar uma reflexão substancial e madura acerca da melhor política a ser adotada com respeito à taxação na internet. Antes da implementação do Ato de Isenção, em outubro de 1988, vários estados vinham taxando o acesso à internet e, virtualmente, todos os estados impuseram critérios de taxação, tanto nas classes de bens como nas de serviços oferecidos, via internet, semelhantes aos aplicados em relação a catálogos de vendas tradicionais.

Preocupações consistentes surgiram, especialmente no que toca aos efeitos que a Internet, livre de impostos, poderia causar aos comércios locais. Assim, formou-se um consenso, no sentido da necessidade da implementação de regras que visassem à neutralidade no tratamento conferido ao comércio eletrônico e ao tradicional, não eletrônico. A preocupação dos Estados, naquele país, persiste ainda na questão das transações eletrônicas, via Internet, e nas reduções de arrecadação, bastante significativas, de impostos.

No Brasil, a Constituição Federal, em seu art. 155, inciso II, preleciona a tributação dos chamados “serviços de comunicação”:

> Art. 155 – Compete aos Estados e ao Distrito Federal instituir impostos sobre:
>
> (...)
>
> II – operações relativas à circulação de mercadorias e sobre prestações de serviços de transporte interestadual e intermunicipal e de comunicação, ainda que as operações e as prestações se iniciem no exterior.

Efetivamente, o legislador não se preocupou em abranger qual seria o conteúdo da comunicação, mas o serviço que a permite, isto é, o veículo que viabiliza a comunicação entre as pessoas. E este veículo pode ser uma carta, um jornal, uma televisão, um rádio, um telefone, bem como a própria internet. Como visto acima, o texto constitucional é expresso, em afirmar que o Imposto sobre a Circulação de Mercadorias e Serviços deve incidir sobre as operações relativas à circulação de mercadorias e sobre os serviços de transporte interestadual e intermunicipal e de comunicações.

O serviço de comunicação apresenta, como característica fundamental, o oferecimento do equipamento capaz de fazer com que a comunicação ocorra, isto que, que a informação ou a mensagem possa ser transmitida e recebida.

De enfatizar desde logo que há distinção entre a comunicação e o serviço de comunicação. Hugo de Brito Machado (2001, p.89) ressalta o seguinte: "na publicidade, por exemplo, quem torna público sem dúvida está comunicando. Está fazendo comunicação. Mas, a comunicação, em si mesma, não é que sofre a incidência do ICMS. Tal incidência é sobre o serviço de comunicação."

E continua o autor mais adiante:

> É claro que a palavra comunicação tem sentido amplíssimo, no qual se encartam as informações, as manifestações de idéias e pensamentos em geral, por palavras, gestos e por qualquer outro meio, ainda que se trate de transmissão apenas unilateral. Não é neste sentido, porém, que a palavra está no texto do art. 155, inciso II, da Constituição Federal. (Machado, 2001, p.89)

O ilustre constitucionalista, o Prof. Celso Ribeiro Bastos (2001, p. 73), em estudo realizado na matéria, faz distinção entre a atividade de comunicação e o serviço de comunicação, de modo que a primeira seria a que ocorre diretamente entre os interlocutores, relacionada à livre manifestação do pensamento, enquanto que a segunda visaria apenas a proporcionar o meio para que ocorra a comunicação, de forma que seria sobre este segundo aspecto que incidiria a tributação do Imposto sobre Circulação de Mercadorias e Serviços (ICMS).

Há, assim, por parte desses provedores, a prestação de serviços de comunicação, o que nos leva, por conseguinte, ao entendimento de que ocorre, naquela prestação, fato gerador do Imposto sobre a Circulação de Mercadorias e Serviços – ICMS.

O serviço prestado pelos provedores de acesso à Internet afigura-se muito mais como serviço de valor adicionado, conforme o prescrito no art. 61 da mesma Lei Geral das Telecomunicações, que ensina que esta é a atividade que acrescenta, a um serviço de telecomunicações que lhe dá suporte e com o qual não se confunde, novas utilidades relacionadas ao acesso, armazenamento, apresentação, movimentação ou recuperação de informações, não constituindo serviço de telecomunicações.

Os provedores de acesso não realizam o transporte de sinais de telecomunicações. Eles somente fornecem os meios de acesso e não a comunicação, eis que realizam serviço de valor adicionado. Valor adicionado, segundo o artigo 61[20], da Lei nº 9.472, de 16 de julho de 1997, que dispõe sobre a organização dos serviços de telecomunicações.

Assim, sob esta ótica, o serviço que prestam os provedores é mero serviço auxiliar, adicional, no dizer da lei das telecomunicações, de modo que apenas a linha telefônica é tributada pelo ICMS, e não o serviço do provedor em si. Esta controvérsia ainda não foi decidida pelo Judiciário, apesar da tributação por alguns entes federais.

---

[20] Art. 61. Serviço de valor adicionado é a atividade que acrescenta, a um serviço de telecomunicações que lhe dá suporte e com o qual não se confunde, novas utilidades relacionadas ao acesso, armazenamento, apresentação, movimentação ou recuperação de informações.

§1º Serviço de valor adicionado não constitui serviço de telecomunicações, classificando-se seu provedor como usuário do serviço de telecomunicações que lhe dá suporte, com os direitos e deveres inerentes a essa condição.

§2º É assegurado aos interessados o uso das redes de serviços de telecomunicações para prestação de serviços de valor adicionado, cabendo à Agência, para assegurar esse direito, regular os condicionamentos, assim como o relacionamento entre aqueles e as prestadoras de serviço de telecomunicações.

Uma recente controvérsia sobre a tributação dos serviços e produtos na Internet reside na incidência do Imposto sobre Serviços à empresas disponibilização, sem cessão definitiva, de conteúdo de áudio, vídeo, imagem e texto.

O Imposto Sobre Serviços de Qualquer Natureza (ISS) é um tributo que os Municípios e o Distrito Federal podem exigir de prestadores de determinados tipos de serviços. Sua instituição possibilita, *prima facie*, saber que o imposto poderá ser exigido quando ocorrer prestação de serviço e que o seu montante deverá ser proporcional ao valor do serviço. Mas é tormentoso saber qual Município poderá exigir o imposto quando o prestador de serviços for domiciliado num e prestar serviço noutro.

A competência dos Municípios para exigir ISS tem fundamento legal no artigo 156 da Constituição e na Lei Complementar 116 de 2003.

O artigo 156 da Constituição dispõe que compete aos Municípios instituir imposto sobre serviços de qualquer natureza, não compreendidos dentre os discriminados no inciso II do seu artigo 155, conforme forem definidos por lei complementar (inciso III do artigo 156). O parágrafo 3º do referido artigo 156 dispõe que cabe à lei complementar fixar as suas alíquotas máximas e mínimas (inciso I), excluir da sua incidência exportações de serviços para o exterior (inciso II) e regular a forma e as condições como isenções, incentivos e benefícios fiscais serão concedidos e revogados (inciso III).

Na verdade, a Constituição não institui tributos, mas outorga competências tributárias para a União, para os Estados e o Distrito Federal e para os Municípios. Cada competência tributária outorgada pela Constituição é limitada através da descrição de uma regra matriz. Pois, o exercício da referida competência, isto é, a instituição do tributo através de atividade legislativa, é limitada pela regra matriz estipulada pela Constituição. A regra matriz do ISS está formulada no artigo 156 da Constituição Federal.[21]

---

[21] Art. 156. Compete aos Municípios instituir impostos sobre:
I - propriedade predial e territorial urbana;
II - transmissão "inter vivos", a qualquer título, por ato oneroso, de bens imóveis, por natureza ou acessão física, e de direitos reais sobre imóveis, exceto os de garantia, bem como cessão de direitos a sua aquisição;
III - serviços de qualquer natureza, não compreendidos no art. 155, II, definidos em lei complementar. (Redação dada pela Emenda Constitucional nº 3, de 1993) (grifo nosso)
IV - (Revogado pela Emenda Constitucional nº 3, de 1993)

Segundo o entendimento que se consolidou no Superior Tribunal de Justiça, a competência para arrecadar o ISS é do município onde o serviço é prestado, apesar do que dispõe o artigo 12 do Decreto-lei 406 de 1968.

O principal fundamento do entendimento foi a impossibilidade de prevalência de disposições do decreto-lei frente ao princípio constitucional da autonomia municipal, isto é, não é defeso à legislação infraconstitucional determinar que fato ocorrido em um município seja submetido à lei tributária de município diverso. Com outras palavras, o STJ privilegiou o princípio da territorialidade das normas tributárias.

A partir de julho de 2003 a Lei Complementar 116 instituiu novas regras para determinação do local de prestação de serviços. Segundo aquela lei complementar o serviço considera-se prestado e o imposto devido no local do estabelecimento prestador ou, na falta do

---

§1º Sem prejuízo da progressividade no tempo a que se refere o art. 182, § 4º, inciso II, o imposto previsto no inciso I poderá: (Redação dada pela Emenda Constitucional nº 29, de 2000)

I – ser progressivo em razão do valor do imóvel; e (Incluído pela Emenda Constitucional nº 29, de 2000)

II – ter alíquotas diferentes de acordo com a localização e o uso do imóvel. (Incluído pela Emenda Constitucional nº 29, de 2000)

§2º O imposto previsto no inciso II:

I - não incide sobre a transmissão de bens ou direitos incorporados ao patrimônio de pessoa jurídica em realização de capital, nem sobre a transmissão de bens ou direitos decorrente de fusão, incorporação, cisão ou extinção de pessoa jurídica, salvo se, nesses casos, a atividade preponderante do adquirente for a compra e venda desses bens ou direitos, locação de bens imóveis ou arrendamento mercantil;

II - compete ao Município da situação do bem.

§3º Em relação ao imposto previsto no inciso III do caput deste artigo, cabe à lei complementar: (Redação dada pela Emenda Constitucional nº 37, de 2002)

I - fixar as suas alíquotas máximas e mínimas; (Redação dada pela Emenda Constitucional nº 37, de 2002)

II - excluir da sua incidência exportações de serviços para o exterior. (Incluído pela Emenda Constitucional nº 3, de 1993)

III – regular a forma e as condições como isenções, incentivos e benefícios fiscais serão concedidos e revogados. (Incluído pela Emenda Constitucional nº 3, de 1993)

§4º (Revogado pela Emenda Constitucional nº 3, de 1993)

estabelecimento, no local do domicílio do prestador. Entretanto estipulou vinte e duas exceções à referida regra geral (artigo 3º).

Recentemente, a Câmara dos Deputados aprovou Projeto de Lei Complementar para que alguns "serviços" virtuais passem a pagar ISS (Imposto sobre Serviços de Qualquer Natureza), tributo cobrado por municípios. A Lei Complementar 157/2016 alterou a LC 116/2003, em seu artigo 3º, que passou a ter a seguinte redação:

> Art. 3º O serviço considera-se prestado, e o imposto, devido, no local do estabelecimento prestador ou, na falta do estabelecimento, no local do domicílio do prestador, exceto nas hipóteses previstas nos incisos I a XXV, quando o imposto será devido no local:

Por fim, a novel Lei Complementar trouxe em seu anexo a incidência do ISS sobre serviços de informática e, mais precisamente, os que propiciam a disponibilização, sem cessão definitiva, de conteúdos de áudio, vídeo, imagem e texto por meio da internet, respeitada a imunidade de livros, jornais e periódicos.

O avanço na tecnologia de servidores armazenamento de dados, já narrado neste trabalho, permitiu que as infraestruturas computacionais pudessem ser instaladas em diferentes lugares e não nas instalações das empresas, cada vez mais dependentes da tecnologia da informação e comunicação para conduzir seus negócios com eficiência e agilidade.

Esta evolução propiciou condições mercadológicas para o surgimento de empresas interessadas em investir na construção de *datacenters*, com o fito de prover infraestrutura computacional remota com serviços operacionais especializados, trazendo vantagens, como escalabilidade, alta disponibilidade e segurança operacional, tanto patrimonial quanto cibernética. Nos primórdios, prevalecia o modelo de aluguel de espaço no *datacenter*, porém, gradualmente, os provedores de *datacenter,* impulsionados, por melhores condições de custo decorrentes de compras em escala e capacidade de investimento, passaram a ofertar também o “aluguel” do *hardware*.

A contínua evolução da tecnologia possibilitou, assim, a virtualização de *hardware* de armazenamento e de rede com a Internet. Os avanços mais recentes nos *softwares* de gestão de infraestrutura computacional possibilitam que a capacidade computacional alugada possa ser aumentada ou reduzidas em função das necessidades do usuário e que a carga computacional seja balanceada entre várias máquinas

físicas, podendo estar, até mesmo, localizadas em distintos *datacenters*, por exemplo.

Uma importante característica introduzida nas ofertas de Computação em Nuvem é a possibilidade de contratação de forma remota através da Internet, por intermédio de portais que permitem ao usuário especificar as características técnicas e a capacidade desejadas, adequando o serviço ao que é desejado por ele. Este modelo de contratação é conhecido como *pay-per-use*, sendo baseado em pagamento realizado na medida da utilização da plataforma. Ou seja, o provedor determina um preço unitário, em função do tipo de máquina virtual especificada, e uma unidade de utilização, por exemplo, tempo de processamento ou de uso do armazenamento. O cálculo do valor devido pelo contratante pode ser realizado ao final de um período avençado.

A oferta dos serviços da Computação em Nuvem são feitas por *Infrastructure as a Service* (IaaS), *Platform as a Service* (*PaaS*), que é usualmente caracterizada como oferta de *softwares* relacionados à infraestrutura, tais como, sistema de gerenciamento de banco de dados e plataformas de desenvolvimento ou integração de aplicações. Neste sentido, a oferta de *PaaS* pode ser ou não conjugada à oferta de *IaaS*.

Os *softwares* em Computação em Nuvem são disponibilizados em diversas formas, por exemplo, em computadores pessoais, é usual o acesso ao aplicativo a partir de navegadores da Web. Já, em *smartphones* ou *tablets*, aplicativos específicos são disponibilizados para os vários sistemas operacionais, em complemento ao acesso através dos navegadores da Web. O *software* em nuvem, per si, são usualmente executados em servidores de alta performance localizados em *datacenters* conectados à Internet.

Os aplicativos de acesso ao sistema em nuvem são disponibilizados através de *download*, gratuita ou onerosamente, a depender do fornecedor. Frise-se que quando o aplicativo é objeto de cobrança, usualmente o preço cobre também o *software* executado nos servidores localizados nos *datacenters*.

A cobrança do *software* em nuvem é usualmente mensal, podendo variar em função de certos parâmetros, tais como, número de usuários, capacidade de armazenamento, extensões ou funcionalidades adicionais, voltadas ou não para clientes empresarias. Não se verifica esta comercialização por intermédio de licença de uso perpétuo.

Em temos gerais, é possível distinguir dois ramos mercadológicos, caracterizados pelos tipos de operação: (a) as operações comerciais, envolvendo produtos primários, agrícolas ou minerais, e industrializados; e (b) as operações de serviço, envolvendo todo restante, incluindo

serviços financeiros, serviços de base laboral e até alugueis. Tal conceituação dicotômica, possivelmente mercê de sua simplicidade, permeia o senso comum.

É evidente que a evolução tecnológica trouxe várias e importantes modificações para os mercados de *hardware* e *software*, sendo uma das mais importantes, sob a ótica negocial, a disseminação das contratações no modelo de aluguel em detrimento das operações de compra de venda. Estas transformações ocorreram tanto no *hardware*, com o aluguel de equipamentos, instalados tanto nas premissas dos contratantes quanto em *datacenters* de terceiros; quanto no aluguel de licenças de uso e gozo de *software*, por tempo definido, ambos com pagamentos usualmente mensais ou mesmo anuais.

Ora, se tudo que não for compra e venda é, pelo senso rasteiro e comum, uma modalidade de serviço, então o aluguel de equipamentos em *datacenters* facilmente entendido na expressão "Infraestrutura como Serviço" e o aluguel de licença de uso e gozo de *software* como "Software como Serviço" podem ser classificados de serviços.

Todavia, a subsunção tributária, conforme o Art. 110[22] do CTN, se dá a partir da definição, do conteúdo e do alcance de institutos, conceitos e formas do direito privado, sejam eles expressos ou implícitos. De acordo com a regra exegética do diploma tributário pátrio, a denominação comercial de uma operação só tem relevância na medida em que, ela mesma, se coaduna com a conceituação jurídica.

A proposta de oferta de serviços através de Computação em Nuvem envolve três operações distintas: a) Disponibilização onerosa e remota de servidores e outros *hardwares* localizados em *datacenters*, acessível por meio de pagamento periódico, com a natureza jurídica de aluguel bens móveis; b) Licenciamento oneroso de *softwares*, como sistema operacional ou aplicativos de gestão de infraestrutura, acessível por meio de pagamento periódico, com natureza jurídica de aluguel de direito de uso e gozo de direito pessoal intangível; c) Serviços técnicos de comissionamento, operação, suporte e manutenção dos *hardwares* e dos *softwares*, serviços de atendimento e suporte aos usuário, usualmente prestados à distância, acessíveis através de pagamento periódico, mas com natureza jurídica de prestação de serviço.

---

[22] Art. 110. A lei tributária não pode alterar a definição, o conteúdo e o alcance de institutos, conceitos e formas de direito privado, utilizados, expressa ou implicitamente, pela Constituição Federal, pelas Constituições dos Estados, ou pelas Leis Orgânicas do Distrito Federal ou dos Municípios, para definir ou limitar competências tributárias.

Considerando as operações de oferta dos produtos da Computação em Nuvem é possível concluir, no tocante às hipóteses de incidência tributária: 1) Na operação de disponibilização onerosa de hardwares localizados em *datacenters*, por se tratar de aluguel de bens móveis, não há incidência de Imposto sobre Serviços (ISS) de acordo com a Súmula Vinculante nº 31[23], por conseguinte, não há incidência de nenhum outro imposto; 2) Nas operações de licenciamento oneroso de softwares não há incidência de Imposto Sobre Circulação de Mercadorias e Serviços (ICMS), por não se caracterizar a operação mercantil, e, por se tratar de cessão de uso e gozo de direito pessoal de caráter patrimonial, conforme o Art. 83, III,[24] do Código Civil, tem natureza jurídica de aluguel de bens móveis, não havendo, portanto, incidência de ISS de acordo com a Súmula Vinculante nº 31; 3) Nas operação de prestação de serviços técnicos há a incidência de Imposto sobre os Serviços (ISS), conforme subitem 1.07 da Lista de serviços anexa à Lei Complementar nº 116/2003[25], a ser pago no local do do domicílio do prestador de serviços, quando este for no Brasil, de acordo com o Art. 3º do referido Diploma Complementar, ou no estabelecimento do tomador ou intermediário do serviço, quando o serviço for prestado a partir do exterior, conforme Art. 3º, I, e Art. 1º, §1º, do mesmo referido diploma.

Em 2014, a Receita Federal do Brasil publicou o Ato Declaratório Interpretativo nº 7 com a seguinte dicção:

> Dispõe sobre a natureza das operações realizadas por empresas contratadas no exterior para disponibilizar infraestrutura para armazenamento e processamento de dados em alta performance para acesso remoto, identificada no jargão do mundo da informática como data center.
> O SECRETÁRIO DA RECEITA FEDERAL DO BRASIL, no uso da atribuição que lhe confere o inciso III do art. 280 do Regimento Interno da

[23] Súmula Vinculante 31: É inconstitucional a incidência do Imposto sobre Serviços de Qualquer Natureza – ISS sobre operações de locação de bens móveis. Data: 04/02/2010

[24] Art. 83. Consideram-se móveis para os efeitos legais:
III - os direitos pessoais de caráter patrimonial e respectivas ações.

[25] Lista de serviços anexa à Lei Complementar nº 116/2003
1.07 – Suporte técnico em informática, inclusive instalação, configuração e manutenção de programas de computação e bancos de dados.

> Secretaria da Receita Federal do Brasil, aprovado pela Portaria MF nº 203, de 14 de maio de 2012, e tendo em vista o disposto nos arts. 585, 682 e 708 do Decreto nº 3.000, de 26 de março de 1999, no art. 2º-A da Lei nº 10.168, de 29 de dezembro de 2000, e no art. 1º da Lei nº 10.865, de 30 de abril de 2004, declara:
> Art. 1º Os valores pagos, creditados, entregues ou remetidos por residente ou domiciliado no Brasil para empresa domiciliada no exterior, em decorrência de **disponibilização de infraestrutura para armazenamento e processamento de dados para acesso remoto, identificada como data center, são considerados para fins tributários remuneração pela prestação de serviços, e não remuneração decorrente de contrato de aluguel de bem móvel.**
> Parágrafo único. Sobre os valores de que trata o caput devem incidir o Imposto sobre a Renda Retido na Fonte (IRRF), a Contribuição de Intervenção no Domínio Econômico destinada a financiar o Programa de Estímulo à Interação Universidade-Empresa para o Apoio à Inovação (Cide-Royalties), a Contribuição para o PIS/Pasep-Importação e a Cofins-Importação.
> Art. 2º Ficam modificadas as conclusões em contrário constantes em Soluções de Consulta ou em Soluções de Divergência emitidas antes da publicação deste ato, independentemente de comunicação aos consulentes.

A dicção do Art. 1º que, sem nenhum pudor, afronta o entendimento claro de civilistas quanto à natureza jurídica da obrigação do armazenamento e processamento de dados remotos, contrariando também a Súmula Vinculante nº 31, que versa justamente sobre incidência tributária. A antijuricidade do artigo é intrínseca à sua própria dicção, na medida em que define ser uma prestação de serviços, ou seja, uma obrigação de fazer, a "disponibilização de infraestrutura", indubitavelmente uma obrigação de dar.

Frise-se que o interesse público não se confunde com o interesse do Estado ou da Administração, uma vez que o verdadeiro interesse público é a maximização do benefício-agregado, traduzido nos efeitos econômicos e sociais, considerando, necessariamente, o impacto da

tributação sobre o mercado e sobre o bolso do cidadão. O afã arrecadatório presente na interpretação macula o ato de violação do princípio da pessoalidade, na medida em que procura tão somente o interesse do Estado na maximização dos seus interesses, ao arrepio do Sistema Tributário Nacional. Procedendo à análise das variações de carga tributária sobre Computação na Nuvem, seja *IaaS* ou *Paas*, providos no exterior e localmente, considerando as interpretações manifestadas pelos vários órgãos da administração pública, é possível vislumbrar o equívoco do gestor tributário, bem como seu afã arrecadatório. Conforme sumarizado no quadro abaixo, a interpretação do Art. 1º do Ato Declaratório Interpretativo RFB nº 7/2014, considerada como *status quo*, aglutina as três operações comerciais em uma única hipótese de incidência tributária, prestação de serviços, fazendo incidir as maiores alíquotas dos tributos federais, a saber, PIS/Cofins Importação, CIDE-Royalties e IRRF, Imposto de Renda Retido na Fonte, sobre o valor total da operação aglutinada para a Nuvem Provida a partir do Exterior.

Ficam afastadas as incidências sobre Aluguel de Hardware e Licenciamento de Software, que são muito menos onerosas. Ressalte-se, à guisa de clareza metodológica, que a incidência do ISS foi considerada com base no ordenamento do Município de São Paulo, cidade em que agrega a maior quantidade de usuários por metro quadrado do Brasil.

Incidência Tributária sobre Conputação e Software na Nuvem com Procedência do Exterior

Tributo (Lastro legal, jurisprudencial ou infralegal)	Alíquota	Status Quo (Prest. de Serviços)	Conforme a Constituição (Três operações)
PIS-Importação: Serviços Lei nº 10.865/2004, Art. 3º,II, Art. 7º,II, e Art. 8º,II	1,65%	Valor Total	Para cada operação
Cofins-Importação: Serviços Lei nº 10.865/2004, Art. 3º,II, Art. 7º,II, e Art. 8º,II	7,60%	Valor Total	Para cada operação
CIDE-Royalties: Serviços Técnicos Lei nº 10.168/2000, Art. 2º,§2º e §3º	10,0%	Valor Total	Serviços Técnicos
IRRF: Serviços Técnicos Decreto nº 3.000/1999, Art. 708 e Lei nº 10.168/2000, Art. 2º-A	15,0%	Valor Total	Serviços Técnicos
IRRF: Remuneração de Direitos Decreto nº 3.000/1999, Art. 709	15,0%	Não Aplicável	Aluguel de Hardware Licenciamento de Software
ICMS-SP: Licenciamento de Software Decreto nº 61.791/2016 do Estado de São Paulo, Artigo 1º	5,0%	Não Aplicável	Não Aplicável
ISS-SP: Licenciamento de Software Lei nº 13.701/2003 da Cidade de São Paulo, Art. 1º, 1.05, e Art. 16,II	2,0%	Não Aplicável	Não Aplicável
ISS-SP: Suporte Técnico e Manutenção Lei nº 13.701/2003 da Cidade de São Paulo, Art. 1º, 1.07, e Art. 19	5,0%	Valor Total	Serviços Técnicos
Não incide ISS em aluguel de bens móveis Súmula Vinculante nº 31	0%	Não Aplicável	Aluguel de Hardware Licenciamento de Software

Fonte: Gallindo, Sergio Paulo Gomes. 2017. P. 174

A análise comparativa entre o *status quo*, definido pelo ato administrativo infralegal e a interpretação do ordenamento tributário conforme a Constituição Federal, índica que a interpretação da Receita Federal produz um aumento na carga tributária média das duas modalidades de Serviços na Nuvem.

Assim, considerando a transversalidade da Computação na Nuvem tem nos setores da economia, representando instrumentos de redução de custos, aumento de eficiência operacional e produtividade, o aumento desproporcional de uma carga tributária já elevada não pode ser considerado um ato em prol do melhor interesse público.

No tocante à Nuvem Local, sumarizada no quadro a seguir, surgem duas questões relevantes: (a) a situação de conflito interpretativo entre os Estados e Municípios em torno da tributação sobre *software*, e (b) a relativa insegurança jurídica que paira sobre a incidência tributária constitucionalmente adequada para as ofertas na nuvem. A primeira questão, tem levado os agentes econômicos a uma situação de bitributação, totalmente incompatível com o Sistema Tributário Constitucional Pátrio.

Incidência Tributária sobre Conputação e Software na Nuvem com Procedência Local

Tributo (Lastro legal, jurisprudencial ou infralegal)	Alíquota	Status Quo (Bitributação)	Conforme a Constituição (Três operações)
PIS Lei nº 9.718/1998, Art. 4º,IV	0,65%	Aplicável	Para cada operação
Cofins Lei nº 9.718/1998, Art. 4º,IV	3,0%	Aplicável	Para cada operação
ICMS-MG: Licenciamento de Software Decreto nº 46.877/2015 do Estado de Minas Gerais	18,0%	Bitributação	Não Aplicável
ISS-BH: Serviços de informática e congeneres Lei nº 8.725/2003 da Cidade de Belo Horizinte, Art. 14, IV	5,0%	Bitributação	Não Aplicável
ICMS-SP: Licenciamento de Software Decreto nº 61.791/2016 do Estado de São Paulo, Artigo 1º	5,0%	Bitributação	Não Aplicável
ISS-SP: Licenciamento de Software Lei nº 13.701/2003 da Cidade de São Paulo, Art. 1º, 1.05, e Art. 16,II	2,0%	Bitributação	Não Aplicável
ISS-SP: Suporte Técnico e Manutenção Lei nº 13.701/2003 da Cidade de São Paulo, Art. 1º, 1.07, e Art. 16 Instrução Normativa nº 8 de 2011, Prefeitura de São Paulo, Art. 1º	3,0%	Aplicável	Serviços Técnicos
Não incide ISS em aluguel de bens móveis Súmula Vinculante nº 31	0%	ISS por receio de insegurança jurid.	Aluguel de Hardware Licenciamento de Software

Fonte: Gallindo, Sergio Paulo Gomes. 2017. P. 176

Os serviços de Tecnologia da Informação e Comunicação (TIC), dentre os quais estão os serviços em Nuvem des são transversais na economia e potencializadores de eficiência para todas as demais atividades. A tributação exagerada afeta equilíbrio entre oferta e demanda, inibindo a segunda. Um possível efeito de uma política tributária onerosa é o retardamento da adoção de tecnologias voltadas a eficiência, produzindo, como consequência, perda de competividade relativa.

A despeito da controvérsia apresentada, o Poder Judiciário ainda não se manifestou sobre as possíveis bitributações mencionadas, o que prejudica a apresentação de uma conclusão jurisdicional. Assim sendo, uma política tributária bem concebida certamente será um poderoso fator de indução do setor de TIC em ambiente pátrio.

3.3 - A Segurança da Informação sob o enfoque do Marco Civil brasileiro da Internet

O Marco Civil e regulatório da Internet no Brasil trouxe alguns meios de desestímulo e obstaculização à apropriação indevida e injusta da informação, bem como garante minimamente a preservação da privacidade do usuário/consumidor e também a segurança dos dados postos na nuvem, dando-lhes garantias, mesmo que que elementares, contra atos perniciosos e danosos.

Todavia, o marco regulatório, por si só, não é suficiente para a proteção dos dados disposto em nuvem computacional, que é calcada na instantaneidade do fluxo da informação, haja vista que a estrutura que a provem fica completamente delegada a um terceiro prestador de serviços. É sábido que o princípio da segurança jurídica está diretamente ligado às garantias fundamentais, asseguradas pelo ordenamento jurídico brasileiro. A aprovação do Marco Civil da Internet, que estabeleceu princípios, garantias, deveres e direitos para o uso da Internet no Brasil.

A segurança da informação se refere à proteção sobre as informações de uma determinada empresa ou indivíduo. Aplica-se tanto às informações corporativas quanto às pessoais. Todavia, existe uma relação inversa quando se trata de privacidade e segurança, pois quanto maior a segurança coletiva, geralmente menor é a privacidade individual. Um exemplo dessa relação são os sistemas de monitoramento com vídeo em prédios e ambientes públicos. Para Sweeney (2002, p.5)[26]:

[26] Tradução livre: An area that might appear to have a common ancestry with the subject of this paper is access control and authentication, which are traditional areas associated with computer security. Work in this area ensures that the recipient of information has the authority to receive that information. While access control and authentication protections can safeguard against direct disclosures, they do not address disclosures based on inferences that can be drawn from released data. The more insidious problem in the work that is the subject of this paper is not so much whether the recipient can get access or not to the information as much as what values will constitute the information the recipient will receive. A general doctrine of the work presented herein is to release all the information but to do so such that the identities of the people who are the subjects of the data (or other sensitive properties found in the data) are protected. Therefore, the goal of the work presented in this paper lies outside of traditional work on access control and authentication.

> Uma área que pode parecer ter uma ascendência comum com o assunto deste artigo é o controle de acesso e a autenticação, que são áreas tradicionais associadas à segurança do computador. O trabalho nesta área garante que o destinatário da informação tenha autoridade para receber essa informação. Embora as proteções de controle de acesso e autenticação possam se proteger contra divulgações diretas, elas não abordam divulgações baseadas em inferências que podem ser extraídas de dados divulgados. O problema mais insidioso no trabalho que é o assunto deste artigo não é tanto se o destinatário pode acessar ou não a informação tanto como quais valores constituirão a informação que o destinatário receberá. Uma doutrina geral do trabalho aqui apresentado é liberar todas as informações, mas fazê-lo de tal forma que as identidades das pessoas que são os sujeitos dos dados (ou outras propriedades sensíveis encontradas nos dados) estão protegidas. Portanto, o objetivo do trabalho apresentado neste documento está fora do trabalho tradicional de controle de acesso e autenticação.

Em suma, a autora afirma que a segurança computacional não implica em proteção à privacidade, pois embora mecanismos de controle de acesso e autenticação possam proteger as informações contra a divulgação, eles não tratam da propagação indireta da informação, nem de divulgações com base em inferências e correlações sobre informações extraídas de outras fontes.

É possível aduzir que a segurança da informação está diretamente relacionada com proteção de um conjunto de informações, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. São propriedades básicas da segurança da informação: confidencialidade, integridade, disponibilidade e autenticidade. Não está restrita somente a sistemas computacionais, informações eletrônicas ou sistemas de armazenamento. A ISO/IEC 17799:2005[27], em sua seção introdutória, define segurança da informação como "a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio,

[27] Disponível em http://www.ciencianasnuvens.com.br/site/wp-content/uploads/2014/09/215545813-ABNT-NBR-177991.pdf

minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio".

A segurança computacional ou da informação passou por várias fases: inicialmente pretendia-se prevenir as violações de proteção; em seguida, o objetivo foi detectar e limitar as violações que não podiam ser prevenidas. O esquema de segurança computacional necessita preservar as propriedades básicas: confidencialidade, integridade, disponibilidade, autenticidade e não repúdio. Possui como três objetivos primordiais: i) integridade, que tem como objetivo garantir a exatidão da informação, assegurando que pessoas não autorizadas possam modificá-la, adicioná-la ou removê-la, seja de forma intencional ou acidental; ii) disponibilidade, garante que os autorizados a acessarem a informação possam fazê-lo sempre que necessário; iii) e confidencialidade da informação, que é é a garantia de que somente pessoas autorizadas terão acesso a ela, protegendo-a de acordo com o grau de sigilo do se conteúdo.

Sêmola (2003), por sua vez, acrescenta outros dois objetivos: a) legalidade, que seria a garantia de que a informação foi produzida em conformidade com a lei; b) autenticidade, garantia de que num processo de comunicação os remetentes sejam exatamente o que dizem ser e que a mensagem ou informação não foi alterada após o seu envio ou validação.

À medida em que as empresas se tornam mais dependentes da tecnologia da informação, mais vulneráveis ficam a crimes e fraudes cometidas com o uso de recursos computacionais. Logo, em razão do alto valor mercadológico da informação, a proteção de dados importantes para o negócio precisam ser protegidas contra as ameaças que podem levar à sua destruição, indisponibilidade temporária, adulteração ou divulgação não autorizada.

Com o escopo de aumentar, melhorar, bem como padronizar os critérios de segurança foram desenvolvidas várias normas de âmbito nacional e internacional sobre a segurança da informação. Em dezembro de 2000, foi publicada a norma internacional ISO 17799:2000. Em 2001, a Associação Brasileira de Normas Técnicas (ABNT) publicou a versão brasileira que ficou com a denominação de NBR/ISO 17799 – Código de Prática para a Gestão da Segurança da Informação. Em setembro de 2005, a norma foi revisada e publicada como NBR ISO/IEC 17799:2005. (ISO 17799, 2005)

Nas palavaras da Professora Adriana Beal (2005, p.32): "Normas e padrões têm por objetivo definir regras, princípios e critérios, registrar as melhores práticas e prover uniformidade e qualidade a processos, produtos ou serviços, tendo em vista sua eficiência e eficácia.". As políticas de segurança envolvem a definição de regras para proteção do

nível físico; contenção, recuperação de desastres, backup, preservação e destruição de mídias; operação envolvendo treinamento do usuário e registro de todas as ações de suporte; uso de criptografia e ciclos de vida de chaves; controle de acesso a sistemas e a recursos; não violação a leis e a ética etc.

Estas normas definem os controles que compõem o Sistema de Gestão de Segurança da Informação (Information Security Management System – ISMS), que, por sua vez, agrupa 11 seções de controles: 1) Política de Segurança da Informação; 2) Organização da Segurança da Informação; 3) Gestão de Ativos; 4) Segurança em Recursos Humanos; 5) Segurança Física e do Ambiente; 6) Gestão das Operações e Comunicações; 7) Controle de Acesso; 8) Aquisição, Desenvolvimento e Manutenção dos Sistemas de Informação; 9) Gestão de Incidentes da Segurança da Informação; 10) Gestão da Continuidade do Negócio; e 11) Conformidade.

Desta maneira, a adequação de qualquer empresa à norma ISO IEC 27002:2005 garante conformidade com as melhores práticas em gestão da segurança da informação, porém não há imunidade à ataques, mas tão-somente a utilização das melhores técnicas de segurança da informação.

As ameaças à segurança da informação são relacionadas diretamente à perda de algum dos três principais objetivos: a) perda de confidencialidade: há uma quebra de sigilo de uma determinada informação (ex: a senha de um usuário ou administrador de sistema) permitindo que sejam expostas informações restritas as quais seriam acessíveis apenas por um determinado grupo de usuários; b) perda de integridade: determinada informação fica exposta a manuseio por uma pessoa não autorizada, que efetua alterações que não foram aprovadas e não estão sob o controle do proprietário (corporativo ou privado) da informação; c) perda de disponibilidade: a informação deixa de estar acessível por quem necessita dela. Seria o caso da perda de comunicação com um sistema importante para a empresa, que aconteceu com a queda de um servidor ou de uma aplicação crítica de negócio, que apresentou uma falha devido a um erro causado por motivo interno ou externo ao equipamento ou por ação não autorizada de pessoas com ou sem má intenção.

No caso de ameaças à rede de computadores ou a um sistema, estas podem vir de agentes maliciosos, muitas vezes conhecidos como crackers, hackers, que são motivados a fazer esta ilegalidade por vários motivos, dentre eles: notoriedade, autoestima, vingança e enriquecimento ilícito.

A nível de legislação brasileira, o Marco Civil da Internet trata sobre segurança da informação em seus artigos 10, 11 e 12. As normas dos dispositivos mencionados coadunam-se com os princípios do artigo 7º da mesma lei, buscando atribuir a responsabilidade da coleta, a rmazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações para os provedores de acesso à rede mundial de computadores.

Infelizmente, o legislador brasileiro, apesar de tratamento isonômico entre os usuários objetivado pelo Marco Civil da Internet, atribuiu tal responsabilidade ao provedor genericamente, pois este, em sua função primordial, não tem o escopo de coletar ou guardar dados informacionais.

O professor Leonardi do Programa de Educação Continuada do Direito FGV (2012, p.4) conceituou os chamados provedores de serviços de internet: "provedor de serviços de internet é gênero do qual as demais categorias são espécies. Assim, provedor de internet é a pessoa natural ou jurídica que fornece serviços relacionados ao funcionamento da internet, ou por meio dela.".

A primeira espécie de provedor, na doutrina de Leonardi, é o chamado Provedor de Backbone ou Provedor de Estrutura, que se refere à pessoa jurídica proprietária das redes capazes de administrar grandes volumes de informações, constituídos por roteadores de tráfego interligados por circuitos de alta velocidade. O Marco Civil da Internet não faz menção a este provedor, pois o usuário dificilmente terá alguma relação jurídica direita com ele. Por exemplo, no Brasil, a Embratel é o principal provedor de estrutura.

Provedor de Acesso ou Provedor de Conexão é a pessoa jurídica fornecedora de serviços que consistem em possibilitar o acesso de seus consumidores à internet. Para sua caracterização, basta que ele possibilite a conexão dos clientes à internet. Por exemplo: Brasil Telecom, GVT, Telemar Norte Leste (OI) e operadoras de telefonia celular como TIM, Claro e Vivo. A legislação pátria conceituou este provedor como uma forma de provisão de conexão à internet, cabendo ao administrador de sistema autônomo o respectivo dever de manter os registros de conexão.

O Provedor de Correio Eletrônico é a pessoa jurídica fornecedora e serviços que consistem em possibilitar o envio de mensagens do usuário a seus destinatários, mediante o uso de um nome de usuário e senha exclusivos. Os provedores de correio mais populares são Gmail (Google), Yahoo e Hotmail (Microsoft).

Há também o Provedor de Hospedagem que é a pessoa jurídica fornecedora de serviços que consistem em possibilitar o armazenamento

de dados em servidores próprios de acesso remoto, permitindo o acesso de terceiros a esses dados, de acordo com as condições estabelecidas com o contratante do serviço. Um provedor de hospedagem oferece dois serviços distintos: o armazenamento de arquivos em um servidor e a possibilidade de acesso a tais arquivos. Os provedores de hospedagem podem oferecer plataformas prontas para seus usuários, objetivando acessar websites, blogs, publicação de vídeos, acesso a músicas, criação de websites e redes sociais.

O Provedor de Conteúdo é toda pessoa natural ou jurídica que disponibiliza na internet as informações criadas ou desenvolvidas pelos provedores de informação, utilizando servidores próprios ou os serviços de um provedor de hospedagem para armazená-las.

Finalmente, o Provedor de Informação é o efetivo autor da informação, assim, a pessoa natural que mantenha um website, ou mesmo uma conta em uma rede social, é um provedor de conteúdo. Se esta mesma pessoa insere informações no site, ela passa a ser, também, um provedor de informação ou autor.

O Marco Civil da Internet não traz nenhuma definição ou distinção específica sobre os provedores, tratando especificamente de duas espécies de provedores, os de conexão e de aplicação de internet. Os primeiros, Provedores de Conexão à Internet, não há maiores dificuldades, pois correspondem à definição clássica de provedor de acesso ou provedor de conexão. Os Provedores de Aplicação de Internet (PAI) podem ser conceituados, grosso modo, como provedores de serviços online (POSs). O Marco Civil da Internet, em seu artigo 5°, trouxe algumas definições, entretanto não tratou de conceituar as espécies de provedores. O inciso VI, do mesmo artigo 5°, apresenta o conceito de provedores de "aplicação da internet: aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet."

Consequentemente, é possível analisar o artigo 15 do Marco Civil da Internet e chegar a um conceito de provedor de aplicação da internet (PAI), aduzindo que Provedor de Aplicação de Internet (PAI) é um termo que descreve qualquer empresa, organização ou pessoa natural que, de forma profissional ou amadora, forneça um conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet, não importando se os objetivos são econômicos.

Nota-se que o artigo 15 da Lei 12.965/2014 aponta a existência do Provedor de Aplicação de Internet (PAI), bem como a possibilidade de criar o conceito:

> O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.
>
> §1º Ordem judicial poderá obrigar, por tempo certo, os provedores de aplicações de internet que não estão sujeitos ao disposto no caput a guardarem registros de acesso a aplicações de internet, desde que se trate de registros relativos a fatos específicos em período determinado.
>
> §2º A autoridade policial ou administrativa ou o Ministério Público poderão requerer cautelarmente a qualquer provedor de aplicações de internet que os registros de acesso a aplicações de internet sejam guardados, inclusive por prazo superior ao previsto no caput, observado o disposto nos §§ 3º e 4º do art. 13.
>
> §3º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.
>
> §4º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência.

Inobstante a variedade de provedores somente dois foram contemplados na legislação brasileira, o que mostra a incompletude da norma, forçando ao hermeneuta a utilizar uma arcabouço de conceitos técnicos para diferenciar a natureza ou conceito dos objetos envolvidos na norma.

Não há que olvidar se falar sobre servidores de internet, que, em suma, são os dispositivos físicos, cuja função é monitorar e controlar todas as informações que transitam para dentro e fora da sua empresa por

meio da internet. Os servidores costumam ser usados para armazenar dados digitais.

O termo servidor é amplamente aplicado a computadores completos, embora um servidor possa equivaler a um *software* ou a partes de um sistema computacional, ou até mesmo a uma máquina que não seja necessariamente um computador. Pode fornecer várias funcionalidades, como a partilha de dados ou recursos do sistema entre vários clientes. Um único servidor pode servir vários clientes, e um único cliente pode usar vários servidores.

Após análise dos conceitos e termos da Tecnologia da Informação aplicados pelo Marco Civil da Internet brasileira é possível vislumbrar que o legislador aponta como principais responsáveis pela segurança da informação e, consequentemente, pela lisura dos dados, os provedores de conexão e os aplicação da internet.

Como se percebe, o Marco Civil da Internet impõe aos provedores que fornecem acesso à Internet o dever de guardar, por um ano, os registros de conexão, nos termos definidos no art. 5º, inciso VI, como o "conjunto de informações referentes à data e hora de início e término de uma conexão à Internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados". Já a guarda de registros de acesso a aplicações de internet é facultada aos provedores de aplicações.

É salutar que o Marco Civil da Internet tenha adotado modelos diferentes para os registros de conexão, de guarda obrigatória pelo prazo de um ano, e para os registros de acesso a aplicações da Internet, de guarda facultativa. Evita-se, com isso, adotar um modelo único de retenção de dados de forma indiscriminada, o que implicaria tratar todos os usuários de Internet como suspeitos da prática de atos ilícitos, com sérias implicações para sua privacidade.

Em contrapartida, o Marco Civil da Internet privilegia o modelo de preservação de dados, impondo a provedores de conexão e de aplicações que recebem uma ordem judicial o dever de preservar, a partir daquele momento, dados específicos de usuários determinados, suspeitos de terem praticado crimes ou atos ilícitos por meio da Internet. Todos os demais usuários do provedor não são afetados. Note-se que os provedores de serviços de Internet também têm o dever de manter em sigilo todos os dados cadastrais e de conexão de seus usuários, observando-se, apenas, as exceções previstas contratualmente e as outras que forem aplicáveis, na forma da lei.

Evidentemente, o sigilo dos dados cadastrais e de conexão de um usuário pode ser afastado quando este comete um ato ilícito por meio da

Internet. Em tal situação, caso os provedores de serviços de Internet tenham armazenado tais dados, poderão informá-los à vítima, sempre mediante ordem judicial específica. Isso porque fornecer dados de usuários da Internet, sem ordem judicial específica, representaria desobediência às normas impositivas da Constituição Federal que asseguram a privacidade e o sigilo de dados do indivíduo. Além disso, a obtenção, sem ordem judicial, de dados de usuários supostamente envolvidos em atos ilícitos poderia ser prejudicial à própria investigação, já que provas obtidas em desobediência à Carta Magna e fora do devido processo legal podem, eventualmente, ser consideradas inadmissíveis, ante o disposto no art. 5º, inciso LVI, da CF.

3.4 - O Projeto de Lei 5.344/2013

O Deputado Federal Ruy Carneiro (PSDB/PB) apresentou o Projeto de Lei 5.344/2013[28], que, segundo as palavras do parlamentar, traduzia-se em uma tentativa de regulamentação da tecnologia da Computação em Nuvem no Brasil, haja vista a ausência de norma específica. Neste sentido, assevera uma das justificativas do mencionado Deputado:

> Um ambiente regulatório adequado – que não isole o Brasil, mas que garanta segurança jurídica aos cidadãos, empresas e governo – é, atualmente, fundamental para promover a ampliação da nuvem computacional no país e fazer do Brasil um espaço competitivo para acolher investimentos externos neste domínio, sendo escolhido como país para a instalação de datacenters, assim como estimular empresas brasileiras a internacionalizarem-se por esta via.

O Projeto de Lei equivocadamente apontou um conceito de Computação em Nuvem restringindo a *cloud computing* a um serviço de backup e armazenamento de dados *online* quando, na realidade, seu

---

[28] CÂMARA DOS DEPUTADOS. Projeto de Lei 5.344/2013. Dispõe sobre diretrizes gerais e normas para a promoção, desenvolvimento e exploração da atividade de computação em nuvem no País. Disponível em:<http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra;jsessionid=844786B2A3104162335C1 E52C491AE20.node1?codteor=1074235&filename=PL+5344/2013> acesso em 02 de outubro de 2017.

conceito é muito mais amplo, abrangendo, inclusive, uma verdadeira alocação e disponibilização de recursos virtuais e de software ao seu usuário. Desta forma, o o artigo 1º e seu parágrafo 1º dispõem:

> Art. 1º Esta Lei estabelece diretrizes gerais para a promoção, desenvolvimento e exploração da atividade de computação em nuvem no País, garantindo a possibilidade da adoção da computação em nuvem por entidades de direito público ou privado de forma segura.
>
> §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, sendo regido por esta lei e no que aplicável, pelo Código de Defesa do Consumidor, pela legislação específica de proteção de dados, de propriedade intelectual, legislações setoriais e outras aplicáveis.

O artigo 2º do Projeto de Lei aponta algumas diretrizes pela qual a Computação em Nuvem deve obedecer no âmbito do território brasileiro. Dentre os balizadores, encontra-se o princípio da extraterritorialidade do armazenamento de dados (inciso I), concebendo que estes não precisam ficar adstritos ao território nacional:

> I. Reconhecimento de extraterritorialidade de armazenamento: com necessidade de adoção de medidas que respeitem a concepção de que a computação em nuvem cria a possibilidade de armazenamento de dados em qualquer parte do mundo (virtualização de dados e serviços), gerando eficiências e ainda possibilitando uma maior garantia contra desastres naturais, de forma que não é necessário que as informações estejam guardadas necessariamente em território nacional, excetuando-se casos previstos em legislações ou regulamentações específicas.

O direito à privacidade, intimidade e proteção dos dados e da propriedade intelectual estão estipulados no inciso IV do referido artigo, que aduz:

> IV. Reconhecimento da privacidade, intimidade e proteção dos dados e da propriedade intelectual: necessidade de adoção de medidas que reconheçam e que promovam a proteção dos dados de forma clara e transparente em especial aqueles relativos à privacidade e intimidade, em atendimento à garantia constitucional e legal e garantindo a proteção à propriedade intelectual.

Este projeto visou também observar a responsabilização dos provedores de serviços, prevendo, inclusive, que em caso de omissão do contrato, haverá integral responsabilidade do provedor de computação em nuvem por atos de seus subcontratados, conforme o inciso V do artigo 2º:

> V. Clara definição de responsabilidades para os provedores do serviço e seus contratantes, em especial aqueles que por meio do serviço realizam tratamento de dados de terceiros, conforme vier a ser especificado em contrato ou em seu silêncio a assunção plena de responsabilidade do provedor de computação em nuvem por atos de seus subcontratados.

Dentre outros elementos caracterizadores das obrigações do prestador de serviços em Nuvem Computacional, o Projeto traz interessante disposição acerca da figura da exceção de contrato não cumprido disposto no Código Civil de 2002, ao dispor de forma contrária à disposição da lei civil.

Todavia, este Projeto de Lei encontra-se arquivado em razão da mudança de legislatura, nos moldes do artigo 105 do Regimento Interno da Câmara dos Deputados Federais. De qualquer maneira, trata-se de um tentativa legislativa bem-vinda, uma vez que a mercantilização informacional não poderá ficar submetida indefinidamente às normas de defesa do consumidor e direito civil.

CAPÍTULO 4 – RESPONSABILIDADE JURÍDICA DOS PROVEDORES DE COMPUTAÇÃO EM NUVEM

É cediço que todo o sistema computacional precisa ser minimamente protegido, mas é necessária uma análise sobre a importância dos dados que uma aplicação suportará, para que a segurança seja adequadamente dimensionada. Como já afirmado, a segurança da informação passou por várias fases: inicialmente pretendia-se prevenir as violações de proteção; em seguida, o objetivo foi detectar e limitar as violações que não podiam ser prevenidas. O esquema de segurança computacional necessita preservar as propriedades básicas: confidencialidade, integridade, disponibilidade, autenticidade e não repúdio.

Além dos objetivos apontados, alguns princípios devem ser considerados, como a responsabilização dos autores por suas ações, fornecimento do mínimo de privilégios possível para o desempenhar de uma atividade, minimização da quantidade, do tamanho e da complexidade dos componentes confiáveis do sistema e priorização do modo de operação seguro durante a implantação e utilização do sistema.

A segurança de sistemas computacionais envolve temas como políticas de segurança e sua utilização em diferentes contextos – comercial, militar, doméstico etc. e a gerência de riscos. As políticas de segurança envolvem a definição de regras para proteção do nível físico; contenção, recuperação de desastres, backup, preservação e destruição de mídias; operação envolvendo treinamento do usuário e registro de todas as ações de suporte; uso de criptografia e ciclos de vida de chaves; controle de acesso a sistemas e a recursos; não violação a 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, mitigá-las ou tolerá-las. De maneira geral os mecanismos utilizados para dar suporte ao esquema citado acima são: definição de domínios de segurança vinculando os usuários a seus respectivos domínios, implantação de operações de autenticação, autorização, controle de acesso e auditoria, e a utilização de criptografia.

Como já explicitado neste trabalho, os serviços fornecidos pela Nuvem Computacional podem ser disponibilizados em qualquer local físico de abrangência do sistema. A gerência de um grande número de serviços (SaaS, PaaS, IaaS) e recursos físicos pode gerar um volume considerável de dados a ser administrada de maneira centralizada, pois

será necessário coletar, armazenar, analisar e processar estes dados. Assim, a administração centralizada pode ser considerada impraticável, e portanto faz-se necessário distribuir em instâncias os serviços de gerenciamento.

Outrossim, a implantação de mecanismos de autenticação e esquemas de delegação de direitos funcionando de maneira confiável são fundamentais para o correto gerenciamento de identidades e para a prestação de serviços em nuvens computacionais, evitando ou obstaculizando possíveis falhas.

Para o ambiente de nuvem, o gerenciamento da autenticação deve fornecer suporte aos processos de criação e emissão das credenciais (e.g. senhas, certificados digitais) utilizadas pelos usuários. O usuário dos serviços também precisa ter a usabilidade considerada, pois esse pode necessitar utilizar um conjunto de métodos para as aplicações internas a organização, e outro conjunto para acessar os serviços na nuvem.

Um dos princípios da computação em nuvem é a redução dos custos com de *hardware* ou *software* e a respectiva manutenção associada aos mesmos, permitindo que as empresas concentrem-se em seus negócios. Esta abordagem tem benefícios financeiros e operacionais, mas deve ser cuidadosamente avaliada devido as preocupações com a segurança.

Os provedores de Computação em Nuvem possuem o custo para suportar vários mecanismos de autenticação, acomodando as necessidades de consumidores através de mecanismos heterogêneos, o que se torna pouco atrativo para a entidade que mantém a nuvem computacional. Neste caso, o ideal é a padronização dos mecanismos de autenticação para resolver estas limitações impostas pelas características de computação em nuvem.

Com o modelo de Computação em Nuvem, a informática passa a ser um utilitário que pode ser contratado e utilizado de acordo com a necessidade, sem que o consumidor tenha que se preocupar com o gerenciamento da infraestrutura. Apesar dos benefícios que a computação em nuvem pode trazer, os consumidores estão preocupados com os riscos que a utilização de um ambiente novo pode representar para os ativos (assets) da organização. Em outras palavras, uma organização estará terceirizando um sistema pelo qual é responsável, por exemplo, sem ter total controle sobre o mesmo.

O ambiente de computação em nuvem está sendo utilizado para hospedar vários tipos de serviços, e todos exigem garantias de segurança dos dados sendo processados e armazenados. Para o máximo proveito de todo o poder oferecido pela nuvem computacional, as diferentes entidades

– provedores e consumidores de serviços – necessitam de abordagens de segurança abrangentes e confiáveis.

A definição de um sistema de segurança baseado em políticas é uma necessidade administrativa e de uso da nuvem computacional, pois é possível controlar o acesso e uso individual de cada usuário do ambiente. Cada organização consumidora de serviços fornecidos pela nuvem precisa definir políticas para seus usuários. Os perfis e as políticas de controle de acesso podem variar de acordo com o tipo de consumidor ou usuário de serviços da nuvem. Quando o consumidor é uma organização as políticas envolvem a definição de regras para a totalidade do domínio da organização consumidora, enquanto para usuários da organização as políticas precisam ser individualizadas. O perfil do usuário pode ser descrito como um conjunto de atributos utilizados pela nuvem para customizar o serviço e possivelmente restringir o acesso a outros serviços.

Os usuários, consumidores ou organizações consumidoras devem avaliar o risco e as opções de segurança antes de transferir seus dados, sistemas e aplicativos para o ambiente de computação em nuvem, uma vez que é imprescindível avaliar quais dados e serviços podem ser transferidos para o ambiente externo a organização se a nuvem for pública, por exemplo. Os principais tipos de ativos suportados pela nuvem são: dados, aplicações, processos e serviços. Estes ativos devem ser analisados para que se possa determinar sua importância para o negócio da organização ou do usuário. Neste processo de análise busca-se avaliar os impactos gerados caso algum requisito de segurança (confidencialidade, integridade ou disponibilidade) seja comprometido.

Os controles de segurança na computação em nuvem são, em sua maioria, iguais aos controles de qualquer ambiente de tecnologia da informação. Porém, há variação de acordo com os modelos de serviço, modo de operação e tecnologias utilizadas para prover os serviços na nuvem, estes pode apresentar diferentes riscos para o ususário quando comparado com as abordagens tradicionais. Na computação em nuvem se abre mão de alguns controles (físico, por exemplo) enquanto se mantêm as responsabilidades sobre o gerenciamento operacional.

A segurança e a privacidade são os principais desafios que podem impedir a ampla adoção da abordagem de computação em nuvem, pois, falhas de segurança em qualquer um dos componentes podem impactar os demais componentes de segurança e consequentemente a segurança de todo o sistema poderá entrar em colapso.

Gonzalez et al (2013, p. 33), ao tratar sobre os desafios da segurança da Computação em Nuvem, afirma que:

> O modelo de computação em nuvem, no entanto, traz consigo uma série de desafios de segurança que devem ser analisados e endereçados por todos os envolvidos no modelo (tanto usuários como provedores de serviços). A falta de entendimento e atenção às questões de segurança pode trazer reflexos negativos para as empresas e para os indivíduos que fazem uso de tais serviços. Um exemplo dessa situação foi a falha do serviço AWS (Amazon Web Services) em abril de 2011, que afetou a grande maioria dos sites que se utilizavam da sua infraestrutura, lo calizada na costa leste dos EUA. Entre os afetados estão sites famosos, que utilizam os recursos da AWS para oferecer os seus serviços, como: Quora, Reddit, FourSquare e Everyblock.

Diferente das abordagens tradicionais de tecnologia da informação, a Computação em Nuvem oferece grande flexibilidade para os usuários, visto que estes não precisam se preocupar com a complexidade de gerenciamento inerente a cada sistema, por exemplo: os banco de dados podem ser transferidos para *datacenters* de grandes empresas especializadas. Entretanto, o gerenciamento dos dados em ambientes terceirizados nem sempre é confiável. Assim, é necessária a utilização de modelos de armazenamento de dados seguros visando garantir a integridade dos dados dos consumidores. A grande maioria dos provedores de computação em nuvem expõe um conjunto de interfaces para gerenciar e interagir com os serviços oferecidos (e.g. provisionamento, gerenciamento, orquestração, monitoramento etc.).

Outrossim, é importante destacar que as responsabilidades pela segurança dos serviços executados em Nuvem Computacional diferem-se entre si de acordo com o tipo de serviço e recursos contratados. Contudo, sempre há responsabilidades tanto por parte do usuário como do provedor e, desse modo, nenhuma das partes é desprovida de responsabilidades no âmbito de segurança, uma vez que esta necessita de um entendimento mútuo entre os envolvidos, pois de nada adiantaria o provedor criar vários mecanismos de segurança e o usuário não utilizá-los de forma minimamente adequada.

A segurança e a disponibilidade de alguns serviços da nuvem dependem de mecanismos de segurança da informação, por exemplo, autenticação, controle de acesso, cifragem e monitoramento. As interfaces dos aplicativos devem ser projetadas para se proteger de

tentativas acidentais ou maliciosas de violação de políticas. O modelo de segurança das interfaces disponibilizadas pelo provedor deve ser cuidadosamente analisado e avaliado, assegurando-se que mecanismos consistentes de autenticação e controle de acesso estejam implementados.

4.1 – O analfabetismo digital como causa da insegurança digital

Como já exposto anteriormente, com a finalidade de aumentar a mobilidade e a independência da interligação entre o indivíduo e seus dados digitais, criou-se o sistema de Computação em Nuvem, uma ferramenta-meio para o acesso de dados digitais armazenados em servidores, através de qualquer dispositivo inteligente, como *notebook's, ultrabook's, tablet's, smartphone's* etc. Deste modo, a Computação em Nuvem se propõe, dentre outros vários serviços, a delegar a tarefa de armazenamento e gerenciamento de dados de seus usuários a terceiros em servidores localizados em pontos diversos do globo.

A disseminação e crescente popularização da Computação em Nuvem foram possíveis em razão do crescente aumento de renda das camadas sociais, que permitiu um incremento do número de computadores domésticos e, consequentemente, de usuários de Internet no Brasil e no mundo, criando, assim, um fenômeno de inclusão social, em que a pessoa conectada e globalizada encontra-se imersa na sociedade tecnológica e de consumo. Todavia a adoção plena deste sistema é obstacularizada pela ausência de confiança, o cerne da questão, pois, como qualquer negócio jurídico, o sistema baseado na "nuvem" deve sempre se permear de lealdade, boa-fé, segurança, bem como abster-se de usar cláusulas abusivas, e outras situações perniciosas. Entretanto, o desafio é incutir na mentalidade da sociedade que os serviços da Computação em Nuvem podem ser seguros mesmo que as partes contraentes se desconheçam completamente e estejam separadas por milhares de quilômetros de distância.

Inobstante, a implantação de todo um sistema de segurança proporcionado pelo servidor ao oferecer o serviço de armazenamento em nuvem computacional, não pode o usuário ser submetido a este produto sem garantias mínimas, seja legal ou contratual. Por outro lado, deve haver por parte do usuário, um grau 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. Segundo Patrícia Peck (2002, p.16):

> A complexidade de tal sistema, do ponto de vista jurídico, está nas relações resultantes dessa interação, principalmente as relações comerciais. Este ambiente de pessoas conectadas tornou-se extremamente propício para o comércio – aqui surge o conceito de e-commerce. A grande vitrine virtual passa a atrair não apenas empresas, mas também profissionais liberais, shopping, consumidores, redes de ensino a distância, hospitais, laboratórios, bancos, corretoras e todo aquele interessado em obter uma informação, colocar um produto ou serviço à venda, ou simplesmente buscar entretenimento. Surgem as comunidades virtuais, os portais horizontais, os portais verticais, os websites institucionais as homepages pessoais, os metamercados de consumidor-consumidor, empresa-consumidor e empresa empresa – uma verdadeira rede de apatriados. Todas essas relações entre pessoas e empresas passam a exigir novas regras, princípios, regulamentos, assim como possibilitam a aplicação de antigos princípios que continuam tão atuais para o direito como eram em sua origem.

Ademais, a instantaneidade da Internet, juntamente com a virtualização dos negócios, eliminou a figura da pessoa do vendedor. Patrícia Peck (2002, p.92) aduz: "O comércio eletrônico é apenas uma evolução da transação eletrônica. Permite que não apenas a transação seja virtual, mas também seus participes e documentos comprobatórios permaneçam virtuais, que ambos se apresentem eletronicamente." Logo, o negócio jurídico dos serviços da Computação em Nuvem carece dos elementos tradicionais dos contratos, entre eles, a pessoalidade, causando a desconfiança do usuário/consumidor.

As relações humanas atuais estão cada vez mais sob a égide da tecnologia da nuvem computacional, que se faz presente em escala cada vez maior na vida, nos lares e também na maior parte dos ambientes de trabalho da sociedade da era digital. Verifica-se, cada vez mais, a existência de uma maciça penetração de dispositivos tecnológicos e de produtos e serviços de *cloud computing*, que servem a trazer maior facilidade e conforto para uma sociedade ávida por mobilidade e informação acessível e instantânea. A sociedade que usa os serviços e produtos da Computação em Nuvem e que, geralmente por falta de

conhecimento tecnológico, acaba não sabendo usá-los corretamente, ocasionando consequências ruins para a segurança da informação.

No Brasil, problema da utilização ignorante dos serviços da Computação em Nuvem possui a tendência de ter proporções um pouco mais graves, pois, apesar de se informatizar cada vez mais, o país não está preparado o consumo consciente da Computação em Nuvem, em razão da existência de uma grande parcela de pessoas que não sabem utilizá-la ou tem bastante dificuldade de interpretá-la e manuseá-la, havendo um analfabetismo digital defendido por Bruno Pires Malaquias (2008, p.2):

> Em todo o mundo, a modernização das sociedades, o desenvolvimento tecnológico, a ampliação da participação social e política colocam demandas cada vez maiores com relação às habilidades de leitura e escrita. A questão não é mais apenas saber se as pessoas sabem ou não ler e escrever, mas também o que elas são capazes ou não de fazer com essas habilidades. Isso quer dizer que, além da preocupação com o analfabetismo, problema que ainda persiste nos países mais pobres e também no Brasil, emerge a preocupação com o alfabetismo, ou seja, com as capacidades e usos efetivos da leitura e escrita nas diferentes esferas da vida social. Ocorre que aquele que não domina a informática é um verdadeiro analfabeto, marginalizado pela rápida evolução tecnológica que possibilita o acesso à informação. O analfabetismo digital é um grande fator de exclusão, que resulta em sérias implicações sociais, políticas, jurídicas e econômicas. Antes se falava que aquele que não fosse devidamente alfabetizado, que não conseguisse interpretar e compreender um texto, estava marginalizado, estigmatizado. Com esteio nesta assertiva, essa tal pessoa não teria sua cidadania exercida plenamente, estando, pois, fadada inexoravelmente a um destino sem perspectivas, restando-lhe somente subempregos.

Entretanto, o usuário/consumidor não poderá ser submetido a um serviço sem uma proteção mínima necessária ao resguardo de seus dados digitais ou informações pessoais, devendo os provedores de serviços de Computação em Nuvem adotar protocolos de segurança. O acesso aos

produtos e serviços da Computação em Nuvem é instantâneo, proporcionado principalmente pela conexão de banda larga de Internet. A possibilidade de um acesso digital rápido provoca uma avalanche de dados sobre os provedores de Computação em Nuvem, os quais devem ter uma estrutura segura para aguentar esta avalanche informacional.

4.2 – Privacidade na Computação Em Nuvem

A tecnologia da computação em nuvem é desenvolvida para ser um sistema autônomo gerenciado de forma transparente para seus usuários. A autonomia dos serviços de computação em nuvem está adstrita, necessariamente, à capacidade de *hardware* e de *software* do provedor que presta o serviço. Dessa forma, tanto os componentes físicos (*hardware*) quanto os abstratos (*software*) podem ser configurados automaticamente. Estas configurações são apresentadas ao usuário como uma imagem única do sistema. Essa autonomia é importante, uma vez que reduz o custo de equipe de monitoramento do sistema.

A ausência de uma grande autonomia a contemplar todas as demandas dos usuários pode ser um empecilho à difusão da tecnologia da computação em nuvem, na medida em que, caso o fornecedor não consiga suportar a carga demandada, poderão existir problemas afetos à fruição do serviço, proporcionando uma propaganda negativa.

O espraiamento da tecnologia da Computação em Nuvem enfrenta o desafio da disponibilidade de serviços, que uma vez que este sistema deve permitir aos usuários a possibilidade de acessar e utilizar a nuvem onde e quando desejarem. É cediço que objetivo da referida tecnologia dá ampla mobilidade e disponibilidade dos serviços.

Inicialmente, pode-se afirmar que o objetivo almejado pela tecnologia debatida é graças à popularização da "*Internet* de banda larga", que proporciona efetivo e instantâneo acesso à rede mundial de computadores, a qualquer momento.

Entretanto, como se trata da *Internet,* podem ocorrer os chamados "sistemas indisponíveis", pois é uma sistema sujeito a falhas e interrupções comuns a qualquer meio de comunicação. Para tanto, os desenvolvedores podem utilizar técnicas de balanceamento de carga dinâmica e composição de nuvens de forma a atender as necessidades dos usuários. Por exemplo, podem-se construir aplicações altamente disponíveis com a implantação de duas ofertas de nuvem diferentes. Caso uma das nuvens falhe, a outra nuvem continua a apoiar a disponibilidade das aplicações. Sobre este assunto, Endler et. al (2011, p.2):

> Por um lado, há um consenso de que um dos grandes entraves para uma adoção mais abrangente desse paradigma está nas atuais limitações da rede internet: a pequena largura de banda de muitas redes de acesso, que inviabilizam a transferência de grandes volumes de dados de, para e entre as

> nuvens, e a deficiência em mecanismos que garantam a qualidade de serviços[...]

Outra característica fundamental da Computação em Nuvem é escalabilidade, já conceituada neste trabalho. As plataformas oferecidas neste sistema podem ser dimensionadas por vários fatores, tais como localizações geográficas, desempenho ou configurações, inobstante as mais diversas limitações de rede e segurança. Esta característica refere-se à capacidade que um computador, produto ou sistema tem de expandir-se para servir a um número maior de usuários sem sofrer pane.

A escalabilidade evidencia que o fornecedor do serviço de nuvem computacional deve investir constantemente na ampliação de suas capacidades e de sua rede, visando atender ao constante fluxo de dados que pode levar, eventualmente, à picos de elevada demanda.

Se o sistema não puder entregar aos usuários o acesso instantâneo aos recursos e informações alocados nos servidores, a "nuvem" poderá ruir por completo, na medida em que a razão de sua existência, como já visto, está calcada no fornecimentos, por terceiros, da estrutura necessária para operar os aparatos eletrônicos, com ênfase no conforto e praticidade para permitir plena fruição de suas benesses.

Os modelos padrões de infraestrutura de tecnologia da informação são limitados, em razão da dificuldade de escalar recursos, ou seja, aumentar ou diminuir, de acordo com as necessidades. Este problema é ligado ao excesso de recursos alocados para atender picos de uso, geralmente resultando em baixa utilização.

Por outro lado, a habilidade de automaticamente escalar uma infraestrutura com baixo ou nenhum impacto para as aplicações que estão sendo executadas, mostra-se como uma das características mais úteis da Computação em Nuvem.

A escalabilidade permite que usuário pague apenas quando utilizam os recursos, sem adicional de custos administrativos para manter os padrões de níveis de serviço na nuvem. Isto é, a partir do momento que os recursos computacionais são gerenciados por meio de softwares, eles podem ser implementados rapidamente de acordo com novas necessidades, buscando atender a uma demanda particular quando solicitados. Outrossim, o autoatendimento possibilita ao usuário de uma aplicação em nuvem de obter os recursos computacionais necessários, ou, no mínimo, o potencial para usar certos recursos computacionais, com um simples pedido.

Outro fator importante para a utilização da Computação em Nuvem é a interoperabilidade, que está ligada à capacidade dos usuários de

executar os seus programas e os seus dados em diferentes nuvens, plataformas e sistemas operacionais. Isso permite, por exemplo, que as aplicações não fiquem restritas a somente um sistema de Computação em Nuvem. Assim, é possível afirmar que interoperabilidade surgiu da necessidade de harmonizar operacionalmente ambientes com redes heterogêneas, compartilhamento de informação e para melhorar a coordenação das tarefas.

Para Dikaiakos et al (2009, p.10/13), a interoperabilidade da nuvem se refere a habilidade de utilizar os mesmos artefatos, como ferramentas de gerenciamento, servidores de imagens virtuais, entre outras, entre a variedade de fornecedores de Computação em Nuvem e plataformas.

Torna-se um desafio para os fornecedores, uma vez que os mesmos devem pensar coletivamente em termos de mercado para oferecer boa capacidade de troca entre as nuvens. Embora o mercado de Computação em Nuvem tenha evoluído, não faltam críticas sobre sua falta de interoperabilidade, gerando receios quanto ao aprisionamento a determinado fornecedor.

Segundo Dikaiakos et al (2009, p.12), a interoperabilidade irá possibilitar que as infraestruturas de Computação em Nuvem evoluam para uma plataforma transparente e mundial, aos quais as aplicações não são restritas para nuvens corporativas.

Empós da análise sobre a interoperabilidade, um outro fator que afigura-se como um dos maiores desafios da Computação em Nuvem é a privacidade. Este fator é um direito constitucionalmente protegido pela Constituição Federal, sob a tutela da dignidade da pessoa humana. Cavalieri Filho (2008, p.80) afirma que as espécies de direitos personalíssimos são incluídas no direito à dignidade:

> Os direitos à honra, ao nome, à intimidade, à privacidade, e à liberdade estão englobados no 'direito à dignidade', verdadeiro fundamento e essência de cada preceito constitucional relativo aos direitos da pessoa humana.
> À luz da Constituição vigente, podemos conceituar o 'dano moral' por dois aspectos distintos. Em 'sentido estrito', dano moral é 'violação do direito à dignidade'. E foi justamente por considerar a inviolabilidade da intimidade, da vida privada, da honra e da imagem corolário do 'direito à dignidade' que a Constituição inseriu em seu art. 5º, V e X, a plena reparação do dano moral.

No presente trabalho, é possível dizer que a privacidade é o direito que indivíduos, grupos ou instituições têm de definir quando, e em que medida, informações a seu respeito pode ser transmitidas a terceiros.

Já no que concerne à privacidade de informação, Ransome e Rittinghouse (2010) propõem uma definição associada ao relacionamento entre coleção e disseminação de dados, tecnologia, expectativa pública sobre a privacidade e aspectos legais envolvidos.

O desafio da privacidade dos dados está no fato de compartilhar dados, porquanto são protegidas as informações próprias que possam identificar organizações e pessoas.

A privacidade na Computação em Nuvem está associada aos direitos que os usuários tem em relação à proteção dos seus dados, pois este sistema tem implicações significativas para a privacidade de informações pessoais, bem como com a confidencialidade de informações de organizações públicas e privadas.

O fornecedor do serviço deve, para manter a privacidade dos usuários, promover a separação de dados confidenciais dos dados não confidenciais, seguido da criptografia de elementos confidenciais. Um exemplo simples é o armazenamento de cartões de créditos. Pode-se ter uma complexa aplicação de comércio eletrônico armazenando muitos relacionamentos entre dados, mas será necessário separar os dados dos cartões de crédito de outros para se iniciar a construção de uma infraestrutura.

Os consumidores que utilizam Computação em Nuvem precisam estar cautelosos em relação à privacidade, uma vez que todo sistema é passível de *hack*. Também é importante ressaltar que os fornecedores devem apresentar garantias sistêmicas de segurança e de privacidade dos dados dos usuários. Ransome e Rittinghouse (2010) enfatizaram que os riscos de privacidade e confidencialidade dos usuários variam significativamente com os termos de serviço e a política de privacidade estabelecida com o fornecedor. Logo, é possível concluir que, em uma comparação entre pequenos e grandes fornecedores, quanto menor a empresa, menores são as garantias oferecidas, uma vez que as maiores empresas possuem maiores estruturas para garantir a privacidade dos dados armazenados.

Intrinsicamente ligado à privacidade, está a segurança dos dados armazenados em Computação em Nuvem. Este desafio envolve políticas, procedimentos e medidas técnicas utilizadas para impedir acesso não autorizado, alteração, roubo ou danos físicos a sistemas de informação.

George Reese (2009) citou alguns pontos que estão relacionados a segurança na Computação em Nuvem, que seriam basicamente: 1) Recuperação de desastres: é capacidade de retomar os sistemas normalmente quando o mesmo enfrenta um cenário de desastre; 2) Segurança dos dados: controle físico define como o usuário controlará o acesso físico aos servidores que suportam sua infraestrutura; 3) Controle dos dados: A diferença entre os data centers tradicionais e a nuvem é a localização dos dados no servidor. Há organizações que terceirizaram seus data centers, migrando para serviços gerenciados pelo sistema de Computação em Nuvem, onde não se possuem a liberdade de ver ou tocar nos servidores onde os dados estão armazenados. O significado desta mudança de alguma maneira, é uma questão emocional, mas não mostra os desafios reais. O consumidor não tem conhecimento de onde os dados estão armazenados, podendo ser considerado um problema por alguns. Assim, um modelo seguro de Computação em Nuvem deve oferecer informações confiáveis em relação a localização dos dados aos usuários; 4) Segurança da Rede: tem relação com as regras de firewall e detecção de entradas não desejadas na rede. Um firewall é um software que protege o perímetro entre um ou mais segmentos de rede. A detecção de entradas não desejadas na rede, por sua vez, monitora o tráfico local para eventuais irregularidades; 5) Segurança do Servidor: o servidor deve estar organizado em relação às tarefas de prevenção de ataques, minimização do impacto de um ataque bem sucedido no sistema como um todo e respostas aos ataques quando eles ocorrerem; 6) Segmentação dos dados: ao presumir que os servidores possuem falhas de segurança, deve-se estar ciente que eventualmente uma delas será comprometida, logo, uma infraestrutura de qualidade deve ser criada e suportada. Na Computação em Nuvem, os dados ficam armazenados com o fornecedores que, consequentemente, devem adotar checagens de seguranças para garantir a seguridade dos dados e prevenir brechas relacionadas a vulnerabilidades na segurança dos aplicativos ou por meio de hackers; 7) Integridade dos dados: é um dos fatores mais críticos em qualquer sistema e é mantida pela base de dados e transações. Em um sistema distribuído, existem múltiplas bases de dados e aplicações. Para manter a integridade dos dados, as transações entre muitas fontes de dados devem ser realizadas de maneira segura; 8) Segregação dos dados: os dados de vários usuários ficam na mesma localidade, sendo que a entrada de dados não desejados pode ser possível. Sistema de Computação em Nuvem deve garantir uma limitação para os dados de cada usuário. 9) Acesso aos dados: primordialmente relacionada a políticas de segurança oferecidas pelos usuários enquanto acessam os dados; 10) Autenticação e autorização: o

software fica sediado fora do firewall da empresa, sendo que muitas vezes as credenciais dos usuários são guardadas nas bases de dados dos provedores e não como parte da infraestrutura de TI da organização. Isso significa que os clientes precisam lembrar-se de remover contas quando funcionários deixam a organização, por exemplo; 11) Confidencialidade dos dados: todo o conteúdo dos usuários deve ser guardado em um único provedor ou vários provedores, e os fornecedores devem assegurar que os dados não serão acessados por outros clientes; 12) Segurança no aplicativo de Internet: o aplicativo de Internet deve ser seguro na medida não possibilitem a invasão por parte de ameaças externas; 13) Violação dos dados: implica na possibilidade dos dados serem perdidos ou violados devido a fatores diversos; 14) Vulnerabilidade da virtualização: envolve garantir que diferentes instâncias, rodando na mesma máquina, estão isoladas umas das outras; 15) Backup: o fornecedor deve garantir que os dados dos clientes serão regularmente copiados em diferentes fontes; 16) Gerenciamento de identidades e processo de entrada: área administrativa relacionada a identificação dos indivíduos que utilizam um sistema e a autorização dos mesmos a utilização do sistema.

É bastante difícil afirmar com certeza qual fornecedor terá melhor ou pior sistema de segurança para a Computação em Nuvem, pois, aliado ao fato de que os dados podem deixar um país e serem alocados sob diferentes leis, podendo se mover ao longo do tempo, não é possível estimar uma classificação entre os fornecedores, mas tão-somente um padrão mínimo de mercado, já que não regulação legal sobre o tema.

A segurança da informação se refere à proteção sobre as informações de uma determinada empresa ou indivíduo, entretanto, existe uma relação inversa entre a privacidade e a segurança, pois quanto maior a segurança coletiva, geralmente menor é a privacidade individual, por exemplo e possível citar s sistemas de monitoramento com vídeo em prédios e ambientes públicos.

As preocupações com a privacidade dentro do modelo de Computação em Nuvem não são recentes, uma vez que esta é uma preocupação recorrente entre os usuários, que não armazenariam suas informações em um servidor sem controles adequados.

A privacidade é um direito à reserva de informações pessoais e da própria vida privada. A proteção atribuída à privacidade pelo Código Civil de 2002[29] realizou-se no capítulo referente aos direitos da

[29] Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.

personalidade e com atenção ao tratamento jurisprudencial. Na menção feita pelo CC2002 à "vida privada", sente-se de imediato o eco da disposição constitucional de proteção à vida privada, presente no artigo 5º, X[30] da Constituição Federal - que, literalmente, protege não somente esta como também a intimidade, a hora e a imagem.

Faz-se importante a discussão dos princípios relativos à privacidade de dados pessoais mantidos em um sistema informacional. Estes princípios foram primordialmente trabalhados pelo estudioso americano Willis H. Ware, que, em 1973, em sua obra *Records, Computers and the Rights of Citizens* (1973), trouxe como conjunto de princípios para a privacidade em um contexto mais amplo: 1) Responsabilidade: uma organização é juridicamente responsável pelas informações pessoais sob o seu controle. É necessária a existência de contratou ou termos sobre responsabilidade de uso prevendo sanções legais em caso do mau uso das informações guardadas; 2) Identificação de objetivos: os objetivos para os quais as informações pessoais são coletadas devem ser identificados pela organização previamente ou enquanto a informação é coletada; 3) Consentimento: é necessário o consentimento dos usuários para a coleta, uso e/ou divulgação de informações pessoais, que não podem ser transferidas para outras entidades, salvo se autorizado e com um nível de proteção adequado; 4) Limite de coleta: a coleta de informação pessoal deverá ser efetuada por meios conhecidos e com amparo legal e será limitada ao necessário para os fins identificados pela organização; 5) Limite de uso, divulgação e retenção: Não poderá haver desvio de finalidade para as informações pessoais coletadas, ou seja, não devem ser utilizadas ou divulgadas para outros fins que não aqueles para os quais foram coletadas, exceto com o consentimento do usuário ou se exigido por lei; 6) Precisão: as informações pessoais deverão ser tão precisas, completas e atualizadas quanto for necessário para os propósitos definidos; 7) Salvaguardas: medidas de segurança adequadas à sensibilidade das informações devem ser usadas para protegê-las, tanto em relação à sua confidencialidade

---

[30] Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

quanto à sua integridade; 8) Transparência: a organização deve tornar disponíveis e transparentes aos indivíduos informações específicas sobre suas políticas e práticas relativas à gestão das informações privadas; 9) Acesso individual: a pedido, todo indivíduo deve ser informado da existência, uso e divulgação de suas informações pessoais e deve ser permitido seu acesso a essa informação; 10) Crítica à Conformidade: um indivíduo deve ser capaz de criticar a precisão e integridade de suas informações e modificá-las se necessário.

Desta forma, a privacidade pode ser definida como o direito de uma pessoa física ou jurídica, agindo em seu próprio nome, de determinar o grau de interação de suas informações com contexto onde se encontra inserida, incluindo o grau de disposição em divulgar essas informações para outras pessoas. Existem basicamente três elementos na privacidade: o sigilo, o anonimato e o isolamento (ou solidão, o direito de ficar sozinho). Sobre o tema, Arlindo Marcon Jr., et al (2010, p.55) afirmam que:

> O direito à privacidade é um conceito consolidado em algumas áreas, como a médica, a jurídica e a fiscal. No contexto médico [Beaver e Harold 2004], a privacidade consiste na limitação do acesso às informações de um indivíduo, ao acesso ao próprio indivíduo ou à sua intimidade. Em outras palavras, é o direito do indivíduo não ter sua vida ou seus dados observados sem autorização. Para os juristas, privacidade é o direito de ficar sozinho [Staples 2007]. A privacidade está atrelada à questão do anonimato, ou seja, à condição de um indivíduo ter suas informações pessoais protegidas [Shirey 2000]. A privacidade também pode ser vista como a capacidade de um usuário realizar ações em um sistema sem ser identificado.

Sobre a privacidade na informática, complementam os autores:

> A definição mais comum e aceita no mundo da informática diz que *a privacidade consiste nos direitos e obrigações dos indivíduos e organizações com relação à coleta, uso, conservação e divulgação de informações pessoais* [Mather et al. 2009]. A privacidade pode ser vista como um aspecto da confidencialidade. A confidencialidade define que uma informação não deve estar disponível ou divulgada a indivíduos,

> entidades ou processos não autorizados pela política de acesso [Shirey 2000]. Por sua vez, a privacidade é a proteção contra a exposição indevida de informações pessoais ou o desejo de controlar o nível de exposição e uso dessas informações. Marcon Jr., et al (2010, p.55)

Inobstante a conceituação de privacidade na informática ser compatível com o consolidado no ordenamento jurídico, os termos de privacidade dos serviços de Internet não dão quaisquer garantias com relação à segurança das informações entregues a estes. Pelo contrário, verifica-se a existência de uma extensa coleta de informações para uso em publicidade, em formação de perfil, em vendas, etc. Por exemplo, destaca-se os termos de privacidade do Google[31], por exemplo:

> **Como usamos as informações que coletamos**
> Usamos as informações que coletamos em todos nossos serviços para fornecer, manter, proteger e melhorar esses serviços, desenvolver novos e proteger a Google e nossos usuários. Também usamos essas informações para oferecer ao usuário um conteúdo específico, por exemplo, fornecer resultados mais relevantes de pesquisa e anúncios.
> Podemos usar o nome que o usuário fornece em seu Perfil do Google em todos os serviços que oferecemos e que exijam uma Conta do Google. Além disso, podemos substituir seus nomes antigos associados com sua Conta do Google de modo que o usuário esteja representado de maneira consistente em todos nossos serviços. Se outras pessoas já tiverem o e-mail ou outras informações que identifiquem o usuário, nós podemos mostrar-lhes estas informações do Perfil do Google que são publicamente visíveis (como nome e foto).
> Se o usuário tem uma Conta do Google, o nome e a foto do perfil, bem como as ações realizadas em aplicativos do Google ou de terceiros que estejam conectados a essa Conta do Google (como marcações +1, avaliações e comentários postados), podem aparecer nos nossos serviços, inclusive para

[31] Política de Privacidade do Google: https://www.google.com/intl/pt-BR/policies/privacy/#infouse. Acessado em 10 de setembro de 2017.

exibição em anúncios e em outros contextos comerciais. Respeitamos as opções de compartilhamento limitado ou configurações de visibilidade que o usuário faz para a Conta do Google.

Quando o usuário entra em contato com a Google, mantemos um registro da comunicação para ajudar a resolver qualquer problema que ele possa estar enfrentando. Podemos usar o endereço de e-mail do usuário para informar a ele sobre nossos serviços, por exemplo, as próximas mudanças ou melhorias.

Usamos as informações coletadas de cookies e de outras tecnologias, como etiquetas de pixel, para melhorar a experiência do usuário e a qualidade geral dos nossos serviços. Um dos produtos que usamos para fazer isso com nossos próprios serviços é o Google Analytics. Por exemplo, quando o usuário salva suas preferências de idioma, nossos serviços aparecem no idioma que o usuário escolhe. Quando exibimos anúncios personalizados, não associamos um identificador proveniente de cookies ou tecnologias semelhantes a categorias sensíveis, como aquelas baseadas em raça, religião, orientação sexual ou saúde.

Nossos sistemas automatizados analisam o conteúdo do usuário (incluindo e-mails) para fornecer recursos de produtos relevantes ao usuário, como, por exemplo, resultados de pesquisa e propaganda personalizados e detecção de spam e malware.

Podemos combinar informações pessoais de um serviço com informações (pessoais inclusive) de outros serviços da Google para facilitar o compartilhamento de informações com pessoas que o usuário conhece, por exemplo. Dependendo das configurações da conta, as atividades do usuário em outros sites e apps podem ser associadas às informações pessoais dele para melhorar os serviços da Google e os anúncios fornecidos por ela.

Solicitaremos sua autorização antes de usar informações para outros fins que não os definidos nesta Política de Privacidade.

A Google processa informações pessoais em nossos servidores de muitos países do mundo.

> Podemos processar as informações pessoais do usuário em um servidor localizado fora do país em que este vive.

Desta forma, verifica-se que o usuário encontra-se desprotegido, à mercê de um sistema de mercado, que vislumbrou na informação, uma mercadoria bastante apreciada e negociada a caro preço. Outrossim, os termos da Política de Privacidade do Google demonstram que os princípios sobre a privacidade podem ser mitigados em razão do pacto, posto que ao assinar tal contrato, o usuário permitirá o uso de seus dados pessoais para as finalidade ali apresentadas.

Genericamente, é possível aduzir que a informação pessoal é termo utilizado de para identificar informações de diferentes indivíduos. Pearson et al. (2009)[32] propõem a caracterização de informações privadas como: a) Informações de identificação pessoa: qualquer informação que pode ser usada para identificar ou localizar um indivíduo (nome ou endereço, por exemplo) ou informações correlacionadas com outras informações para identificação do indivíduo (número de cartão de crédito ou de telefone); b) Informações sensíveis: informações sobre religião, raça, saúde, orientação sexual, partidária, dados financeiros, desempenho profissional ou outras informações similares consideradas privadas. Há também outras informações consideradas sensíveis que possam identificar o indivíduo, como informações biométricas ou imagens de câmeras de vigilância em locais públicos; c) Dados comportamentais: dados coletados a partir do uso do computador ou outros dispositivos, como históricos de navegação na Internet ou contatos de amigos virtuais; d) Dispositivos de identificação única: outros tipos de informação que possam ser identificadas pelo uso de um dispositivo exclusivo do usuário, tais como endereço IP, dispositivos RFID ou tokens de gerência de identidade baseados em hardware.

A privacidade dessas informações possui três aspectos: divulgação, sensibilidade e as partes afetadas. Sob a ótica da divulgação, a privacidade pode ser estabelecida de acordo com o nível de controle que se deseja dar a uma informação, ou seja, para quem o dono da informação deseja permitir o acesso. Por exemplo, a partir do momento que um

[32] PEARSON, S., Shen, Y., e Mowbray, M. (2009). A privacy manager for cloud computing. Em Jaatun, M., Zhao, G., e Rong, C., editores, Cloud Computing, volume 5931 of LNCS, páginas 90–106. Springer.disponível em: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.369.71&rep=rep1&type=pdf. Acessado em 10 de setembro de 2017.

indivíduo divulga uma informação considerada privada a outro indivíduo, este, por sua vez, terá poder de divulgar a terceiros se assim o desejar. Já, em relação à sensibilidade, pode-se considerada sensível qualquer informação que possibilite uma violação de segurança, isto é, uma violação da integridade, disponibilidade ou confidencialidade.

A sensibilidade da informação é exemplificada como dados pessoais sobre opiniões religiosas, políticas, condições de saúde ou origem. As partes afetadas podem ser indivíduos, empresas, organizações, governos, etc., que atribuem níveis de sensibilidade às suas informações, por exemplo, um hospital considera as informações sobre seus pacientes como privadas, enquanto um país considera privadas as informações militares ou diplomáticas.

Para a Computação em Nuvem, a privacidade é uma importante propriedade, uma vez que é uma questão-chave e precisa ser considerada em todas as fases de adoção deste ambiente informático. Os riscos e ameaças à privacidade diferem de acordo com o uso da computação em nuvem, como, por exemplo: o usuário de serviços em nuvem poderia ser forçado ou persuadido a aceitar o monitoramento das suas atividades ou a fornecer informações pessoais contra sua a vontade; o usuário poderia ver suas informações armazenadas na nuvem perdidas ou divulgadas indevidamente.

Grosso modo, é possível afirmar que a proteção da privacidade de dados pessoais pode ser realizada através de leis de proteção à privacidade definidas por cada governo ou por tratados internacionais, uma vez que os requisitos de privacidade variam de países. Também, através da auto-regulamentação de práticas leais entre organizações e usuários, consubstanciados em códigos de conduta promovidas para manipular informações; por tecnologias que aumentem a privacidade; e, por último, pela educação sobre privacidade a usuários e profissionais de Tecnologia da Informação. Infelizmente, a privacidade é muitas vezes mal gerida e, por consequência, ocorrem abusos no uso das informações. Essa má gerência da privacidade se dá pela inobservância de alguma das medidas de proteção acima expostas.

Os serviços oferecidos através da Computação em Nuvem são heterogêneos e podem utilizar atributos distintos para a identificação dos usuários. Deste modo, surgem problemas de interoperabilidade entre as aplicações, que podem ir desde o uso de *token*[33] de identidade diferentes

[33] Token é um dispositivo eletrônico gerador de senhas, geralmente sem conexão física com o computador, podendo também, em algumas versões, ser conectado a uma porta USB.

ou o uso de informações diferenciadas para identificar o usuário, como C.P.F. ou e-mail, por exemplo.

O uso de informações diferentes para montar uma identidade cria outro problema: a heterogeneidade de identidades, que ocorre quando usuários e provedores de serviços usam vocabulários diferentes para os atributos de uma identidade. Essa multiplicidade de identidades diferentes dificulta a utilização da Computação em Nuvem, pois o usuário pode fornecer informações desnecessárias ou mesmo erradas para um provedor. A utilização de um gerenciador de identidades para identificar o usuário dificulta a violação da privacidade do mesmo. Logo, a utilização de gerenciador de identidade (IdM) associado a um protocolo de privacidade, que utilize técnicas de criptografia e ontologias, facilitaria a identificação precisa do usuário nos vários serviços da nuvem.

Arlindo Marcon Jr., et al (2010, p. 60) relata a proposta de considerar a privacidade como um serviço da Computação em Nuvem (*Privacy as a Service* – PasS):

> O trabalho [Itani et al. 2009] apresenta uma proposta para assegurar a privacidade das informações pessoais dos usuários na nuvem, observando a legislação correspondente. Conhecido como Privacy as a Service (PasS), o projeto é baseado em um conjunto de protocolos de segurança, com processamento e auditoria das informações sensíveis através de processadores criptográficos. Os processadores criptográficos são indicados por serem invioláveis e à prova de falsificação (de forma análoga ao TPM), de acordo com as especificações definidas em [FIPS 140-2 2001]. Esses processadores são posicionados em um domínio de execução seguro e confiável dentro da infraestrutura da nuvem, devendo estar física e logicamente protegidos contra acessos não-autorizados.
>
> O modelo proposto é baseado em uma solução de nuvem típica composta de duas partes: um provedor, que gerencia e opera uma infraestrutura de nuvem para armazenamento e serviços, e um usuário, que utiliza o armazenamento na nuvem e os recursos remotos para processamento de dados. O projeto oferece ao usuário o controle completo sobre os mecanismos de privacidade aplicados às

> informações na nuvem. O serviço de privacidade proposto baseia-se no grau de sensibilidade das informações do usuário para definir os níveis de confiança no provedor do serviço. O serviço de privacidade oferece suporte a três níveis de confiança:
> 1. Confiança total: este nível se aplica às informações não-sensíveis, que podem ser processadas e armazenadas na nuvem sem uso de criptografia. O provedor é considerado totalmente confiável para o armazenamento e processamento de informações deste nível.
> 2. Confiança parcial: este nível envolve as informações que precisam ser armazenadas cifradas, seja por questões jurídicas ou por regras de conformidade (como registros médicos ou de transações financeiras, por exemplo). Neste nível o consumidor confia no provedor para armazenar suas informações cifradas utilizado chaves fornecidas por ele.
> 3. Sem confiança: este nível aplica-se a informações sensíveis que devem ser ocultadas do provedor. Este tipo de informação deve ser armazenado cifrado, usando chaves criptográficas especificadas pelo usuário e transformadas em repositórios isolados na nuvem. Esses repositórios são configurados, distribuídos e mantidos por um terceiro confiável compartilhado pelo provedor e pelo usuário.

A existência de um gama de provedores de serviços de Computação em Nuvem possibilita aos usuários acessar serviços diversos, entretanto na troca de informações entre as aplicações heterogêneas de serviços diferentes, surge o problema da violação da privacidade, com a indevida divulgação de informações pessoais. A solução deste problema reside na criptografia dos dados pessoais compartilhados, através de um algoritmo de anonimato. A circulação de dados pessoais nos sistemas de Computação em Nuvem acaba por exigir o uso da criptografia.

Como já afirmado outrora, a Computação em Nuvem traz redução de gastos com recursos locais da empresa, porém existem diversos riscos associados à adoção deste sistema porque é necessária a delegação do controle sobre os dados para entidades terceirizadas, surgindo a

necessidade forte de confiança do usuário/consumidor no provedor e vice-versa, pois se o provedor armazena dados cifrados, pode estar fornecendo um repositório para material criminoso, por exemplo, por outro lado se o consumidor não cifra seus dados pode ter sua privacidade violada intencional ou acidentalmente.

Ademais, a disponibilidade é uma das mais vigentes preocupações em serviços da Computação em Nuvem, pois podem ocorrer períodos de inatividade ocasionados por falhas de comunicação de softwares ou por ataques de *hackers*. O armazenamento de dados em locais remotos necessita de garantias de integridade fornecidas pelo provedor da nuvem. Logo, o mal funcionamento de um programa no provedor pode liberar o acesso aos dados privados do consumidor. Quando vários usuários utilizam um mesmo provedor de maneira colaborativa, a consistência durante o acesso concorrente aos recursos também deve ser garantida.

A padronização das aplicações de Internet (APIs) permitirá que desenvolvedores implantem serviços com portabilidade ou compatibilidade para armazenamento de dados em diversos provedores de Computação em Nuvem. Desta forma, é possível desenvolver técnicas de replicação ou *backup* para não depender integralmente de um único provedor, pois se este falhar o consumidor poderá acionar seu plano de contingência, recuperando cópias dos dados de outro provedor. Esta padronização também permitirá que os mesmos *softwares* sejam utilizados em nuvem privada e pública.

Atualmente, cada nuvem possui sua própria solução para o gerenciamento de identidades. A crescente demanda por segurança e conformidade com leis e políticas também pode ser uma boa razão para a utilização de Computação em Nuvem, pois somente o provedor de serviços em nuvem deverá ser capaz de arcar com os custos para fornecer elevados níveis de segurança para um grande número de consumidores.

4.3 - Responsabilidade jurídica dos provedores de Computação em Nuvem sob a ótica do Marco Civil da Internet

Após uma breve exposição acerca da possibilidade de falha no serviço ou produtos da Computação em Nuvem em razão do analfabetismo digital de algumas pessoas, o que pode ocasionar uma divulgação indevida ou corrupção de dados digitais, será iniciada a análise da responsabilização jurídica dos provedores de sistema de Computação em Nuvem, quando a falha se dá por culpa destes, podendo ocasionar graves prejuízos aos direitos de personalidade do indíviduo.

A teoria dos direitos da personalidade, surgida no século XIX, foi criada por Otto Von Gierk e sua denominação jurídica foi aperfeiçoada com decorrer da evolução do Direito. Em Roma, por exemplo, a proteção jurídica era dada à pessoa, no que concerne aos aspectos fundamentais da personalidade, como a *actio iniuriarium*, que era dada à vítima de delitos de *iniuria*, que poderia ser qualquer agressão física como também, a difamação, a injúria e a violação de domicílio.

Neste sentido, há de ser observado que já havia, em Roma, a tutela de diversas manifestações da personalidade, apenas não apresentando a mesma intensidade e o mesmo aspecto que hoje, principalmente devido à diferente organização social daquele povo, distantes e desprendidos da visão individualista que possuímos de nossa pessoa, e da inexistência de tecnologia e aparelhos que viessem a atacar e violar as diversas manifestações da personalidade humana. A contribuição do pensamento filosófico grego para teoria dos direitos da personalidade reflete-se no dualismo entre o direito natural, ordem superior criada pela natureza, e o positivo, leis estabelecidas pelos homens, sendo o homem a origem e razão de ser da lei e do direito.

Posteriormente, no Cristianismo, desenvolveu-se a ideia da dignidade humana, reconhecendo a existência de um vínculo entre o homem e Deus, que estava acima das circunstâncias políticas as quais determinavam, em Roma, o conceito de pessoa - *status libertatis, civitatis* e familia.

Em verdade, foi, particularmente, na Idade Média que se lançaram as sementes de um conceito moderno de pessoa humana, baseado na dignidade e na valorização do indivíduo como pessoa. Tais ideais foram desenvolvidos no Renascimento e no Humanismo, ambos do século XVI. Entretanto, foi no Iluminismo, séculos XVII e XVIII, onde se desenvolveu a teoria dos direitos subjetivos que consagra a tutela dos direitos fundamentais e próprios da pessoa humana (*ius in se ipsum*).

Finalmente, a proteção da pessoa humana, veio consagrada nos textos fundamentais que se seguiram, como o *Bill of Rights*, em 1689, a Declaração de Independência das Colônias inglesas, em 1776, a Declaração dos Direitos do Homem e do Cidadão, proclamada em 1789, com a Revolução Francesa, culminando na mais famosa, a Declaração Universal dos Direitos do Homem, votada em 1948, pela Assembléia Geral da ONU, que se constituem em verdadeiros marcos históricos da construção dos direitos da personalidade.

No Brasil, a Constituição Imperial, de 1824, já trazia alguns precedentes acerca dos direitos da personalidade, como a inviolabilidade da liberdade, igualdade e o sigilo de correspondência. A primeira

Constituição Republicana, de 1891, acrescentaria, por sua vez, a tutela dos direitos à propriedade industrial e o direito autoral, ampliando-se o seu regime nas de 1934 e 1946.

Foi com o advento da Constituição Federal de 1988, que os direitos da personalidade foram acolhidos, tutelados e sancionados, tendo em vista a adoção da dignidade da pessoa humana, como princípio fundamental da República Federativa do Brasil, o que justifica e admite a especificação dos demais direitos e garantias, em especial dos direitos da personalidade, expressos no art. 5º, X, que diz:

> Art. 5º. Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> …
>
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação;

O Código Civil Brasileiro, por sua vez, em consonância com a prescrição constitucional e com as novas relações sociais que reclamaram à necessidade da tutela dos valores essenciais da pessoa, dedicou capítulo especial (Capítulo II, artigos 11 ao 21) aos direitos da personalidade. Assim, assentes na legislação atual, os direitos da personalidade são disciplinados e protegidos, pela Constituição Federal, pelo Código Civil de 2002, bem como pelo Código Penal e ainda, em sede de legislação especial, como a Lei de Imprensa, a Lei dos Transplantes, dos Direitos Autorais etc.

Então é possível concluir que, inevitavelmente, em face dos princípios, normas e conceitos que formam o sistema brasileiro dos direitos da personalidade, a tutela jurídica dessa matéria se estabelece em nível constitucional, civil e penal. Em resumo, é imperioso aduzir que a teoria dos direitos da personalidade, assim como suas formas de tutela, evoluiu progressivamente à medida que se desenvolveram as idéias de valorização da pessoa humana, sendo que os direitos da personalidade adquiriram tanto mais revelo quanto se distinguiu, na pessoa humana, o elemento incorpóreo da dignidade, qual seja um conjunto dos direitos personalíssimos atribuídos à pessoa humana.

Recentemente tornaram-se direito subjetivo e segundo Maria Helena Diniz (2002), o direito da personalidade é o direito da pessoa de defender o que lhe é próprio, como a vida, a identidade, a liberdade, a imagem, a privacidade, a honra, etc.

A conceituação de Direito da Personalidade é bastante difícil de ser feita, pois não há unanimidade na doutrina a respeito do conceito dos direitos personalíssimos. Então, será feita uma análise dos elementos dos direitos da personalidade com o intuito de buscar um conceito científico deste rol de direitos.

O primeiro elemento é a personalidade, um conjunto de atributos próprios da pessoa humana, que traz, em sua concepção jurídica, a capacidade jurídica de adquirir direitos e obrigações. Boa parte da doutrina afirma que os direitos da personalidade somente são inerentes à pessoa humana, física, pois, conforme o entendimento doutrinário, somente o ser humano é passível de direito à vida, à honra, à imagem etc. Sendo, então, a pessoa humana o segundo elemento para a configuração do conceito dos direitos personalíssimos. E o último elemento é a imaterialidade dos bens tutelados pelos direitos personalíssimos, como a vida, a honra, ao nome, a imagem etc.

Com a soma dos elementos acima, podemos, então, conceituar os direitos personalíssimos ou da personalidade, como direitos inerentes aos atributos, qualidade, ou características físicas ou mentais, sem cunho econômico direto ou imediato, da pessoa humana.

É oportuno ressaltar que tais direitos são inatos e vitalícios, pois se originam com o nascimento da pessoa humana e extinguem-se com sua morte. São, ainda, imprescritíveis, inalienáveis e absolutos, porque perduram enquanto durar a personalidade; não são, em regra, objetos alienação, ou seja, estão fora do comércio; bem como podem ser oposto *erga omnes*, respectivamente.

O Direito, ao tutelar a dignidade da pessoa humana, busca proteger todas as pessoas contra a ação ou omissão de outrem. Estas ações, quando não reprimidas, ocasionam lesões, danos de ordem material ou moral ou até mesmo ambas, concomitantemente. Saliente-se que, por causa desta sua função de protetor social, o Estado tem o dever (ônus) de punir os agentes danosos. A responsabilidade pelos atos praticados será diferenciada em civil ou penal, em virtude da norma violada pelo agente causador do dano. Se a norma infringida for de caráter público, o agente deverá ser responsabilizado penalmente, posto que qualquer ofensa "direta" à sociedade, vítima genérica de todos os ilícitos, configura-se crime. Ao passo que se a violação for decorrente de norma de direito

privado, a responsabilidade será civil, haja vista não haver dano "direto" à sociedade, mas, sim, ao particular.

A responsabilidade pelos atos praticados será diferenciada em civil ou penal, em virtude da norma violada pelo agente causador do dano. Se a norma infringida for de caráter público, o agente deverá ser responsabilizado penalmente, posto que qualquer ofensa "direta" à sociedade, vítima genérica de todos os ilícitos, configura-se crime. Ao passo que se a violação for decorrente de norma de direito privado, a responsabilidade será civil, haja vista não haver dano "direto" à sociedade, mas, sim, ao particular. Em muitos casos, as duas responsabilidades se confundem entre si, pois, raramente, uma pessoa ao causar dano a outrem, não prejudicará à sociedade.

Na seara da Informática Jurídica, a publicação da Lei 12.965/2014, que institui o "Marco Civil da Internet", foi bastante relevante para a proteção dos direitos de personalidade, uma vez que, construído como um verdadeiro tratado, é referenciado como "Constituição da Internet", por dispor de princípios, garantias, deveres e direitos para o seu uso no país. O Marco Civil não pode ser considerado como uma ilha normativa deserta, isolada das demais fontes jurídicas. Dever ser visto como um ponto de irradiação normativa que disciplina o comportamento dos indivíduos no mundo virtual.

A Constituição Federal, como lei fundamental do nosso país, impõe as coordenadas principiológicas do ordenamento jurídico, ao fluxo da qual tramitarão as interpretações que chegarão ao Marco Civil da Internet. Trata-se de uma consequência do que se convencionou como a constitucionalização do diversos ramos do Direito.

Os demais diplomas, como o Código de Defesa do Consumidor, Código Civil e outros mais, não serão ignorados, mas serão igualmente estimados na regulação dos fatos jurídicos cibernéticos, conforme convite expresso do parágrafo único do art. 3º e o art. 6º[34] da nova lei. Ademais,

---

[34] Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
...
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. 6º Na interpretação desta Lei serão levados em conta, além dos fundamentos, princípios e objetivos previstos, a natureza da internet, seus usos e costumes particulares e sua importância para a promoção do desenvolvimento humano, econômico, social e cultural.

por regular normas de direito civil, é possível concluir que o novel diploma legal não cuida da responsabilização penal dos agentes envolvidos, cujos tipos penais permanecem sendo aqueles já previstos no Código Penal e na legislação extravagante.

A resposta para eventuais conflitos entre o Marco Civil da Internet e outros diplomas legais não deverão ser feitas apenas nos critérios tradicionais de solução de antinomias de normas, como o da especialidade, mas também na moderna teoria do Diálogo das Fontes, idealizada na Alemanha pelo jurista Erik Jayme, fartamente acatada pela doutrina e pela jurisprudência do STJ.

A Carta Magna prevê em seu art. 5°, XXXII, que o Estado promoverá, na forma da lei, a defesa do consumidor. Desta maneira, o Código de Defesa do Consumidor rege as relações de consumo, protegendo o consumidor, que figura como parte vulnerável desta relação. Por sua vez, o consumidor eletrônico não se vê desamparado, primeiramente pelo fato de que deles se refere à aplicabilidade imediata do Código de Defesa do Consumidor, e ainda, por dizer respeito ao princípio geral da boa fé, devendo direcionar toda a conduta do homem, sobretudo às instituídas no Marco Civil da Internet.

A responsabilidade criminal não pode ser dividida, e o poder estatal de punir que infrinjam as normas de caráter público, respeitados as garantias individuais constitucionais, chama-se de *jus puniendi*.

A responsabilidade civil, por seu turno, pode ser dividida em duas, que são classificadas em responsabilidade extracontratual e contratual. A primeira é inerente a qualquer dano ou violação de direito em decorrência de ato ilícito, não havendo, pois, a conjugação de vontades entre as pessoas envolvidas na relação jurídica, ou um negócio jurídico preexistente. Já a responsabilidade contratual é decorrente de relação obrigacional, ou seja, o dever de reparar algum dano é oriundo de dever obrigacional não cumprido. É preciosa a lição de Sergio Cavalieri Filho (2008, p.15):

> se preexiste um vínculo obrigacional, e o dever de indenizar é conseqüência do inadimplemento, temos a responsabilidade contratual, também chamada de ilícito contratual ou relativo; se esse dever surge em virtude de lesão a direito subjetivo, sem que entre o ofensor e a vítima preexista qualquer relação jurídica que o possibilite, temos a responsabilidade extracontratual, também chamada de ilícito aquiliano ou absoluto.

A responsabilização jurídica na seara do Marco Civil da Internet pode ser oriunda tanto de relação jurídica contratual, que se delineia pela relação provedor-consumidor; como extracontratual, porém o provedor não poderá ser punido por dano decorrente de conteúdo gerado por terceiro, salvo se não tiver tomado providências para retirar o conteúdo ofensivo da rede, nos termos da Seção III do Capítulo III da Lei 12.965/2014.[35]

---

[35] Da Responsabilidade por Danos Decorrentes de Conteúdo Gerado por Terceiros
Art. 18. O provedor de conexão à internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros.
Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário.
§1º A ordem judicial de que trata o caput deverá conter, sob pena de nulidade, identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material.
§2º A aplicação do disposto neste artigo para infrações a direitos de autor ou a direitos conexos depende de previsão legal específica, que deverá respeitar a liberdade de expressão e demais garantias previstas no art. 5º da Constituição Federal.
§3º As causas que versem sobre ressarcimento por danos decorrentes de conteúdos disponibilizados na internet relacionados à honra, à reputação ou a direitos de personalidade, bem como sobre a indisponibilização desses conteúdos por provedores de aplicações de internet, poderão ser apresentadas perante os juizados especiais.
§4º O juiz, inclusive no procedimento previsto no §3º, poderá antecipar, total ou parcialmente, os efeitos da tutela pretendida no pedido inicial, existindo prova inequívoca do fato e considerado o interesse da coletividade na disponibilização do conteúdo na internet, desde que presentes os requisitos de verossimilhança da alegação do autor e de fundado receio de dano irreparável ou de difícil reparação.
Art. 20. Sempre que tiver informações de contato do usuário diretamente responsável pelo conteúdo a que se refere o art. 19, caberá ao provedor de aplicações de internet comunicar-lhe os motivos e informações relativos à indisponibilização de conteúdo, com informações que permitam o contraditório e a ampla defesa em juízo, salvo expressa previsão legal ou expressa determinação judicial fundamentada em contrário.
Parágrafo único. Quando solicitado pelo usuário que disponibilizou o conteúdo tornado indisponível, o provedor de aplicações de internet que exerce essa

Antes da edição da Constituição da Internet, o Superior Tribunal Justiça consolidou o entendimento de que a responsabilidade do provedor surgiria a partir do momento em que se omitisse perante notificação extrajudicial por parte daquele que se sentiu ofendido[36]. No entanto, o artigo 19 do Marco Civil atribuiu um novo ônus àqueles que se sentirem ofendidos, qual seja, a necessidade, em regra, de que a pessoa ofendida ingresse com ação judicial exigindo a retirada do conteúdo, sendo que o provedor apenas pode ser responsabilizado civilmente caso descumpra essa ordem. Este ônus é excetuado pela regra do artigo 21, que impõe o dever ao provedor de aplicações de internet de retirar, após notificação do usuário ou de seu representante legal para retirar o conteúdo ofensivo, como nudez ou atos sexuais de caráter privado, por exemplo.

---

atividade de forma organizada, profissionalmente e com fins econômicos substituirá o conteúdo tornado indisponível pela motivação ou pela ordem judicial que deu fundamento à indisponibilização.

Art. 21. O provedor de aplicações de internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo.

Parágrafo único. A notificação prevista no caput deverá conter, sob pena de nulidade, elementos que permitam a identificação específica do material apontado como violador da intimidade do participante e a verificação da legitimidade para apresentação do pedido.

[36] AGRAVO REGIMENTAL. AGRAVO DE INSTRUMENTO EM RECURSO ESPECIAL. AÇÃO DE INDENIZAÇÃO POR DANOS MORAIS DECORRENTES DO USO DE PERFIL FALSO EM REDE SOCIAL DA INTERNET. REEXAME DO CONJUNTO PROBATÓRIO. INCIDÊNCIA DA SÚMULA 7 DESTA CORTE. DECISÃO AGRAVADA MANTIDA. IMPROVIMENTO.

1.- Alterar a conclusão do Acórdão quanto ao fato de que a responsabilidade da requerida limita-se aos caso em que, devidamente notificada deixa de retirar as informações, importa reexame de quadro probatório.

2.- O Agravante não trouxe qualquer argumento capaz de modificar a conclusão alvitrada, a qual se mantém por seus próprios fundamentos. Incidência da Súmula 7 desta Corte.

3.- Agravo Regimental improvido" (AgRg no AREsp 216.878/RS, Rel. Ministro SIDNEI BENETI, TERCEIRA TURMA, julgado em 16/10/2012, DJe 05/11/2012)

Ademais, procedendo a uma interpretação lógica, é possível vislumbrar que o Marco Civil não exige ordem judicial para a remoção de conteúdo da Internet, uma vez que o provedor de aplicações de internet poderá indisponibilizar ou remover determinado conteúdo se houver ofensa aos termos de uso e políticas da plataforma. O artigo 19 é um dispositivo sobre o regime de responsabilidade adotado pela Lei e não sobre requisitos para remoção de conteúdo. Logo, por envolver a existência de um conteúdo que pode ser reconhecido como ilícito pelo Judiciário, pode o provedor antecipar-se e remover o conteúdo ofensivo. O Marco Civil condiciona a responsabilidade civil dos provedores de aplicações ao não cumprimento de uma ordem judicial específica. Essa afirmação em nada impede os provedores de criarem regras que definam o que pode e o que não pode ser exibido em sua plataforma. Sendo assim, se um provedor receber uma notificação apontando que um determinado conteúdo é ilícito, ele terá liberdade para decidir se deve ou não mantê-lo. Todavia, se mantiver o conteúdo, poderá ser alvo da ação judicial, ora comentada.

No âmbito da responsabilização contratual, o Marco Civil estipula que os provedores responsáveis pela guarda de registros de conexão, de acesso a aplicações de internet, de dados pessoais e do conteúdo de comunicações privadas deverão proteger os dados de seus usuários, de acordo como artigo 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." Esta proteção tem por finalidade a preservação da intimidade, da privacidade, da honra e da imagem dos usuários, sendo certo que a disponibilização dessas informações somente se dará por ordem judicial, ressalvada a possibilidade, pelas autoridades administrativas, como Ministério Público, Receita Federal etc.

O descumprimento dos deveres mínimos estipulados importará na aplicação das seguintes sanções estipuladas no artigo 12, além daquelas já previstas em outros diplomas legais, aplicáveis conforme a gravidade, a natureza da infração e os danos resultantes. Dentre outras circunstâncias as sanções variam de advertência, multa de até 10% do faturamento da empresa responsável até a suspensão temporária das atividades de coleta, armazenamento, guarda e tratamento de registros e dados pessoais ou de comunicações, ou, ainda, a proibição de exercício dessas atividades. Entretanto, não restou claro qual será o órgão incumbido de aplicar tais

sanções, restando ao Poder Judiciário apontar a competência para a aplicação das sanções:

> 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.

A guarda desses registros sob sigilo deve ser mantida pelo prazo de um ano, conforme dispõe o artigo 13[37] do Marco Civil, ressalvada a

[37] Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.
§1º A responsabilidade pela manutenção dos registros de conexão não poderá ser transferida a terceiros.
§2º A autoridade policial ou administrativa ou o Ministério Público poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no caput.
§3º Na hipótese do § 2o, a autoridade requerente terá o prazo de 60 (sessenta) dias, contados a partir do requerimento, para ingressar com o pedido de autorização judicial de acesso aos registros previstos no caput.
§4º O provedor responsável pela guarda dos registros deverá manter sigilo em relação ao requerimento previsto no §2º, que perderá sua eficácia caso o pedido

possibilidade dessas mesmas autoridades requererem a preservação desses dados por prazo superior.

Outrossim, a lei vedou expressamente, nos termos do artigo 14[38], a guarda dos registros de acesso de aplicações de Internet por parte do provedor de conexão, ou seja, este deverá se restringir somente a possibilitar o acesso à rede mundial. Por outro lado, os dados de acesso às aplicações de Internet ficará sob a guarda de seus provedores próprios, constituídos por pessoa jurídica regular para exercer suas atividades, nos termos do artigo 15 do Marco Civil, que, por sua vez, traz os deveres de guarda e proteção do sigilo de dados dos usuários de aplicações de Internet:

> Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.
> §1º Ordem judicial poderá obrigar, por tempo certo, os provedores de aplicações de internet que não estão sujeitos ao disposto no caput a guardarem registros de acesso a aplicações de internet, desde que se trate de registros relativos a fatos específicos em período determinado.
> §2º A autoridade policial ou administrativa ou o Ministério Público poderão requerer cautelarmente a qualquer provedor de aplicações de internet que os registros de acesso a aplicações de internet sejam guardados, inclusive por prazo superior ao

---

de autorização judicial seja indeferido ou não tenha sido protocolado no prazo previsto no §3º.
§5º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.
§6º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência.

[38] Art. 14. Na provisão de conexão, onerosa ou gratuita, é vedado guardar os registros de acesso a aplicações de internet.

> previsto no caput, observado o disposto nos §§ 3º e 4º do art. 13.
> §3º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.
> §4º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência.

Como estipulado no artigo 13, o dispositivo normativo do artigo 15, §2º permite que a autoridade policial ou administrativa ou o Ministério Público poderão requerer que a guarda desses dados permaneça por prazo superior, cuja disponibilização, de qualquer forma, dependerá de ordem judicial. Ficam vedadas, ainda, a guarda de dados pessoais que excedem a finalidade para a qual o titular deu seu consentimento, além da guarda dos registros de acessos a outras aplicações sem o consentimento do titular.

A responsabilidade jurídica dos provedores de *cloud computing* decorre do fato de que, alheio à necessidade de tomar todos os cuidados com relação à contratação do serviço, não permita que uma situação de vulnerabilidade que possa cheguar a um patamar insustentável clamando a intervenção estatal pelo Judiciário para tentar restabelecer o equilíbrio contratual. Ou seja, ocorrendo qualquer ilícito, através da falha na prestação de serviços, em que possa resultar danos morais e materiais aos usuários/consumidores de computação em nuvem, o instituto da responsabilidade civil deve ser amplamente utilizado, ainda mais em se tratando de relações de consumo, onde o consumidor é parte mais fraca da relação e deve ser amplamente protegido com base nos direitos fundamentais constitucionais.

Logo, a falha na prestação de serviços na Computação em Nuvem não deixa de ser uma violação ao dever de atendimento à teoria de qualidade, corolário da relação de consumo que, na verdade, se traduz num verdadeiro processo que se inicia com a oferta e se desdobra em tantas fases quantas forem as etapas a serem cumpridas antes, durante e após o cumprimento do contrato, mas que se relacionam ao atendimento das legítimas expectativas do consumidor.

4.4 – Aplicação da Lei brasileira no tocante da responsabilidade jurídica dos provedores de Computação em Nuvem sediados em país estrangeiro

Após a análise sobre a responsabilidade jurídica dos provedores de aplicação de Computação em Nuvem, faz-se necessário um estudo sobre a aplicação da legislação nacional a provedores sediados em país estrangeiro.

Primeiramente, é importante ressaltar que não há qualquer discrepância jurídica quando se falar em provedor de Computação em Nuvem sediado no Brasil, pois é sobejamente óbvia a aplicação da lei nacional. A celeuma recai sobre a aplicação da legislação brasileira em face de entidades que não estão em solo nacional ou da possibilidade de utilização da legislação estrangeira para o consumidor brasileiro.

Assim, é possível a indagação: caso um usuário/consumidor domiciliado no Brasil acessa, via internet, um provedor de aplicações de internet sem filial no País e tenha a privacidade de seus dados aviltada pelo fornecedor do serviço, seja por erro, dolo ou culpa em *stricto sensu*, qual a lei deveria ser aplicada?

Primeiramente, é necessário, para facilitar a didática do presente estudo, apresentar os cenários normativos anterior e posterior à sanção do Marco Civil da Internet.

Num cenário anterior à promulgação do Marco Civil da Internet, quando um usuário domiciliado no Brasil acessa um provedor de aplicações de Internet, em que guarda e armazena dados importantes, estaria celebrando um contrato regido pela legislação estrangeira, conforme aregra do artigo 9º, §2º da Lei de Introdução às Normas do Direito Brasileiro:

> Art. 9º Para qualificar e reger as obrigações, aplicar-se-á a lei do país em que se constituirem.
> §1º Destinando-se a obrigação a ser executada no Brasil e dependendo de forma essencial, será esta observada, admitidas as peculiaridades da lei estrangeira quanto aos requisitos extrínsecos do ato.
> §2º **A obrigação resultante do contrato reputa-se constituida no lugar em que residir o proponente**. (destaque do autor)

De acordo com a LINDB, o usuário não poderá invocar, de modo algum, a legislação brasileira, como, por exemplo, o Código de Defesa do Consumidor, uma vez que este contrato se equivaleria ao que seria

celebrado pessoalmente em território estrangeiro – *locus regit actum*. Nos termos do artigo 9º da LINDB, aplica-se a lei do local da celebração do contrato e o cumprimento de suas formalidade. Assim, se tiver de ser a obrigação cumprida no Brasil, entretanto, e depender de forma essencial na nossa lei, esta deverá ser observada, além das normas estrangeiras. Entretanto, se não se puder determinar o local de constituição do contrato, reputa-se este constituído no local onde residir o proponente.

Para Amorim (1995, p.45):

> Em razão desta disposição, alguns doutrinadores são de opinião que o sistema jurídico brasileiro de aplicação da lei estrangeira, pelo simples fato de aceitar as peculiaridades desta mesma lei, quanto aos requisitos extrínsecos do ato, acabou por abrir uma exceção à imperatividade da regra *lócus regit actum*.

Santos (2011, p.66) assevera que:

> Tanto a doutrina quanto a jurisprudência admitem que contratos realizados no estrangeiro, com indicação da lei brasileira a ser observada, são plenamente válidos. A LICC de 1916 permitia entender-se aceita a autonomia da vontade, pois prescrevia, no caput do artigo 13, a regulação das obrigações quanto à substância e aos seus efeitos pela lei do lugar em que fossem contraídas, salvo estipulação em contrário. A supressão dessa expressão pela LICC, em 1942, que se manteve na LINDB, significa, para alguns autores, que os contratantes não podem dispor de sua vontade, enquanto outros afirmam que o silêncio da nova norma mantém o princípio jurídico até então admitido.

Do ponto de vista processual, o usuário, se se sentir lesado, poderia ajuizar, no Brasil, ação judicial contra o provedor de aplicações alienígena. O juiz brasileiro, por meio de carta rogatória, promoveria a citação da empresa. Essa carta rogatória seria encaminhada ao Estado estrangeiro, que, nos termos de seu ordenamento, promoveria a citação ou recusaria o pedido. O magistrado brasileiro, após essas comunicações processuais, daria curso ao feito e, ao final, proferiria sentença, julgando o caso de acordo com a legislação estrangeira. Se a empresa alienígena

fosse condenada, a execução dessa sentença ocorreria por intermédio do mecanismo de carta rogatória. O direito brasileiro regula, expressamente, como o juiz deve aplicar o direito estrangeiro.

Embora o teor da lei não seja muito claro, é possível concluir de que a lei estrangeira deve ser conhecida por todos os envolvidos na celeuma, e o juiz deve aplicá-la, em princípio de ofício, porém, caso a desconheça poderá exigir de quem a invoca prova do texto e da vigência, conforme o estipulado no artigo 14 da LINDB.

No que tange à contratação de provedores de aplicação de Computação em Nuvem com filial no Brasil, o contrato será regido pela legislação brasileira, mesmo que a sede da empresa fornecedora seja fincada em terras estrangeiras. Este entendimento se dá em virtude da interpretação dada pelo Superior Tribunal de Justiça no sentido de que multinacionais com filial no Brasil e que promovam *marketing* direcionado aos consumidores brasileiros sujeitam-se às regras nacionais, ainda que contratem com brasileiros em terra estrangeira.

O entendimento do Superior Tribunal de Justiça impõe que, quando a relação de consumo é firmada com multinacional portadora de renome capaz de atrair os consumidores brasileiros, o contrato deverá submeter-se à legislação brasileira, e a filial da empresa no Brasil deverá responder pelos danos causados ao consumidor.

Essa orientação originou-se de caso envolvendo brasileiro que, em viagem aos Estados Unidos, adquirira máquina filmadora da marca Panasonic e que pleiteou a responsabilização da Panasonic do Brasil por conta do defeito que o produto apresentou. O Superior Tribunal de Justiça no REsp 63.981/SP afirmou decidiu que a economia globalizada não mais tem fronteiras rígidas e estimula e favorece a livre concorrência, imprescindível que as leis de proteção ao consumidor ganhem maior expressão em sua exegese, na busca do equilíbrio que deve reger as relações jurídicas, dimensionando-se, inclusive, o fator risco, inerente à competitividade do comércio e dos negócios mercantis, sobretudo quando em escala internacional, em que presentes empresas poderosas, multinacionais, com filiais em vários países, sem falar nas vendas hoje efetuadas pelo processo tecnológico da informática e no forte mercado consumidor que representa o nosso País.[39]

---

[39]DIREITO DO CONSUMIDOR. FILMADORA ADQUIRIDA NO EXTERIOR. DEFEITO DA MERCADORIA. RESPONSABILIDADE DA EMPRESA NACIONAL DA MESMA MARCA ("PANASONIC"). ECONOMIA GLOBALIZADA. PROPAGANDA. PROTEÇÃO AO CONSUMIDOR. PECULIARIDADES DA ESPÉCIE. SITUAÇÕES A

Em julgado um pouco mais recente, mas antes da sanção do Marco Civil da Internet, o Superior Tribunal de Justiça no REsp 1168547/RJ, em um caso de utilização indevida de imagem em sítio eletrônico de empresa de telefonia espanhola, manteve o entendimento exposto e aplicou a legislação brasileira, haja vista a existência de filial em território nacional, afirmando que a alegada atividade ilícita tiver sido praticada pela internet, independentemente de foro previsto no contrato de prestação de serviço, ainda que no exterior, é competente a autoridade judiciária brasileira caso acionada para dirimir o conflito, pois aqui tem domicílio a autora e é o local onde houve acesso ao sítio eletrônico onde a informação foi veiculada, interpretando-se como ato praticado no Brasil, aplicando-se à hipótese o disposto no artigo 88, III, do antigo CPC.

Desta maneira, sob o prisma ritualístico civilista, o processo deverá ser promovido contra a filial sediada no Brasil, que responderá por qualquer violação ao contrato na ótica da legislação brasileira, ou contra a matriz sediada no estrangeiro, o que acarretará o transtorno decorrente

---

PONDERAR NOS CASOS CONCRETOS. NULIDADE DO ACÓRDÃO ESTADUAL REJEITADA, PORQUE SUFICIENTEMENTE FUNDAMENTADO. RECURSO CONHECIDO E PROVIDO NO MÉRITO, POR MAIORIA.

I – Se a economia globalizada não mais tem fronteiras rígidas e estimula e favorece a livre concorrência, imprescindível que as leis de proteção ao consumidor ganhem maior expressão em sua exegese, na busca do equilíbrio que deve reger as relações jurídicas, dimensionando-se, inclusive, o fator risco, inerente à competitividade do comércio e dos negócios mercantis, sobretudo quando em escala internacional, em que presentes empresas poderosas, multinacionais, com filiais em vários países, sem falar nas vendas hoje efetuadas pelo processo tecnológico da informática e no forte mercado consumidor que representa o nosso País. II – O mercado consumidor, não há como negar, vê-se hoje "bombardeado" diuturnamente por intensa e hábil propaganda, a induzir a aquisição de produtos, notadamente os sofisticados de procedência estrangeira, levando em linha de conta diversos fatores, dentre os quais, e com relevo, a respeitabilidade da marca.

III – Se empresas nacionais se beneficiam de marcas mundialmente conhecidas, incumbe-lhes responder também pelas deficiências dos produtos que anunciam e comercializam, não sendo razoável destinar-se ao consumidor as consequências negativas dos negócios envolvendo objetos defeituosos.

IV – Impõe-se, no entanto, nos casos concretos, ponderar as situações existentes.

V – Rejeita-se a nulidade arguida quando sem lastro na lei ou nos autos. (STJ, REsp 63.981/SP, 4ª Turma, Rel. Ministro Aldir Passarinho Junior, Rel. p/ Acórdão Ministro Sálvio de Figueiredo Teixeira, DJ 20/11/2000)

do emprego das cartas rogatórias como via de comunicação processual, mas sempre aplicando a legislação nacional.

Após a análise sobre as situações de aplicação da lei estrangeira e brasileira acerca dos contratos firmados na rede mundial de computadores com provedores de aplicação de internet sediados em terras estrangeiras, antes da sanção do Marco Civil, faz-se imperioso o estudo sobre tal situação sob a ótica da novel lei.

Com o advento do Marco Civil da Internet, sobretudo à luz de seu artigo 11, a legislação brasileira terá de ser obrigatoriamente respeitada por qualquer empresa estrangeira que, mesmo não tendo filial no Brasil, oferte serviço ao público brasileiro, conforme se depreende da interpretação do parágrafo 2º do dispositivo mencionado:

> Art. 11. *In omissis*
>
> §2º O disposto no *caput* aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.

Apesar a clara exegese da norma, não se pode extrair conclusões rápidas e intuitvas, que poderiam levar a aplicação da lei brasileira a um absurdo jurídico. Em primeiro plano, é preciso apontar o alcance objetivo da legislação pátria, pois, em minha opinião, não é qualquer norma brasileira que atingirá os provedores de aplicação de Internet estrangeiros sem filial no Brasil, mas apenas as normas que tratam de coleta, guarda, armazenamento ou tratamento de registros, dados pessoais ou de comunicações, conforme o que se constata pela redação do *caput* do artigo 11 e do seu §3º:

> 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.
> ...

> §3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto **ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações**. (destaque do autor)

O interesse do legislador foi apenas de submeter as operações de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações à legislação nacional. Desta feita, é possível extrair a exegese de que o Marco Civil não cuidou de definir a legislação que disciplinará o contrato celebrado por um brasileiro que adquire um produto em um *site* estrangeiro, salvo no tocante à coleta, guarda, armazenamento ou tratamento de registros, dados pessoais ou de comunicações.

Então, para a tutela e proteção do consumidor brasileiro que adquire um produto de site estrangeiro sem filial no Brasil, seguem vigentes os elementos de conexão da lei estrangeira e nacional previstos na LINDB e na jurisprudência do Superior Tribunal de Justiça. Carlos Eduardo Elias de Oliveira (2014, p.12) conclui que:

> ... se o site estrangeiro pertence a uma multinacional com filial no Brasil e com marketing voltado ao mercado de consumo brasileiro, aplica-se o entendimento do STJ firmado no supracitado caso Panasonic, de modo que a legislação brasileira (como o CDC) disciplinará o contrato. Se, porém, o site não pertencer a uma empresa com esse perfil (ou seja, não houver filial no Brasil nem marketing direcionado ao mercado brasileiro), somente será aplicável a lei estrangeira para a disciplina do contrato, nos termos do art. 9º, § 2º, da LINDB. O CDC não poderá ser invocado aí.

O autor continua:

> ... o art. 11 do Marco Civil cuida de elemento de conexão específico e exclusivo para aplicação da legislação brasileira relativa à coleta, guarda, armazenamento ou tratamento de registros, dados pessoais ou de comunicações.

> Segundo esse dispositivo, qualquer empresa estrangeira que ofertar serviço ao público brasileiro, ainda que não tenha filial no Brasil, deve respeitar a legislação brasileira relativamente aos dados pessoais, aos registros de conexão e de acessos a aplicações e a comunicações dos internautas. Ela, por exemplo, terá de observar o Marco Civil da Internet, que proíbe a utilização comercial dos registros de acesso às aplicações se não houver consentimento expresso do internauta (art. 7º, VII). (Oliveira. 2014, p.13)

É importante frisar que o dispositivo normativo do artigo 11 visa frear violações de privacidade por meio de coleta, armazenamento e tratamento de registros, dados pessoais ou comunicações, aplicando-se o Marco Civil da Internet quando, pelo menos, um dos atos realizar-se no Brasil ou quando um dos terminais estiver no Brasil e que pessoas jurídicas com sede no exterior devem sujeitar-se à lei brasileira quando tiverem, pelo menos, uma integrante do mesmo grupo econômico com estabelecimento no Brasil ou oferte seus serviços ao público brasileiro.

No que concerne à oferta de serviços ao público brasileiro, há de compreender-se o comportamento da empresa estrangeira em, de forma direcionada e específica, promover *marketing* ao mercado de consumo brasileiro impõe-lhe a aplicação da lei nacional.

A expansão da publicidade por meio da internet e a ampliação do comércio eletrônico, embora o Código de Defesa do Consumidor estabeleça regras que alcançam tais condutas, merecem uma regulamentação específica, a fim de prevenir e reprimir condutas antiéticas e ilícitas praticadas no mercado de consumo. As responsabilidades do *marketing* numa empresa referem-se, pois, à promoção dos seus produtos e serviços, mas há também a responsabilidade jurídica, que incide diretamente no conteúdo de mensagens publicitárias.

Considerando a importância deste marketing voltado para o consumidor brasileiro frente a ausência de estabelecimento físico do provedor de aplicação de internet no país, o legislador impôs a aplicação da lei brasileira. Carlos Eduardo Oliveira (2014, p.13) exemplifica bem a situação:

> Se um brasileiro acessa um *site* de compras chinês que não promove marketing direcionado ao mercado brasileiro (embora disponibilize versão de

> sua página em idioma português), esse *site* chinês somente observará a legislação chinesa:
>
> a) seja no tocante às regras que disciplinam o contrato de compra e venda em si, de modo que não se aplicará o Código de Defesa do Consumidor brasileiro, por força do art. 9º, § 2º, da LINDB;
>
> b) seja no atinente às regras de coleta, guarda, armazenamento ou tratamento de registros, dados pessoais ou de comunicações, de maneira que não se aplicará a lei brasileira do Marco Civil da Internet para, por exemplo, impedir o uso comercial do histórico de navegação do usuário sem o consentimento, tendo em vista o elemento de conexão do art. 11 da Lei do Marco Civil da Internet.

Já quando houver oferta de serviços direcionado ao público brasileiro, haverá aplicação da lei nacional, conforme exemplificado pelo mesmo jurista:

> Todavia, se o brasileiro acessa um *site* de compras norte-americano que promove marketing direcionado ao mercado nacional, ainda que não haja filial no Brasil, aí haverá duas observações:
>
> a) não será aplicada a legislação brasileira quanto à disciplina do contrato de compra e venda, e sim a norte-americana, por força do art. 9º, § 2º, da LINDB, e do fato de a jurisprudência do STJ no famoso "caso Panasonic" ter envolvido uma empresa com filial no Brasil. Obviamente, a jurisprudência pode mudar e passar a dispensar a exigência de filial no Brasil e satisfazer-se com a oferta direcionada de produtos ao mercado de consumo brasileiro. Seja como for, a discussão girará em torno do art. 9º, § 2º, da LINDB.
>
> b) será aplicada a legislação brasileira quanto à coleta, guarda, armazenamento ou tratamento de registros, dados pessoais ou de comunicações, por força do art. 11 do Marco Civil da Internet. Dessa forma, o site de compras norteamericano não poderá, por exemplo, usar comercialmente o

> histórico de navegação do internauta brasileiro sem o seu consentimento expresso, em razão da incidência do disposto no art. 7º, VII, do Marco Civil da Internet brasileiro. (Oliveira. 2014, p.14)

A despeito da boa intenção, a violação pode não acontecer no Brasil, mas poderá acontecer na outra ponta da transmissão de dados no exterior. Mesmo com a previsão das sanções contidas no art.12 do Marco Civil da Internet, entre os quais, advertência, multa de 10% do faturamento do grupo econômico no Brasil em seu último exercício, suspensão temporária de atividades ou proibição de exercício de atividades. Entretanto, estas medidas punitivas poderão ser inócuas, uma vez que a legislação brasileira não possui um alcance jurisdicional para controlar as atividades dessas grandes empresas em suas sedes no exterior, sem filial no país.

Inobstante não haver menção legal direta sobre aos provedores de Computação em Nuvem, toda a discussão apontada é perfeitamente aplicável, uma vez que estes são entidades albergadas pelo Marco Civil da Internet, quando implementadas as condições do artigo 11.

Por fim, é possível afirmar que um cenário ideal da proteção e promoção da segurança da informação na Internet, sobretudo na Computação em Nuvem, exige a conformação pelos Estados de um normativo padrão aplicável internacionalmente. Talvez a adoção de um Tratado internacional a respeito do tema seja a forma coerente e lógica a tutelar a privacidade, o sigilo dos dados pessoais e a segurança da informação posta na *cloud computing*.

CONCLUSÃO

As transformações provocadas pela Internet se solidificam cotidianamente, com interferência em todos os campos sociais. O computador é um equipamento essencial para a própria sobrevivência do homem em sociedade, tendo a ciência jurídica o grande desafio de compreender as inovações tecnológicas, visando a garantia da pacificação social, o desenvolvimento sustentável e da manutenção do próprio Estado Democrático de Direito. A evolução da Internet foi escalonado por várias etapas, que perpassaram pelo uso institucionalizado de Estados soberanos até a interligação rápida de informação entre computadores em âmbito comercial e civil, mitigando as fronteiras físicas entre as pessoas.

Estes avanços tecnológicos proporcionaram a existência de serviços básicos e essenciais de utilidade pública de forma transparente, os quais se tornaram fundamentais para vida diária do homem moderno. Esta ideia de utilidade e essencialidade é aplicada no contexto da informática, através da Computação em Nuvem, que alcança índices globais, ao proporcionar serviços, que atingem o usuário final, por meio de recursos tecnológicos fornecidos para o acesso de sistema computacional guardado ou armazenado em outro lugar, sem a necessidade de conhecimento sobre a tecnologia utilizada. Para a utilização dos serviços, os usuários necessitam minimamente possuir em seus dispositivos um sistema operacional e acesso à Internet.

Através da Computação em Nuvem, ao consumidor é ofertada a aquisição de um produto mais barato, porque necessita de um menor número de componentes estruturais para execução da tarefa almejada.

As tecnologias desenvolvidas no Sistema de Computação em Nuvem foram criadas totalmente inseridas no contexto de personalização, sendo voltadas à atender de forma flexível e única a maior gama possível de necessidades de seus usuários.

No Brasil, a Lei 12.965/2014, conhecida como Marco Civil e Regulatório da Internet, pretende ser o aparato legal a proteger a pessoa interconectada aos meios digitais. Esta lei é atrelada aos grandes ramos do Direito, quando se trata da proteção dos direitos dos usuários, visando a responsabilidade civil dos atores envolvidos. Aliado à norma informacional, existem outras leis que servem para dirimir as controvérsias civis entre particulares, 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).

O Marco Civil da Internet no Brasil trouxe meios de desestímulo e obstaculização à apropriação indevida de informação pessoal, bem como

garante minimamente a preservação da privacidade do usuário, bem como tutela a segurança dos dados guardados ou armazenados em nuvem.

A segurança e a privacidade são quesitos importantes para a adoção dos ambientes de Computação em Nuvem e a possível existência potencial de falhas de segurança e de violação da privacidade deixam os consumidores desconfiados para adotar plenamente o sistema. Os consumidores esperam que os sistemas de Computação em Nuvem sejam confiáveis e que a disponibilidade dos serviços e recursos oferecidos atenda integralmente às suas necessidades.

A produção, o sigilo e o armazenamento da informação sofrem o fenômeno do superdimensionamento do valor mercantil da informação, causado, essencialmente, pelo atual estágio tecnológico em que se encontra a sociedade, pois a dinâmica da produção capitalista da era digital trata a informação como um produto diferenciado no mercado. A segurança da informação se refere à proteção sobre as informações de uma determinada empresa ou indivíduo. Aplica-se tanto às informações corporativas quanto às pessoais.

A segurança da informação está diretamente relacionada com proteção de um conjunto de informações, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. São propriedades básicas da segurança da informação: confidencialidade, integridade, disponibilidade e autenticidade. Não está restrita somente a sistemas computacionais, informações eletrônicas ou sistemas de armazenamento. A segurança de sistemas computacionais envolve temas como políticas de segurança, que se desenrolam na definição de regras para proteção do nível físico; contenção, recuperação de desastres, backup, preservação e destruição de mídias; operação envolvendo treinamento do usuário e registro de todas as ações de suporte; uso de criptografia e ciclos de vida de chaves; controle de acesso a sistemas e a recursos; não violação a leis e a ética etc.

Os controles de segurança na Computação em Nuvem são, em sua maioria, iguais aos controles de qualquer ambiente de tecnologia da informação, mas existe uma variação de acordo com os modelos de serviço, modo de operação e tecnologias utilizadas para prover os serviços na nuvem.

A segurança e a privacidade são os principais desafios que podem impedir a ampla adoção da abordagem de computação em nuvem, pois, falhas de segurança em qualquer um dos componentes podem impactar os demais componentes de segurança e consequentemente a segurança de todo o sistema poderá entrar em colapso. Os riscos e ameaças à privacidade diferem de acordo com o uso da Computação em Nuvem,

como, por exemplo: o usuário de serviços em nuvem poderia ser forçado ou persuadido a aceitar o monitoramento das suas atividades ou a fornecer informações pessoais contra sua a vontade; o usuário poderia ver suas informações armazenadas na nuvem perdidas ou divulgadas indevidamente.

Inobstante, a implantação de todo um sistema de segurança proporcionado pelo servidor ao oferecer o serviço de armazenamento em nuvem computacional, não pode o usuário ser submetido a este produto sem garantias mínimas, seja legal ou contratual. Por outro lado, deve haver por parte do usuário, um grau de maturidade e preparo no que tange ao correto e consciente uso da mencionada tecnologia. Os consumidores que utilizam Computação em Nuvem precisam estar cautelosos em relação à privacidade, uma vez que todo sistema é passível de *hack*.

A responsabilização jurídica na Informática Jurídica brasileira pode ser oriunda tanto de relação jurídica contratual, que se delineia pela relação provedor-consumidor; como extracontratual, porém o provedor não poderá ser punido por dano decorrente de conteúdo gerado por terceiro, salvo se não tiver tomado providências para retirar o conteúdo ofensivo da rede, nos termos da Seção III do Capítulo III da Lei 12.965/2014.

Antes da edição da Constituição da Internet, o Superior Tribunal Justiça consolidou o entendimento de que a responsabilidade do provedor surgiria a partir do momento em que se omitisse perante notificação extrajudicial por parte daquele que se sentiu ofendido. No âmbito da responsabilização contratual, o Marco Civil estipula que os provedores responsáveis pela guarda de registros de conexão, de acesso a aplicações de Internet, de dados pessoais e do conteúdo de comunicações privadas deverão proteger os dados de seus usuários.

A responsabilidade jurídica dos provedores de *cloud computing* reside no fato de que, alheio à necessidade de tomar todos os cuidados com relação à contratação do serviço, permita que uma situação de vulnerabilidade chegue a um patamar insustentável causando dano ao direito de personalidade do usuário, que clamará intervenção estatal pelo Judiciário para tentar restabelecer o equilíbrio contratual.

Assim, na ocorrência de ilícito civil contratual ou não, referente à falha na prestação de serviços de nuvem computacional, em que possa resultar danos morais e materiais aos usuários/consumidores, o instituto da responsabilidade civil deve ser utilizado.

Num cenário anterior à promulgação do Marco Civil da Internet, quando um usuário domiciliado no Brasil acessa um provedor de aplicações de Internet, em que guarda e armazena dados importantes,

estaria celebrando um contrato regido pela legislação estrangeira, conforme aregra do artigo 9º, §2º da Lei de Introdução às Normas do Direito Brasileiro. De acordo com a LINDB, o usuário não poderá invocar, de modo algum, a legislação brasileira, como, por exemplo, o Código de Defesa do Consumidor, uma vez que este contrato eletrônico se equivaleria ao que seria celebrado pessoalmente em território estrangeiro – *locus regit actum*. Nos termos do artigo 9º da LINDB, aplica-se a lei do local da celebração do contrato e o cumprimento de suas formalidade. Asstim, se tiver de ser a obrigação cumprida no Brasil, entretanto, e depender de forma essencial na nossa lei, esta deverá ser observada, além das normas estrangeiras.

No que tange à contração de provedores de aplicação de Computação em Nuvem com filial no Brasil, o contrato será regido pela legislação brasileira, mesmo que a sede da empresa fornecedora seja fincada em terras estrangeiras. Este entendimento se dá em virtude da interpretação dada pelo Superior Tribunal de Justiça no sentido de que multinacionais com filial no Brasil e que promovam *marketing* direcionado aos consumidores brasileiros sujeitam-se às regras nacionais, ainda que contratem com brasileiros em terra estrangeira.

O entendimento do Superior Tribunal de Justiça impõe que, quando a relação de consumo é firmada com multinacional portadora de renome capaz de atrair os consumidores brasileiros, o contrato deverá submeter-se à legislação brasileira, e a filial da empresa no Brasil deverá responder pelos danos causados ao consumidor.

Apesar da clara possibilidade de responsabilizar civilmente o provedor de aplicação de Computação em Nuvem, uma celeuma recai sobre a aplicação da legislação brasileira em face de entidades que não estão em solo nacional ou da possibilidade de utilização da legislação estrangeira para o consumidor brasileiro.

Foram apresentados dois cenários jurídicos: um anterior à edição do Marco Civil da Internet e outro posterior. Em cenário anterior à promulgação da lei informacional, quando um usuário domiciliado no Brasil acessa um provedor de aplicações de Internet, que não tenha filial no país, em que guarda e armazena dados importantes, estaria celebrando um contrato regido pela legislação estrangeira, conforme aregra do artigo 9º, §2º da Lei de Introdução às Normas do Direito Brasileiro. Já, quando houvera a contração de provedores de aplicação de Computação em Nuvem com empresa com filial no Brasil, o contrato será regido pela legislação brasileira, mesmo que a sede da empresa fornecedora seja fincada em terras estrangeiras.

Por outro lado, o advento do Marco Civil da Internet, sobretudo à luz de seu artigo 11, faz com que a legislação brasileira tenha de ser obrigatoriamente respeitada por qualquer empresa estrangeira que, mesmo não tendo filial no Brasil, oferte serviço de guarda, armazenamento ou tratamento de registros, dados pessoais ou de comunicações ao público brasileiro, conforme se depreende da interpretação do parágrafo 2º do dispositivo mencionado. O legislador visou submeter as operações de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações à legislação nacional. No que concerne à oferta de serviços ao público brasileiro, há de compreender-se o comportamento da empresa estrangeira em, de forma direcionada e específica, promover *marketing* ao mercado de consumo brasileiro impõe-lhe a aplicação da lei nacional.

Por outro lado, é possível concluir que o Marco Civil não definiu a legislação que disciplinará o contrato celebrado por um brasileiro que adquiriu um produto em um *site* estrangeiro. Logo, para a tutela e proteção do consumidor brasileiro que adquire um produto de site estrangeiro sem filial no Brasil, seguem vigentes os elementos de conexão da lei estrangeira e nacional previstos na LINDB e na jurisprudência do Superior Tribunal de Justiça.

É importante frisar que o dispositivo normativo do artigo 11 do Marco Civil da Internet visa frear violações de privacidade por meio de coleta, armazenamento e tratamento de registros, dados pessoais ou comunicações, aplicando-se-lhe quando, pelo menos, um dos atos realizar-se no Brasil ou quando um dos terminais estiver no Brasil.

REFERÊNCIAS

ALBAGLI, Sarita. **Novos espaços de regulação na era da informação e conhecimento**. *In* LASTRES, Helena M.M (org.). **Informação e globalização na era do conhecimento**. Rio de Janeiro: Campus, 1999.

ALEXY, Robert. **Teoria dos Direitos Fundamentais**. São Paulo: Malheiros, 2015. Tradução de Virgílio Afonso da Silva.

ALMEIDA, Marco Antônio de; GANZERT, Christian Carvalho. **Informação e Mudanças Sociais no Capitalismo Informacional**. Revista de Ciência Política, No. 40, 2008. Disponível em <http://www.achegas.net/numero/40/ganzert_40.pdf>

AMARAL, Antônio Carlos Rodrigues do. (coordenador). **Direito do Comércio Internacional. Aspectos Fundamentais.** 2ª ed. São Paulo: Lex Editora, 2006.

ANDERSON, Chris. **Free: grátis: o futuro dos preços**. Rio de Janeiro: Elsevier, 2009

ARMBRUST, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinski, A., Lee, G., Patterson, D. A., Rabkin, A., Stoica, I., and Zaharia, M. (2009). **Above the clouds: A berkeley view of cloud computing.** Technical report, EECS Department, University of California, Berkeley.

ASCENSÃO, José de Oliveira. **Sociedade da informação e mundo globalizado**. *In*: WACHOWICZ, Marcos (Org.). **Propriedade Intelectual & Internet**. 1ª ed. Curitiba: Juruá, 2006.

Alves Jr., Nilton. 2000,. **Modelos de qualidade de serviço - aplicações em IP.** <http://mesonpi.cat.cbpf.br/redes/qos.pdf>. Acessado em 20 de setembro de 2017.

BAUMAN, Zygmunt. **44 cartas do Mundo Líquido Moderno.** Rio de Janeiro, Zahar, 2011.

_____. **Vida para consumo: a transformação das pessoas em mercadorias**. Rio de Janeiro: Jorge Zahar, ed. 2008.

BBC NEWS TECHNOLOGY. **Facebook users average 3.74 degrees of separation**. Disponível em: <http://www.bbc.co.uk/news/technology-15844230>. Acesso em 21 jan. de 2014.

BECK, Ulrich. **La Sociedad del Riesgo Global**. Madrid: Siglo Ventiuno, 1999.

BEHRENS, Fabiele. **Assinatura Eletrônica & Negócios Jurídicos**. Curitiba: Juruá, 2007.

BRASIL. **Constituição da República Federativa do Brasil**. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao>

BOIAGO JUNIOR, José Wilson. **Contratação Eletrônica: aspectos jurídicos**. 2ª. ed., Curitiba:Juruá, 2006.

BRUNETTE, Glenn; MOGULL, Rich. **Guia de Segurança para Áreas Críticas Focado em Computação em Nuvem v2.1.** Traduzido por Cloud Security Alliance – Brazilian Chapter, Junho 2010. Disponível em: https://chapters.cloudsecurityalliance.org/brazil/files/2011/07/csaguide-ptbr2.1.pdf

CÂMARA DOS DEPUTADOS. Projeto de Lei 5.344/2013. Dispõe sobre diretrizes gerais e normas para a promoção, desenvolvimento e exploração da atividade de computação em nuvem no País. Disponível em:<http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra;jsessionid=844786B2A3104162335C1E52C491AE20.node1?codteor=1074235&filename=PL+5344/2013>

CAPRA, Fritoj. **As conexões ocultas**. São Paulo: Cultrix, 2006.

CASTELLS, Manuel. **A Sociedade em Rede. A Era da Informação: economia, sociedade e cultura.** v.1. São Paulo: Paz e Terra, 1999.

_____, **A Sociedade em Rede. A Era da Informação: economia, sociedade e cultura**. v. 3. São Paulo: Paz e terra, 1999.

CAVALIERI FILHO. Sérgio. **Programa de Sociologia Jurídica**. 11ª ed. Rio de Janeiro: Forense, 2007.

_____, **Programa de Responsabilidade Civil**, 8ª ed., 2008, Rio de Janeiro, Ed. Atlas.

COHEN, Reuven. **Is Cloud Computing Really Cheaper?** Revista Forbes *online*. Disponível em: <http://www.forbes.com/sites/reuvencohen/2012/08/03/is-cloud-computing-really-cheaper/2/>.

COUTINHO. Emanuel F. SOUZA, Flávio R. C. GOMES, Danielo G. Souza, José N. de. **Elasticidade em Computação na Nuvem: Uma Abordagem Sistemática.** 31o Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos – SBRC 2013. p. 216. Disponível em: < http://sbrc2013.unb.br/files/anais/minicursos/minicurso- 5.pdf>.

CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: Saraiva, 2011.

EMERSON, Ralph Waldo. **Public Quotes**. Disponível em: <http://publicquotes.com/quote/4275/the-human-body-is-the-magazine-of inventions-the-patent-office-where-are-the-models-from-which-every.html>.

ENDLER, Markus. VITERBO, José. FONSECA, Hubert. **Perspectivas e desafios da computação em nuvem na Internet do futuro.**

Departamento de Informática da PUC/RJ. 2011. Disponível em: < http://www.lac.inf.puc-rio.br/sites/default/files/CPqD- rel3.pdf>.

ESPINDOLA, Rodolfo. GALLIZA FILHO, Sergio. **Aldeia Global**. Disponível em: <http://srv.emc.ufsc.br/nepet/tecdev/20121/seminarios/aldeia.pdf>.

FACEBOOK. Disponível em: <http://newsroom.fb.com/content/default.aspx?NewsAreaId=22#Statistics>.

_____. **Politica de Uso de Dados**. Disponível em: <https://pt- br.facebook.com/about/privacy/your-info>. Acesso em 21 jan. de 2014.

FALCÃO, Armando. **Novo Código Civil. Exposição de Motivos e Texto Sancionado.** 2ª ed. Brasília: Senado Federal, 2005. Disponível em: <http://www2.senado.gov.br/bdsf/bitstream/handle/id/70319/743415.pdf?sequence=2>.

FONSECA Filho, Cléuzio. **História da computação** [recurso eletrônico]: O Caminho do Pensamento e da Tecnologia / Cléuzio Fonseca Filho. – Porto Alegre: EDIPUCRS, 2007. 205 p.

FRANKE, Hans Alberto. **Uma abordagem de acordo de nível de serviço para computação em nuvem**.[dissertação]. Programa de pós-graduação em ciência da computação. Florianópolis: UFSC, 2010.

FREIRE, Paulo. **Pedagogia da autonomia.** Rio de Janeiro: Paz e Terra, 1999.

FREITAS, Cinthia Obladen de Almendra. **Redes Sociais: sociedade tecnológica e inclusão digital**. In: WACHOWICZ, Marcos (Org.). **Direito da Sociedade da Informação e Propriedade Intelectual**. Curitiba:Juruá, 2012.

FREITAS, Cinthia Obladen de Almendra; EFING, Antônio Carlos. **Sociedade de Informação: o direito à inclusão digital**. Revista de Direito Empresarial, No. 12. jul/dez 2009.

FROST & SULLIVAN, **Análise Competitiva do Mercado Brasileiro de Datacenters**, dezembro de 2012. Desenvolvido para MCTI, Ministério de Ciência Tecnologia e Inovação e Brasscom, Associação Brasileira de Empresas de Tecnologia da Informação e Comunicação.

GALLINDO, Sergio Paulo Gomes. **Marco Civil da Internet e serviços na nuvem: hermenêutica jurídica e tributação como indutores de inovação tecnológica** / Sergio Paulo Gomes Gallindo. Gallindo, Sergio Paulo Gomes. Dissertação (Mestrado em Direito Político e Econômico). Universidade Presbiteriana Mackenzie, São Paulo, 2017.Gallindo. – 2017.

GARCIA, Gabriel. **Brasil é apenas 73º em velocidade de conexão à internet**. Revista Info. 23 de julho de 2013. Disponível em: <http://info.abril.com.br/noticias/internet/2013/07/brasil-e-apenas-73-em-velocidade- de-conexao-da-internet.shtml.> Acesso em 21 jan. de 2014.

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

GOOGLE. **Termos de Privacidade**. Disponível em: <https://www.google.com.br/intl/pt-BR/policies/privacy/>. Acesso em 21 jan. de 2014.

GOMES, Rafael de Aquino; COSTA, Fabio Moreira; NISHI, Luciana. **Escalabilidade Dinâmica em Nuvens Construídas a partir de Recursos Computacionais Compartilhados**. Disponível em: < http://sbrc2013.unb.br/files/anais/wcga/artigos/artigo-13.pdf.>

GONÇALVES, Everton das Neves. STELZER, Joana. **Estado, Globalização E Soberania: Fundamentos Político-Jurídicos Do Fenômeno Da Transnacionalidade**. Anais do XVIII Congresso Nacional do CONPEDI, realizado em São Paulo – SP nos dias 04, 05, 06 e 07 de novembro de 2009. Disponível em <http://www.publicadireito.com.br/conpedi/manaus/arquivos/anais/sao_paulo/1915.pdf>.

GREENBERG, Albert. JAMES, Hamilton. MALTZ, David A. PATEL, Parveen. **The Cost of a Cloud: Research Problems in Data Center Networks**. ACM SIGCOMM Computer Communication Review archive. Volume 39, Issue 1, January 2009.

GUILLOTEAUS, Stéphane et al. **Privacy in Cloud Computing**. ITU Technology Watch Report. March 2012. Disponível em: <http://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000160001PDFE.pdf>. Acesso em 21 jan. de 2014.

GUIZZO, Erico Marui. **O microchip: pequena invenção, grande revolução**. Disponível em <http://www.lsi.usp.br/~chip/de_onde_vieram.html>. Acesso em 21 jan. de 2014.

HOLLOWAY, John. **Mudar o Mundo sem tomar o poder**. São Paulo: Editora Viramundo. 2003.

JANDL JUNIOR, Peter. **Computação, Ubiquidade e Transparência**. Revista Ubiquidade – Estudos Sobre as Tecnologias da Informação e Comunicação. Número 01, Volume 1, Jundiaí, 2011.

JAVA. Disponível em: < http://www.java.com/pt_BR/download/whatis_java.jsp>.

JORNAL O ESTADO DE SÃO PAULO. **Brasil é o campeão do lixo eletrônico entre emergentes**. Disponível em:

<http://www.estadao.com.br/noticias/vidae,brasil-e-o- campeao-do-lixo-eletronico-entre emergentes,514495,0.htm>. Acesso em 21 jan. de 2014.
KEEN, Andrew. **O culto do Amador: como blogs, Myspace, Youtube e a pirataria digital estão destruindo nossa economia, cultura e valores**. Rio de Janeiro, Jorge Zahar, 2009.
LEHMAN, M. M.; RAMIL, J.F; WERNICK P.D. **Metrics and Laws of Software Evolution - The Nineties View**. Fourth International Symposium on Software Metrics, Metrics 97, Albuquerque, New Mexico, 1997. p.2. Disponível em: <http://users.ece.utexas.edu/~perry/work/papers/feast1.pdf>. Acesso em: 21 jan. de 2014.
LIPOVETSKY, Gilles. **Os Tempos Hipermodernos**. São Paulo: Editora Barcarolla, 2004.
MALAQUIAS, Bruno Pires. **O analfabetismo digital**. Disponível em: <http://www.ibdi.org.br/site/artigos.php?id=159>
MARCON JR, Arlindo; LAUREANO, Marcos; SANTIN, Altair Olivo; MAZIERO, Carlos Alberto. **Aspectos de Segurança e Privacidade em Ambientes de Computação em Nuvem**. Anais de Minicursos do SBSeg 2010 - X Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais. Porto ALEGRE, RS: SBC, 2010. p.55. Disponível em: <http://dainf.ct.utfpr.edu.br/~maziero/lib/exe/fetch.php/research:2010-sbseg-mc.pdf>.
MARQUES, Cláudia Lima. **Contratos no Código de Defesa do Consumidor**. 4ª edição. São Paulo: RT. 2002.
MARQUES, Francisco Paulo Jamil Almeida. **Dimensões da Ciberdemocracia**. 2004,
MELL, Peter. GRANCE, Timothy. **The NIST Definition of Cloud Computing**. Gaithersburg, 2011. Disponível em: <http://www.nist.gov/itl/cloud/>. Acesso em: 21 jan. de 2014.
MEZGÁR, István. **Building Trust in Virtual Communities**. *In*: KISIELNICKI, Jerzy (Org.). **Virtual Technologies. Concepts, Methodologies, Tools and Applications**. Vol. 1. New York: Information Science Reference, 2008.
MILLER, Claire Cain. **F.T.C. Said to Be Near Facebook Privacy Deal**. The New York Times. November, 10,2011. Disponível em: <http://www.nytimes.com/2011/11/11/technology/facebook-is-said-to-be-near-ftc- settlement-on-privacy.html?_r=0>. Acesso em 21 jan. de 2014.
MITCHELL, William C; SIMMONS, Randy T. **Para além da política: mercados, bem-estar social e o fracasso da burocracia**. Rio de Janeiro: Topbooks, 2003.

MOREIRA, Daniela. **Lixo eletrônico tem substâncias perigosas para a saúde humana**. Disponível em: <http://idgnow.uol.com.br/ti-pessoal/2007/04/26/idgnoticia.2007-04-25.3237126805/#&panel1-1>.
MORIN, Edgar. **Para Sair do Século XX**. Rio de Janeiro, Nova Fronteira: 1986.
MULLER, Friedrich. **Democracia e Exclusão Social em Face da Globalização**. Revista Jurídica da Presidência da República. Brasília, vol. 7, n. 72, maio 2005. Disponível em: <http://www.planalto.gov.br/ccivil_03/revista/Rev_72>.
NIELSEN, Katie. **Confused About the Cloud? Deciphering Cloud Services for Consumers**. Disponível em: <http://cloud-services-review.toptenreviews.com/confused-about-the-cloud-deciphering-cloud-services-for- consumers.html>. Acesso em 21 jan. de 2014.
NOGUEIRA, Sandro D'Amato. **Crimes de informática**. Leme: BH Editora e Distribuidora, 2ª. Ed. 2009.
PARCHEN, Charles Emmanuel; FREITAS, Cinthia. O. A. **O Uso da computação em nuvem como possibilidade de redução do uso de matérias primas não Renováveis na fabricação de dispositivos tecnológicos**. Trabalho apresentado no III Simpósio Jurídico dos Campos Gerais, 2012, Ponta Grossa - PR. Anais do III Simpósio Jurídico dos Campos Gerais. Ponta Grossa - PR: UEPG, 2012. v. 1.
PARISER, Eli. **O filtro invisível: o que a internet está escondendo de você**. Rio de Janeiro: Zahar, 2012.
PECK, Patrícia. **Direito Digital**. São Paulo: Saraiva, 2002.
PEREIRA FILHO, José Gonçalves. **Endereçamento IP**. Disponível em: <http://www.inf.ufes.br/~zegonc/material/Redes%20de%20Computadores%202013- 2/Enderecamento%20IP.pdf >.
PINHEIRO, José Maurício Santos. **Sociedade e Tecnologia, um Par Inseparável**. Disponível em: <http://www.projetoderedes.com.br/artigos/artigo_sociedade_e_tecnologia.php>.
PRENSKY, Marc. **Digital Natives, Digital immigrants**. From On The Horizon. MCB University Press. Vol 9. Nº. 5. October 2001.
REALE, Miguel. **Novo Código Civil. Exposição de Motivos e Texto Sancionado**. 2ª ed. Brasília: Senado Federal, 2005. Disponível em:<http://www2.senado.gov.br/bdsf/bitstream/handle/id/70319/743415.pdf?sequence=2>.
REIS, Maria Helena Junqueira. **Computer Crimes**. Belo Horizonte: Del Rey, 1996.
RIBEIRO, Marcia Carla Pereira, *et al*. **Acesso à informação e desenvolvimento socioeconômico**. *In*: WACHOWICZ, Marcos (Coord).

Direito da sociedade da informação & propriedade intelectual. Curitiba: Juruá, 2012.
RIFKIN, Jeremy. **A Era do Acesso**. São Paulo: Makron Books, 2001.
RIVERA, José Antônio. **Los Pueblos Indígenas Originarios En El Nuevo Sistema Constitucional Boliviano**. Bolivia: Fundacion Konrad Adenauer. 2012.
ROSS, Anderson. et al. **Measuring the Cost of Cybercrime.** UK Ministry of Defence. 2012. Disponível em: <http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf>.
ROVER, Aires José; RAMOS JÚNIOR, Hélio Santiago. DEMOCRACIA ELETRÔNICA NA SOCIEDADE DA INFORMAÇÃO. Disponível em: <www.egov.ufsc.br/portal/.../democracia_eletronica_na_sociedade_da_informacao.pdf.>
RUSHKOFF, Douglas**. As 10 Questões Essenciais da Era Digital. Programe Seu Futuro Para Não Ser Programado por Ele**. São Paulo: Saraiva, 2012.
SIMET. Disponível em: <http://simet.nic.br/mapas/>.
SOUZA, Flávio R.C; MOREIRA, Leonardo O; MACHADO, Javam C. **Computação em Nuvem: Conceitos, Tecnologias, Aplicações e Desafios**. 2010. Publicado no ERCEMAPI 2009. Todos os direitos reservados a EDUFPI. p.3. Disponível em: <http://www.es.ufc.br/~flavio/papers/ercemapi2009.pdf>. Acesso em 21 jan. de 2014.
SOUZA, Flávio R.C; MOREIRA, Leonardo O; MACEDO, José Antônio F. de; MACHADO, Javam C. **Gerenciamento de Dados em Nuvem: Conceitos, Sistemas e Desafios**. Publicado no SWIB 2010. Todos os direitos reservados a Sociedade Brasileira de Computação. Disponível em: < http://www.es.ufc.br/~flavio/papers/sbbd2010.pdf>. Acesso em 21 jan. de 2014.
SOUZA FILHO, Carlos Frederico Marés de**. Os direitos invisíveis**. In: OLIVEIRA, Francisco de; PAOLI, Maria Célia. **Os Sentidos da Democracia. Políticas do dissenso e hegemonia global**. 2ª ed. Brasília: NEDIC, 1999.
SYMANTEC. **Glossário de Segurança**. Disponível em: <http://www.symantec.com/pt/br/theme.jsp?themeid=glossario-de-seguranca>.
_____ **Symantec Internet Security Threat Report**. Symantec 2011 Trends. Volume 17, published april 2012. Disponível em: <http://www.symantec.com/content/en/us/enterprise/other_resources/bis

tr_main_report
_2011_21239364.en-us.pdf>.
SWISSINF.CH. **International Service of the Swiss Broadcasting Corporation**. Disponível em: <http://www.swissinfo.ch/por/ciencia_tecnologia/Cern_comemora_os_20_anos_da_we b.html?cid=891624>
TAPSCOTT, Don. **Geração Digital. A crescente e irreversível ascensão da geração Net**. São Paulo: Makron Books, 2009.
_____. **Plano de ação para uma economia digital. Prosperando na nova era do e-business**. São Paulo: Makron Books, 2000.
TAURION, Cezar. **Cloud Computing: computação em nuvem: transformando o mundo da tecnologia da informação**. Rio de Janeiro: Brasport, 2009.
THALER, Richard H; SUSTEIN, Cass R. **Nudge: o empurrão para a escolha certa**. Elsevier Editora. Rio de Janeiro, 2009.
VIEIRA, André Luiz; et al. **Computação em Nuvem**. Trabalho apresentado no MBA em TV digital, radiodifusão e novas mídias de comunicação eletrônica da Universidade Federal Fluminense. Rio de Janeiro. 2009.
VISSIÈRE, Laurent. **Altamente Confidencial**. Revista História Viva. Disponível em:<http://www2.uol.com.br/historiaviva/reportagens/altamente_confidencial.htm>. Acesso em 21 jan. de 2014.
WOLKMER, Antônio Carlos. **História do Direito no Brasil**. Rio de Janeiro: Forense, 2002.
_____. **Pluralismo Jurídico y Constitucionalismo Brasileño**. Disponível em: <http://www.ibcperu.org/doc/isis/12598.pdf>.
YACCOUB, Hilaine. **A chamada "nova classe média"**: **cultura material, inclusão e distinção social**. Horizontes Antropológicos, vol.17, n.36, Porto Alegre, 2011.