PROCESSO JUDICIAL ELETRÔNICO E SEGURANÇA DE DADOS: A PROTEÇÃO DIGITAL COMO NOVO DIREITO HUMANO

ELECTRONIC JUDICIAL PROCESS AND DATA SECURITY: DIGITAL PROTECTION AS A NEW HUMAN HIGHT

Patricia Martinez Almeida
profa.civil@gmail.com

Vladmir Oliveira da Silveira
vladmir@aus.com.br

Recebido em: 16/08/2013
Aprovado em: 10/09/2013

SUMARIO: Introdução 1. Evolução da Sociedade da Informação 2. Segurança Digital como (novo) Direito Humano 3. A Dicotomia entre Direito de Informação e a Proteção de Dados Pessoais: Implantação do Processo Judicial Eletrônico e a Segurança Digital. Conclusão. Referências

RESUMO
O presente estudo sobre processo judicial eletrônico e a segurança de dados tem por finalidade analisar a segurança digital como novo direito humano, delimitando a pesquisa no aspecto da segurança processual e jurídica, dos cidadãos da aldeia digital, no processo judicial eletrônico. Para tanto serão utilizados os métodos hipotético-dedutivo, monográfico, tipológico e histórico, com base em pesquisa teórica bibliográfica e da legislação. Como hipótese inicial adotará como premissa que a proteção de dados no ciberespaço e o exercício da cidadania virtual é projeção da digna condição do homem e conclui que o deslocamento da sociedade real para a virtual não autoriza

ABSTRACT
The present study on electronic judicial proceedings and data security aims to analyze the digital security as a new human right, delimiting the research in an legal and procedural aspect of the security of the citizens of the digital village, in the judicial process electronic. For both methods are used hypothetical-deductive, monographic, typological and historical based on theoretical research literature and legislation. As initial hypothesis adopt the assumption that the protection of data in cyberspace and virtual citizenship projection is worthy of man's condition and concluded that the displacement of the Royal Society for the virtual does not authorize the state to abandonment of full protection to citizens , and even in the invasion of the rights and guarantees to digital security and

o abandono estatal da proteção integral aos cidadãos e, tampouco, a invasão aos direitos e garantias à segurança digital e aos Direitos Humanos já consagrados em nosso ordenamento e tutelados na ordem interna e internacional, visando a proteção integral do ser humano.

PALAVRAS CHAVE
Direitos Humanos; segurança digital; acesso à justiça; processo judicial eletrônico.

Human Rights already enshrined and protected in our internal and international law aiming the protection of the human being.

KEYWORDS
Human Rights; digital security, access to justice, judicial process electronic.

INTRODUÇÃO

O surgimento de novas tecnologias e o compartilhamento de informação pelo ciberespaço acarretou mudanças significativas na sociedade e no comportamento social. A partir da expansão das ferramentas da internet, com maiores possibilidades e realidades na rede mundial de computadores, surge a necessidade da tutela das relações jurídicas havidas na chamada sociedade da informação ou ciberespaço.

O presente estudo busca analisar a evolução da sociedade da informação e os novos aspectos do direito no ciberespaço. Notadamente, o direito aparece da necessidade da sociedade. Nesse sentido, os anseios da geração conhecida como Y, os novos comportamentos sociais e comerciais na dita sociedade da informação, que emanaram com a evolução da rede mundial de computadores necessitou e continua necessitando de disciplina e proteção.

Nesta perspectiva, o Direito, além de disciplinar e tutelar essa nova realidade, precisou se adequar a tendência tecnologia em prol da efetiva e eficiente prestação da jurisdição por intermédio da informatização do processo judicial.

Neste contexto, com a evolução do princípio do acesso à justiça e a necessidade de dar efetividade ao princípio constitucional da duração razoável do processo, com fulcro no art. 5º, LVIII da CF e salvaguardar a celeridade processual, com o advento da Lei 11.419/2006 inaugurou-se uma nova fase processual, qual seja, a do processo judicial telemático.

No primeiro item será estudada a evolução da sociedade da informação e a necessidade de tutela dos direitos e deveres havidos no novo espaço: o ciberespaço, criado com a utilização da *internet* como meio de comunicação interplanetário.

O surgimento da chamada cibercultura e seus princípios e a implementação da cibercidadania, também serão observados.

No segundo item será analisada a disciplina da segurança digital na proteção dos dados pessoais e comerciais veiculados no ciberespaço e a problemática da ausência de força normativa especifica e regramento à nova realidade do espaço virtual, consubstanciando em desterritorialização estatal.

No terceiro item será verificada a dicotomia entre o direito à informação e a proteção digital na implantação do processo judicial eletrônico, esta como inovação necessária na busca da efetivação do princípio da duração razoável do processo, enquanto garantia do acesso à justiça.

Com a finalidade de analisar em que medida a instrumentalização digital do processo judicial efetivamente contribui para o acesso à justiça e para a segurança digital aos jurisdicionados, este trabalho pautar-se-á pelo método de abordagem hipotético-dedutivo, e métodos de procedimento monográfico, tipológico e histórico, uma vez que será estudada a evolução da sociedade virtual, enquanto fenômeno social complexo, para tanto se valerá de pesquisa teórica bibliográfica e da legislação interna e alienígena na consecução da presente pesquisa.

Como hipótese inicial será adotada como premissa que a proteção de dados no ciberespaço e o exercício da cidadania virtual se consubstanciam em projeção da digna condição do homem e que o deslocamento da sociedade real para a virtual não autoriza o abandono da proteção integral aos cidadãos e, tampouco, a invasão aos direitos e garantias à segurança digital e os Direitos Humanos já consagrados em nosso ordenamento e tutelados na ordem interna e internacional, visando o desenvolvimento integral do ser humano.

1. Evolução da sociedade da informação

Segundo Albert Einstein, em entrevista nos anos 50, três grandes bombas explodiram durante o século XX: (1) a demográfica, (2) a atômica e (3) das telecomunicações. Nos dizeres de Pierre Lévy (1999, p.13), esta última assim considerada por gerar grande movimentação de informação, com aumento vertiginoso da disponibilidade de dados de fácil acesso.

Precedida pela comunicação exclusivamente oral e posterior surgimento da escrita estática, e, proporcionada pelo desenvolvimento das tecnologias digitais de informação e comunicação, a comunicação interativa, virtual, traz em seu bojo facilidades na transmissão e na circulação do conhecimento. Entretanto, trouxe também implicações sociais, econômicas e jurídicas.

O ciberespaço, assim denominado por Lévy (1999, p. 17), se consubstancia na infraestrutura material da comunicação digital, nos dados informacionais nela inseridos, assim como os seres humanos que dela se valem e fez emergir uma nova cultura: a cibercultura.

Referida cultura, por ganhar dimensionamento próprio, diante de suas peculiaridades e da interatividade humana em sua consecução, também alcança contornos de ordem social e jurídico.

Utilizado como meio de comunicação e de transmissão de informação, o ciberespaço fornece ambiente propício para acesso aos hipertextos, às informações editáveis (WIKI), sons, imagens e comunicação interativa síncrona e assíncrona nas redes sociais, em que os seres humanos compartilham informação e interagem entre si sem limitação territorial ou temporal.

Assim, é possível executar inúmeras tarefas ao mesmo tempo e sem locomoção física. Pois bem, se de um lado temos esse desdobramento temporal e espacial como solução às necessidades da nossa época, por outro existem as implicações morais e jurídicas do mesmo desdobramento.

Diante da utilização do ciberespaço como meio de comunicação, conforme André Lemos e Pierre Lévy (2010, p.25), emanaram princípios da ligação entre a tecnologia e os processos comunicacionais na cibercultura: (1) liberação da palavra, (2) inteligência artificial, (3) reconfiguração social, cultural e política.

O primeiro princípio da cibercultura é o da "liberação" da palavra, na formação da opinião e da esfera pública, tendo em vista a ampliação do círculo da conversação mundial, por intermédio dos "*blogs, wikins, podcasting, softwares* sociais como o *Orkut* e o *Facebook*", permitindo a troca de informações entre pessoas e comunidades (LEMOS; LÉVY, 2010, p. 26).

Do primeiro emerge o segundo: a "inteligência coletiva", uma vez que a interatividade planetária, proporcionada pelo ciberespaço, abre novos horizontes aos seres humanos formando uma nova concepção de mundo. Este novo paradigma mundial enseja o terceiro princípio da cibercultura denominado de "reconfiguração social, cultural e política" (LEMOS; LÉVY, 2010, p. 26)

A problemática se instaura porque o ciberespaço permite um novo espaço para debates mundiais, sem regramento ou observância dos ditames morais e legais preconizados pela sociedade em que seus atores estão inseridos, consubstanciando em desterritorialização estatal diante da ausência de contrato social estabelecido, convolando na falsa ideia de liberdade absoluta no espaço virtual.

Vale lembrar que nas palavras de Thomas Hobbes (1651, p. 47) segundo as leis naturais a liberdade consiste:

> Por liberdade entende-se, conforme a significação própria da palavra, a ausência de impedimentos externos, impedimentos que muitas vezes tiram parte do poder que cada um tem de fazer o que quer, mas não podem obstar a que use o poder que lhe resta, conforme o que seu julgamento e razão lhe ditarem.

Destarte, assumindo que o ciberespaço reúne homens em uma sociedade virtual, que dada a sua proporção planetária de interação instaure um novo processo de caos diante da ausência de soberania, ou seja, a desterritorialização estatal, os internautas estariam sob as leis da natureza ou direito natural e em liberdade, tal como preconizada em Hobbes.

Daí a necessidade de relembrar o alerta feito pelo filósofo contratualista em sua obra O Leviatã (HOBBES, 1651, p. 48) sobre o exercício da liberdade humana plena:

> (...) a condição do homem é uma condição de guerra de todos contra todos, sendo neste caso cada um governado por sua própria razão, e não havendo nada, de que possa lançar mão, que não possa servir-lhe de ajuda para a preservação de sua vida contra seus inimigos, segue-se daqui que numa tal condição todo homem tem direito a todas as coisas, incluindo os corpos dos outros. Portanto, enquanto perdurar este direito de cada homem a todas as coisas, não poderá haver para nenhum homem (por mais forte e sábio que seja) a segurança de viver todo o tempo que geralmente a natureza permite aos homens viver.

O alerta feito no século XVII parece ser tão recente, pois a cada minuto novos dados são inseridos no ciberespaço, mais computadores são conectados à rede mundial e mais informações são apropriadas e transmitidas pelos usuários da rede. Com efeito, isso gera grande preocupação quanto à confiabilidade e a legalidade na transmissão dos referidos dados, assim como a segurança jurídica neste novo ambiente.

A preocupação vai além da confiabilidade e da legalidade da simples transmissão da informação no ambiente virtual, pois sem regramento na manipulação dos dados no ciberespaço poderá acarretar em violação dos direitos e garantias preconizados pela sociedade, na busca da paz social, e, convolando em atentado contra a proteção da dignidade da pessoa humana.

Diante destes fatos, os Estados têm discutido diretrizes na manipulação virtual de dados e informações e editado marco próprio e unificado para a proteção de dados pessoais na comunicação eletrônica, como garantia de defesa dos direitos da personalidade em atenção à dignidade e proteção dos Direitos Humanos, ao mesmo

tempo que têm evitado exagerar em legislações nacionais para não dificultarem a difusão das novas tecnologias, ou até mesmo para não evidenciarem os seus limites nessa nova realidade.

2. Segurança digital como (novo) Direito Humano

A segurança de dados no ciberespaço fomenta discussões calorosas sobre os limites das liberdades na rede mundial de computadores e a proteção ao usuário. Não é só a intimidade da vida privada dos cidadãos da aldeia digital o mote primordial nas referidas discussões, mas, principalmente, a proteção do internauta ante sua vulnerabilidade e hipossuficiência técnica na manipulação do meio comunicacional planetário.

Para Pérez Luño "um dos desafios mais importantes de nossa época consiste em estabelecer uma equação exata, correspondente às restrições do tempo, sobre as relações entre os avanços tecnológicos e a proteção das liberdades"[1] (2010, p. 101).

Alerta o Autor espanhol, sobre as consequências da consolidação da "aldeia global" e os escândalos não muito distantes que abalaram a opinião pública européia quanto ao tráfego de imagens de prostituição infantil e difusão de propaganda neonazista e terrorista, o que confirmou os perigos noticiados por diversos estudiosos no decorrer dos últimos trinta anos quanto a manipulação das novas tecnologias e a possibilidade de ser utilizada como instrumento para violação dos direitos da personalidade e meio de incremento da criminalidade como nas sabotagens, furto de dados, pelos incontáveis piratas cibernéticos (LUÑO, 2010, p. 104).

Em analogia ao estado de natureza hobbesiano, a liberdade exacerbada no ciberespaço nos conduz a mesma solução contra os vilipêndios às liberdades fundamentais, qual seja, a intervenção do Leviatã para instituição de regramento mínimo de conduta para ilidir os abusos e amenizar os riscos no ambiente virtual.

Há, portanto, a real necessidade de regulamentação da ordem social no espaço virtual, pois conforme preconizado por Jean-Jacques Rousseau, em sua obra O contrato social "(...) a ordem social é um direito sagrado que serve de alicerce a todos os outros. Esse direito, todavia, não vem da natureza; está, pois, fundamentado sobre convenções" (2002, p. 5).

[1] "Uno de los retos más importantes de la época en que vivimos consiste en establecer una ecuación exacta, correspondiente a los apremios del tiempo, en las relaciones entre los avances tecnológicos y la tutela de las libertades".

Analisando o ciberespaço como uma sociedade no espaço virtual, encontramos alguns regramentos em alguns países já instituíram normas para as relações no espaço virtual, como forma de regramento que não fira os direitos já consagrados e ao mesmo tempo proteja os mesmos direitos. Ainda na mesma esteira de pensamento de Rousseau (2002, pp. 9-10):

Encontrar uma forma de associação que defenda e proteja de toda a força comum a pessoa e os bens de cada associado, e pela qual, cada um, unindo-se a todos, não obedeça, portanto senão a si mesmo, e permaneça tão livre como anteriormente. Tal é o problema fundamental cuja solução é dada pelo Contrato Social.

Neste sentido no plano internacional regional, a União Européia editou diretivas para a proteção das pessoas com relação ao tratamento de seus dados pessoais, a primeira em 1995, que traz em um de seus considerandos que os sistemas de tratamento de dados estão ao serviço do Homem e que devem respeitar as liberdades e os direitos fundamentais das pessoas, em atendimento aos princípios contidos na Convenção do Conselho da Europa, de 28 de Janeiro de 1981, relativa à proteção das pessoas no que diz respeito ao tratamento automatizado de dados pessoais.

Ainda na União Européia, fora editada outra diretiva para o tratamento de dados pessoais e proteção da privacidade no setor das comunicações eletrônicas, em 2002, visando assegurar o respeito aos direitos fundamentais e a observância dos princípios reconhecidos, em especial, pela Carta dos Direitos Fundamentais da União Européia.

Isso sem dizer no parecer do Comitê Econômico e Social Europeu sobre o Livro Verde. Segundo tal documento "Um mercado de entrega de encomendas integrado para o crescimento do comércio eletrônico na UE" é necessário para recuperar a confiança do consumidor, assegurar a concorrência leal e a responsabilidade no comércio eletrônico e divulgação de propagandas que protejam as crianças e a dignidade humana, para tanto, as condiciona a três exigências cumulativas: proibição de arbitrariedade, necessidade social e legitimidades dos objetivos.

No plano interno, instituiu-se a Política Nacional de Informática pela da Lei 7.232 de 1984, tendo por objetivo a capacitação nacional nas atividades de informática, em proveito do desenvolvimento social, cultural, político, tecnológico e econômico da sociedade brasileira.

Já na Administração Pública Federal, fora editado o Decreto 3.505 de 2000 que instituiu a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal, tendo como um de seus pressupostos básicos o

de assegurar os direitos individuais e coletivos das pessoas, à inviolabilidade da sua intimidade e ao sigilo da correspondência e das comunicações por meio da proteção dos sistemas de informação, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados em seus bancos de dados.

Com o advento da Lei 11.419 de 2006, que disciplina a informatização do processo judicial, surge preocupação com o sistema de gestão de documentos eletrônicos (GDE) - este compreendido como conjunto de tecnologias que permite o gerenciamento de documentos de forma digital - dada a relevância do teor dos documentos e dos atos processuais que tramitarão exclusivamente por meio digital no ciberespaço e a segurança exigida para o referido procedimento, como garantia aos direitos fundamentais dos envolvidos no processo judicial.

Na mesma esteira de pensamento de Almeida Filho (2007, p. 166), para ilidir a possibilidade de quebra da segurança jurídica do Estado Democrático de Direito, mister se faz a implantação de política de segurança da informação, com normas previamente estipuladas e em observância aos referenciais contidos na norma ABNT 27.001 de 2006, que tem por finalidade prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI).

A problemática suscitada pelo avanço das novas tecnologias e o processo de desterritorialização no ciberespaço, propiciado pela cibercultura, trouxe a necessidade de se instituir um marco regulatório civil do uso da internet no Brasil, para disciplinar os direitos individuais e coletivos, a responsabilidade dos atores, e, as diretrizes governamentais na política de proteção, assim, fora apresentado o Projeto de Lei (PL) 2126/11, apensado ao PL 5403/01, com a finalidade de estabelecer princípios, garantias, direitos e deveres para o uso da Internet no Brasil e determinar as diretrizes da atuação estatal.

Referido PL traz em seu artigo 2º os fundamentos da disciplina do uso da internet no Brasil, dentre eles os Direitos Humanos e o exercício da cidadania em meios digitais e no artigo terceiro os princípios, do quais se destacam a proteção da privacidade e da proteção dos dados pessoais, assim como o dever de observância aos princípios insculpidos no ordenamento pátrio e nos tratados internacionais em que o Brasil seja parte.

Em que pese todas as regras, princípios, fundamentos e objetivos do Estado Democrático de Direito já disciplinados no ordenamento interno, a edição de marco regulatório para o uso da internet no Brasil se faz indispensável à proteção da sociedade brasileira, quer seja pelo regramento de uso da ferramenta comunicacional, quer seja pela proteção dos dados nela transmitidos.

Isto porque, como alhures mencionado, o ciberespaço proporciona comunicação interplanetária, o que importa dizer a desterritorialização do espaço cibernético, pois os agentes que utilizam a internet como meio de comunicação não sofrem limitação de tempo ou espaço territorial, razão pela qual se torna incerta ou duvidosa a aplicação da lei nas relações havidas no ciberespaço e fundamenta a necessidade de um marco regulatório brasileiro.

Não obstante a ausência de lei especifica quanto à proteção dos dados pessoais no uso da internet no Brasil, o direito à intimidade e o direito a vida privada são reconhecidos como direitos fundamentais pela nossa Constituição Federal. Além da inviolabilidade do sigilo da correspondência e das comunicações telegráficas, de dados e telefônicas.

Uma das preocupações suscitadas no PL 2.126/2011 é o de garantir o acesso à internet como essencial ao exercício da cibercidadania e assegurar aos internautas os direitos inerentes à consecução ao acesso efetivo, dentre eles a inviolabilidade do sigilo das comunicações pela internet, salvo por ordem judicial.

Não obstante a necessidade de regulamentação interna, para tentar ilidir ou amenizar a possibilidade de violação aos direitos no ciberespaço, forçoso se faz ponderar a problemática em sua aplicabilidade, uma vez que os atores das relações jurídicas podem ser oriundos de diversos Estados (desterritorialização), assim, o regramento somente será aplicável se legitimado por todos os envolvidos.

Nos dizeres de Lévy (1999, p. 113) "quanto mais o ciberespaço se amplia, mais ele se torna 'universal', e menos o mundo informacional se torna totalizável", em outras palavras, o ciberespaço aceita todos sem distinção de credo, cor ou soberania, e, se constrói apesar das regras das soberanias em que seus participantes estão inseridos.

Além da celeuma da dificuldade na fiscalização do (des) cumprimento do regramento no ciberespaço, diante das peculiaridades da rede mundial de computadores, quer seja na identificação dos responsáveis, quer seja na imputação dos limites de responsabilização dos envolvidos e a execução das sanções a serem estabelecidas, diante da soberania, ainda que relativizada, dos Estados e seus cidadãos pelo (des) cumprimento das obrigações a serem estatuídas.

Outra questão polêmica versa sobre a guarda de *logs*, ou da retenção de dados pessoais, pelos provedores de acesso à internet e provedores de conteúdo ou serviços, isto porque a não regulamentação quanto a forma de guarda e segurança desses dados poderia ser subvertido em constante monitoramento de trafego de dados pessoais dos usuários afrontando, assim, o direito fundamental à inviolabilidade de sigilo de comunicação.

Tendo em vista que o ciberespaço é instrumento comunicacional de ordem planetária, deve ser entendido desta maneira, ou seja, como um meio e não um fim e si mesmo. Logo, as mesmas regras de condutas utilizados na comunicação por meio de átomos, devem ser de observância na comunicação por meio de bits.

Nesta toada Giddens (2007), na obra Mundo em descontrole, como resultado de uma série de palestras proferidas pelo autor em 1999, ao analisar o impacto da globalização em nossas vidas, bem asseverou quanto a evolução comunicacional que a comunicação eletrônica instantânea não se consubstancia apenas uma forma pela qual as notícias ou informações são trazidas a nós, mas que além disso sua existência altera a textura de nossas vidas e dada sua dimensão somos propelidos a uma ordem global.

Em definitivo, o ciberespaço não é um "espaço" sem leis ou sem regras, mas ao contrário, por se tratar ferramenta de interação mundial, as regras de todos os seus participantes devem ser observadas, daí a celeuma do tema – como identificar qual regra, de qual país e em que momento deverá ser utilizada para disciplinar as relações jurídicas havidas no espaço virtual diante da problemática da desterritorialização do ciberespaço.

Como bem pontuado por Lévy (1999, p. 210), as legislações locais só podem ser aplicadas em razão e nos limites das fronteiras do Estado que as emanou, assim, o ciberespaço possibilita que as leis sobre as relações jurídicas de toda natureza sejam violadas, bastando para tanto que o "servidor que distribua ou organize as comunicações violadoras esteja instalado em qualquer paraíso de dados".

Desta forma a cibersegurança ou segurança no ciberespaço se tornou tema recorrente nas discussões sobre a proteção dos dados em diversos países após a denúncia, amplamente divulgada pelos meios de comunicação, de um esquema de espionagem feito por agências secretas dos Estados Unidos a diversos países, incluindo o Brasil, feita pelo ex-funcionário de uma empresa que presta serviços a Agência Nacional de Segurança (NSA), o norte-americano Edward Snowden.

Antes mesmo da referida denúncia, Pérez Luño já noticiava que os Estados Unidos em colaboração com o Reino Unido, Canadá, Austrália e Nova Zelândia utilizavam um sistema de espionagem conhecido como *Echelon* que teria por característica principal o exercício do controle simultâneo de todas as comunicações, inclusive pela internet, por satélite (2010, p.107).

Em 26 de Abril de 2013, a Câmara dos Representantes dos EUA aprovou a lei de Compartilhamento e Proteção de Ciberinteligência (CISPA) com o discurso de "proporcionar o compartilhamento de certa inteligência e informações de ciberameaças entre a comunidade de inteligência e entidades de segurança

cibernética", para obrigar as empresas de comunicação informática, como os sítios de busca na rede e das redes sociais, a entregarem ao governo todos os dados que poderiam ser usados para combater ataques cibernéticos em prol da cibersegurança.

Entretanto, a CISPA tem sofrido diversas criticas das entidades vinculadas aos Direitos Humanos, inclusive, com ameaça de veto presidencial, pois atenta contra as liberdades e outros direitos garantidos, quando obriga as empresas eletrônicas a fornecerem os dados de seus usuários, mesmo sem motivar o pedido ou ordem judicial para tanto.

Vale lembrar que o ciberespaço, enquanto meio de comunicação planetária, envolve internautas de diversos Estados e suas informações pessoais são retidas e armazenadas no ciberespaço.

Assim, a proteção digital pode ser entendida como um Direito Humano, uma vez que a proteção para a segurança da inviolabilidade e o sigilo de dados alcança esfera global, tendo como sujeitos de direito a comunidade planetária que se utiliza da rede mundial de computadores, também conhecida como sociedade da informação.

A evolução conceitual de pessoa humana, enquanto sujeito dos Direitos Humanos, se deu na busca pela igualdade todos os seres humanos, teve na primeira grande discussão conceitual entre os Doutores da Igreja que analisando a identidade de Cristo decidiram, como dogma de fé, que Jesus Cristo possuía uma dupla natureza, humana e divina, numa única pessoa, daí as demais pessoas serem humanas, somente. Na segunda elaboração história conceitual se deu com Boécio que identificou de certa forma a aproximação pessoa humana e o divino, corroborado pelo pensamento tomista de que o homem é um composto de substância espiritual e corporal. Sendo essa igualdade de essência o núcleo do conceito universal de Direitos Humanos (COMPARATO, 2005, pp. 18-20).

Em momento histórico posterior na conceituação se pautou no pensamento kantiano do imperativo categórico, "a dignidade da pessoa não consiste apenas no fato de ser ela, diferentemente das coisas, um ser considerado em si mesmo, como um fim e não como um meio, mas também do exercício de sua autonomia, guiado pelas próprias leis que edita" (COMPARATO, 2005, p. 21).

Fazendo um grande salto na história, para situarmos a problemática da segurança de dados, forçoso concluir que diante do estabelecimento das regras internas e internacionais, além da delegação de competência supranacional na fiscalização e punição às violações aos Direitos Humanos – nas Convenções e Tratados Internacionais de Direito Humanos – para a proteção da pessoa humana assim considerada como um fim em si mesma, não pode um Estado, unilateralmente, editar normas que pretenda relativizar direitos já consagrados em caráter universal.

Nesta toada, temos que a CISPA afrontaria flagrantemente os princípios abarcados na Declaração Universal dos Direitos Humanos que consagra a liberdade de receber e transmitir informações por qualquer meio e independente de fronteiras (XIX) e a defesa da vida privada e da proteção de correspondência (XII), sendo defeso a qualquer Estado sua interpretação com a finalidade de pratica de qualquer ato que tenha por intenção destruir os direitos nela declarados (XXX) – vedação de retrocesso aos Direitos Humanos, violando também a Convenção Interamericana de Direitos Humanos (art. 29).

Dada a escala de alcance da proteção da segurança digital dos usuários do ciberespaço, assim reconhecido como (novo) Direito Humano poderia ser classificado, dentro do processo dinamogênico de declaração e proteção aos Direitos Humanos, como direito de quarta ou quinta geração, a depender da classificação utilizada.

Por processo dinamogênico entende-se "o processo histórico de reivindicação/exigência da declaração e proteção aos direitos inerentes ao homem, consubstanciando em direito de conquista e não mero enquadramento" (SILVEIRA; ROCASOLANO, 2010, p. 109).

Em que pese as discussões doutrinárias quanto a nomenclatura e da existência de todas as classificações de Direitos Humanos, e na mesma esteira de pensamento de Norberto Bobbio (2004, p. 25), temos que o maior problema de nosso tempo já superou o da necessidade de se fundamentar a positivação dos direitos do homem, transladando-se para outro mais importante: sua proteção.

Desta maneira, já nos afastamos da seara filosófica, transpondo as barreiras da conceituação e tentativa da fundamentação do direito como absoluto ou relativo, para nos preocuparmos em tentar alcançar a efetivação dos direitos declarados, ou seja, nas searas jurídica e política.

Daí a justificativa para a positivação do marco civil regulatório do uso da internet no Brasil visando garantir a proteção dos dados pessoais dos internautas, para dar efetividade aos Direitos Humanos já consagrados, em atenção à vedação de retrocesso, para ilidir as possíveis violações sob a alegação de ausência ou incerteza de regulamentação.

No plano internacional, mister se faz a abertura de discussões para a busca de uma hegemonização das soberanias e uma conversação sobre os *standards* no regramento das relações havidas no âmbito do espaço virtual, pois do processo da globalização comunicacional surgiu a nova realidade social, qual seja, o ciberespaço que se constrói e evolui com, sem e apesar das soberanias dos Estados em que os internautas estão inseridos.

Nesta conjectura, Wagner Menezes, em sua obra Ordem global e transnormatividade (2005, p.114), defende que o Direito Internacional "amplia seu campo de atuação e se legitima como instrumento capaz de regular a sociedade que se desenha" na busca de respostas globais aos problemas e às relações jurídicas que surgem da nova realidade social, mediante regramentos oriundos da conversação entre as soberanias e a conseqüente delegação de competência aos foros internacionais, na transnormatização das leis locais e internacionais, tendo em vista a imprescindível manutenção de um senso de justiça internacional, cujas regras não desviem do bem-estar geral.

3. A dicotomia entre direito de informação e a proteção de dados pessoais: implantação do processo judicial eletrônico e a segurança digital

Segundo estudo sobre os princípios para a formação de um regime de dados pessoais, elaborado por Manoel J. Pereira dos Santos (2008, pp. 355-374), as inovações técnicas, no processo da "convergência tecnológica", deu ensejo à sociedade da informação, em que os dados constituem matéria prima da informação, que passa a ter valor econômico.

Dentre os dados informacionais, os pessoais se revestem de interesse de tutela legal, pois refletem a personalidade de alguém, vinculado a um sujeito determinado ou determinável (SANTOS, 2008, p. 358).

No direito comparado, já existe regramento para a proteção de dados pessoais, como alhures mencionado, que trazem em seu bojo princípios norteadores para que os bancos de dados possam coletar, manipular e armazenar os dados pessoais, uma vez, que diante da natureza dos referidos dados, são suscetíveis de ocasionarem violação as liberdades fundamentais ou do direito à vida privada de seus titulares.

Para tanto, disciplinam as condições gerais de licitude e da qualidade dos dados a serem coletados e manipulados. Dentre eles: 1. Princípio da publicidade ou transparência; 2. Da informação e exatidão dos dados, informação clara e precisa da espécie e conteúdo dos dados armazenados e o período de conservação e utilização (direito de oposição); 3. Da finalidade e razoabilidade, consistente na segurança da utilização dos dados na função para qual foram coletados (limitação de uso); 4. Da licitude e da lealdade, consubstanciado na forma pela qual os dados foram obtidos; 5. Da confidencialidade e segurança, que impõe ao responsável pelo banco de dados o dever de tomar as medidas necessárias à proteção dos dados armazenados; e, 6. Da temporalidade, constituindo princípio geral que os dados não devem ser armazenados por tempo indeterminado, salvo quando necessários para finalidades históricas, casos em que os dados deverão ser tronados anônimos (SANTOS, 2008, pp.360-367).

Diante da ausência de regramento interno específico sobre o tratamento de dados pessoais e a problemática do potencial lesivo na subversão da manipulação dos referidos dados, passaremos a analisar os regramentos esparsos em nosso ordenamento na busca pelo reconhecimento de algum sistema protetivo à segurança digital e a dicotomia entre o direito a informação e a segurança de dados.

Segundo a Constituição Federal da República Federativa do Brasil, em seu artigo 5º, XXXIII, "todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo", princípio que deve ser garantido com a finalidade de fomentar a transparência e a democracia participativa.

Preconizado no rol do artigo 5º da Constituição Federal, o direito à informação é direito fundamental do brasileiro e deve ser exercido por intermédio de pesquisas de conteúdo de domínio público para não ferir o direito à privacidade e da segurança de dados pessoais.

Desta forma, para viabilizar o exercício ao direito à informação foi sancionada a Lei 12.527/2011, subordinando os órgãos dos Poderes Executivo, Legislativo, Judiciário e do Ministério Público, às suas diretrizes e atribuindo-lhes o dever de divulgação em local de fácil acesso, às informações de interesse coletivo ou geral por eles produzidas ou custodiadas, independente de requerimentos, e, ainda tornando obrigatória a divulgação em sítios oficiais da rede mundial de computadores.

Na seara do Poder Judiciário, o Conselho Nacional de Justiça editou metas para dar transparência e eficiência da consecução de suas atividades em prol dos jurisdicionados. Para tanto, criou o Comitê Nacional de Gestão de Tecnologia da Informação e Comunicação do Poder Judiciário, que tem por objetivo estabelecer diretrizes da segurança da informação.

E, com o advento da Lei 11.419/2006 que inaugurou a nova fase processual com a possibilidade de implantação do processo judicial eletrônico já vislumbramos as melhorias na informatização de alguns serviços judiciais, uma vez que não se fará[2] necessário o deslocamento até o cartório para visualizar um andamento processual.

Deste modo, bastará acessar o sitio do Tribunal e consultar por meio eletrônico o nome das partes, advogados ou numero do processo, além da utilização do sistema *push*, em que o interessado, após cadastramento, poderá receber informações relativas aos processos de seu interesse via *e-mail*, dando maior acesso às informações judiciais.

[2] Falamos no futuro, pois apesar de já ser uma realidade em alguns Tribunais, o sistema ainda não se consolidou. O Brasil hoje possui 45 (quarenta e cinco) sistemas diversos de peticionamento e acesso eletrônico processual e em alguns estados da federação sequer possui acesso à rede mundial de computadores, apresentando significativa problemática ainda não solucionada.

Além disso, será possível solicitar e consultar pesquisa jurisprudencial em todas as instâncias, acessar as consultas dos indicadores de desempenho e metas a serem alcançadas e o peticionamento eletrônico e a digitalização das peças processuais, o que, facilitará enormemente a vida dos jurisdicionados, pela transparência e acessibilidade.

Com a implantação do processo judicial eletrônico, o direito à informação se tornou mais palpável, pois com a informatização dos atos processuais, além da transparência dos andamentos processuais, deu-se nova dimensão ao princípio do acesso à justiça aos jurisdicionados, uma vez que proporciona aos interessados maior acessibilidade às informações no desenrolar de determinados litígios.

A princípio adotou-se o processo digital, diante da digitalização não só das manifestações dos atores no processo judicial, mas também dos documentos probatórios dos fatos alegados e das ordens exaradas da autoridade judicial. Posteriormente, iniciou-se a implantação do processo judicial eletrônico (PJe), um software criado pelo Conselho Nacional de Justiça (CNJ) para dar fim ao processo de papel e criar o processo judicial totalmente informatizado.

Desta forma, o PJe não se trata de mera digitalização do processo, mas de efetiva implantação de processo totalmente eletrônico, ou seja, com elaboração dos documentos processuais no próprio sistema, por meio de um editor de texto integrado ao navegador da *WEB*, mesmo sistema utilizado na execução de emails e postagens em *blogs*.

A dicotomia se instaura quando nos deparamos com a realidade de que, nos exatos termos do Art. 5º, LX da Constituição Federal, o princípio da publicidade dos atos processuais é regra, somente sendo restringido, quando a defesa da intimidade ou interesse social o exigirem.

Notadamente, o direito à informação, fundamento do princípio da publicidade dos atos processuais, traz a baila outra discussão: a informação como um bem jurídico a ser tutelado, haja vista que graças à rede mundial de computadores, a informação acabou transformada em mercadoria.

Os dados disponibilizados pelos próprios usuários são comercializados no ciberespaço, e, com a utilização dos serviços gratuitos de e-mails, buscas, localizadores, redes sociais, redes profissionais, assim como de sítios de compras coletivas, a informação e os dados pessoais das transações serão retidos no ciberespaço, podendo ser manipulados, cedidos e até subtraídos.

Neste sentido, Teresa Pasquino (2008, pp. 697-701) em seu estudo sobre os Serviços da sociedade de informação: Tutela dos dados pessoais e regras de conduta, adverte que "a telemática mundial tornou-se o espaço metajurídico".

Em que por se penetrar com a finalidade de usufruir dos serviços prestados na sociedade da informação, os dados fornecidos por aqueles que nele interagem são registrados automaticamente em cada acesso (retenção de *logs*), além da coleta por meio de *coockies* ou arquivos do navegador, como contraprestação pela utilização "gratuita" do servidor, para depois da autorização do usuário mediante o *login* no navegador, possam ser direcionados às publicidades de produtos de interesse do usuário, formando um gigantesco banco de dados pessoais e comerciais que são comercializados diuturnamente.

Esta realidade ficou latente com o escândalo ocorrido no Brasil no recente convênio firmado entre o Tribunal Superior Eleitoral (TSE) e a empresa privada Serasa, que gerencia um banco de dados sobre a situação de crédito dos consumidores do País, o TSE decidiu repassar informações cadastrais de 141 milhões de brasileiros para a empresa. O acesso foi determinado por um acordo de cooperação técnica entre o TSE e a Serasa, publicado no dia 23 de julho de 2013, no Diário Oficial da União.

Pelo acordo, o Tribunal entregaria para a empresa privada os nomes dos eleitores, número e situação da inscrição eleitoral, além de informações sobre eventuais óbitos, inclusive a filiação dos cidadãos e a data de nascimento para verificação de homônimos, a serem disponibilizadas aos clientes da empresa nas consultas aos seus bancos de dados.

Tendo em vista a possibilidade de violação ao direito a privacidade dos cidadãos na execução do referido convênio, em 08 de agosto de 2013, a corregedora-geral eleitoral, Laurita Vaz, suspendeu o acordo firmado entre o TSE e a Serasa, até que o plenário da corte decida sobre o assunto.

O que corrobora o entendimento da necessidade de regramento quanto a manipulação e disposição dos dados pessoais dos usuários da rede mundial de computadores no plano interno e internacional.

Além disso, as recentes invasões por *hackers* aos sítios do governo brasileiro tais como a feita pelo grupo *Anonymous* ao sitio da Companhia Paulista de Trens Metropolitanos (CTPM) em 10/02/2013, o ataque simultâneo aos sitio da Receita Federal, Presidência da República, Instituto Brasileiro de Geografia e Estatística (IBGE), Ministério do Esporte e Petrobrás, que foram amplamente divulgadas em 2011, trazem à baila a discussão quanto a segurança dos dados do processo judicial eletrônico.

Conforme relatório do assessor da Organização Mundial de Direito e Informática (OMDI), Mário Paiva (2007), diante dos estudos sobre as novas ferramentas preconizadas pela Lei 11.419/2006, os itens indispensáveis à segurança

dos documentos eletrônicos são a autenticidade tanto do documento, quanto de seu autor, para proteção aos jurisdicionados; a integridade dos documentos eletrônicos que não podem ser objeto de alterações que lhes modifiquem o conteúdo; e, a confidencialidade do acesso aos documentos eletrônicos tem de ser controlado com o uso de técnicas de criptografia.

Com efeito, a Lei 11.419/06 quando possibilitou a criação e tramitação por meio eletrônico, preferencialmente pela rede mundial de computadores, o que autorizou o manejo de qualquer dos meios disponíveis e não só por meio de chave criptografada.

Segundo consta na cartilha do processo judicial eletrônico (PJe) do CNJ, as informações transmitidas via web passarão a ser de responsabilidade do departamento da Tecnologia da informação (TI), para a criação de perfis dos usuários e, inclusive, facilitando a criação de mais de um perfil para o mesmo usuário, o que por si só gera grande preocupação quanto à autenticidade e confiabilidade, ante a possibilidade dos dados serem alterados e o conteúdos dos documentos modificados e apropriados por *hackers*.

Destarte, o direito à informação, direito fundamental abarcado no rol do art. 5º da Constituição Federal, acaba por afrontar outro direito fundamental, qual seja, o direito à privacidade e a intimidade, consubstanciando no direito à segurança digital, uma vez que a publicidade expandida dos dados dos jurisdicionados, ainda que sob segredo de justiça, poderão ser apropriados indevidamente na rede.

Pois bem, com a implementação do processo judicial eletrônico e a publicidade dos atos processuais, restou demonstrado que o direito fundamental à privacidade não é absoluto, na medida em que o individuo ao provocar a tutela jurisdicional terá seus dados pessoais disponibilizados no ciberespaço, salvo os casos em que é atribuído o segredo de justiça ao processo.

Uma vez que o marco civil regulatório do uso da internet no Brasil ainda não foi sancionado e que a política de proteção e segurança da informação não abarca a proteção dos dados pessoais que constarão nos processos eletrônicos, imperativo que diretrizes sejam editadas para a implantação segura do processo judicial eletrônico.

Tais diretrizes deverão abordar as responsabilidades e soluções para possíveis falhas de sistema, invasão por grupos de *hackers*, perda de documento, proteção aos perfis de identificação no sistema, proteção aos dados pessoais dos jurisdicionados, recuperação de dados e armazenamento – GED – para viabilizar o exercício ao direito à segurança digital, uma vez que o deslocamento da sociedade real para o

espaço metajurídico ou ciberespaço e a problemática da desterritorialização estatal não eximem os Estados de prestarem jurisdição às relações havidas dessa nova realidade.

CONCLUSÃO

Diante da pesquisa realizada sobre a evolução da sociedade da informação concluiu-se que diante da modificação no comportamento da sociedade global com as novas tecnologias, o nascimento do ciberespaço como meio comunicacional interplanetário e a evolução da cidadania local para cibercidadania há necessidade de tutelar as relações havidas no ciberespaço, assim como a proteção aos dados pessoais dos usuários da rede mundial de computadores, todavia sem exageros que prejudiquem esta realidade.

Estudada a matéria da proteção de dados e a cibersegurança, tendo em vista que o ciberespaço envolve internautas de diversos Estados e suas informações pessoais são retidas e armazenadas no ciberespaço, concluiu-se que a proteção digital pode ser entendida como um Direito Humano, uma vez que a proteção ao direito da inviolabilidade e do sigilo de dados alcança esfera global.

E, ainda, que em analogia ao estado de natureza hobesiana, concluiu-se que a problemática da desterritorialização do ciberespaço, não justifica o abandono estatal da proteção aos usuários da rede mundial de computadores, tampouco, autoriza a invasão aos direitos e garantias à segurança digital e aos Direitos Humanos já consagrados.

Neste sentido, analisada a matéria relativa dicotomia entre direito à informação e proteção de dados pessoais na implantação do processo judicial eletrônico e a segurança digital concluiu-se que a instrumentalização digital do processo judicial a *priori* contribui para o acesso à justiça, diante da acessibilidade e transparência dos atos processuais pelos jurisdicionados. Entretanto, dada a ausência de regramento protetivo dos dados pessoais dos jurisdicionados no Brasil, o processo judicial eletrônico, nos moldes que fora esculpido, acaba por vulnerar a segurança digital e, logo os Direitos Humanos.

Por fim, entendendo a segurança digital como Direito Humano concluiu-se pela necessidade de regulamentação quanto ao uso da internet no Brasil e em acordos internacionais, pontualmente quanto a proteção das informações e dos dados pessoais transmitidos no ciberespaço, para ilidir possíveis violações sob alegação de ausência ou incerteza de regramento específico.

REFERÊNCIAS

ALMEIDA FILHO, José Carlos de Araújo. A segurança da informação no processo eletrônico e a necessidade de regulamentação da privacidade de dados. **Revista de Processo**, v. 32, n. 152, pp. 165-180, out. 2007.

BOBBIO, Norberto. **A era dos direitos.** Tradução de Carlos Nelson Coutinho; apresentação de Celso Lafer. Rio de Janeiro: Elsevier, 2004.

CAPANEMA, Walter Aranha. **O spam e as pragas digitais: uma visão jurídico-tecnológica**. São Paulo: LTr, 2009.

COMPARATO, Fábio Konder. **A afirmação histórica dos direitos humanos.** São Paulo: Saraiva, 2005.

CONTE, Christiany Pegorari. Eficiência da justiça e duração razoável do processo na sociedade da informação: breves considerações acerca da informatização da atividade jurisdicional. In: SILVEIRA, Vladmir Oliveira da; MEZZAROBA, Orides (Coord.); MAILLART, Adriana S.; COUTO, Monica Bonetti Couto et al (org.). **Justiça e [o Paradigma da] Eficiência**. Coleção: Justiça, Empresa e Sustentabilidade [vol. 1]. São Paulo: Revista dos Tribunais, 2011, pp. 66-88.

DE LUCCA, Newton. **Aspectos jurídicos da contratação informática e telemática**. São Paulo: Saraiva, 2003.

_____. **Direito & Internet- Aspectos Jurídicos Relevantes**, 1º Edição, São Paulo: Quartier Latin, 2000.

GED – Gestão eletrônica de documentos. Disponível em: http://www.ged.net.br/definicoes-ged.html. Acesso em 11 Ago de 2013.

GIDDENS, Anthony. **Mundo em descontrole: o que a globalização está fazendo de nós**. Rio de Janeiro: Record, 2007.

HOBBES, Thomas. **O Leviatã ou matéria, forma e poder de um Estado eclesiástico e civil**. Tradução de João Paulo Monteiro e Maria Beatriz Nizza da Silva. Disponível em: http://www.dhnet.org.br/direitos/anthist/marcos/hdh_thomas_hobbes_leviatan.pdf. Acesso em: 07 set 2013.

LEMOS, André. **O futuro da internet: em direção a uma ciberdemocracia** / André Lemose Pierre Lévy. São Paulo: Paulus, 2010.

LÉVY, Pierre. **Cibercultura**, São Paulo: Editora 34, 2º reimpressão, 2001.

_____. **O que é virtual?** (tradução de Paulo Neves) São Paulo: Editora 34, 5ª reimpressão, 2001.

MENEZES, Wagner. **Ordem global e transnormatividade**. – Rio Grande do Sul: UNIJUÍ, 2005.

NEGROPONTE, Nicholas. **A vida digital**, tradução de Sérgio Tellaroli, 2° Ed., São Paulo: Ed. Companhia das Letras, 2001.

PAESANI, Liliana Minardi. **Direito de informática: comercialização e desenvolvimento internacional do software**. São Paulo: Editora Atlas, 2007.

_____, Liliana Minardi. **O Direito na sociedade da informação II**. São Paulo: Editora Atlas, 2009.

_____. **Informática, Cyberlaw, E-Commerce. in Direito & Internet – Aspectos Jurídicos Relevantes**, obra coletiva, São Paulo: Edipro, 2000.

PAIVA, Mário. Informática: o futuro da justiça. **Revista Jurídica Consulex,** ano XI, n. 244, 15mar. 2007. Disponível em: http://jusvi.com/artigos/24940. Acesso em 31 mai 2013.

PASQUINO, Teresa. Serviços da sociedade de informação: Tutela dos dados pessoais e regras de conduta. in LUCCA, Newton; SIMÃO FILHO, Adalberto (coordenadores). **Direito e Internet, Vol. II**, Aspectos Jurídicos Relevantes, São Paulo: Editora Quartier Latin do Brasil, 2008.

PÉREZ LUÑO, Antonio-Enrique. **Cibernética, Informática y Derecho - Un análisis metodológico**, Bolonia: Publicação do Real Colégio de España, 1976.

_____. **Derechos Humanos, Estado de derecho y constitución.** Décima edición. Madrid, Espanha: Editorial Tecnos, 2010.

_____. Informática y libertad. comentario al articulo 18.4 de la Constitución española. **Revista de Estudios Políticos (Nueva Época)** nº. 24, Noviembre-Diciembre 1981.

_____. **Internet y los derechos humanos. Derecho y conocimiento,** vol. 2, pp. 101-121, ISSN 1578-8202, Facultad de Derecho. Universidad de Huelva Disponível em: http://www.uhu.es/derechoyconocimiento/DyC02/DYC002_A05.pdf. Acesso em 11 ago de 2013.

REVISTA VEJA. Disponível em http://veja.abril.com.br/noticia/internacional/camara-dos-eua-aprova-polemica-lei-de-ciberseguranca. Acesso em 12 Ago de 2013.

ROUSSEAU, Jean-Jacques. **Do contrato social.** Tradução: Rolando Roque da Silva. Edição eletrônica: Ed Ridendo Castigat Mores (www.jahr.org). Disponível em: http://www.dominiopublico.gov.br/download/texto/cv00014a.pdf. Acesso em: 07 set. 2013.

SANTOS, Manoel J. Pereira dos. Princípios para a formação de um regime de dados pessoais. in LUCCA, Newton; SIMÃO FILHO, Adalberto (coordenadores). **Direito e Internet, Vol.II, Aspectos Jurídicos Relevantes**, São Paulo: Editora Quartier Latin do Brasil, 2008.

SILVEIRA, Vladmir Oliveira da; ROCASOLANO, Maria Mendez. **Direitos Humanos: conceitos, significados e funções**. São Paulo: Saraiva, 2010.

TENÓRIO, Caio Miachon. Publicidade x direito à privacidade. In: SILVEIRA, Vladmir Oliveira da; MEZZAROBA, Orides (Coord.); MAILLART, Adriana S.; COUTO, Monica Bonetti Couto et al (org.). **Justiça e [o Paradigma da] Eficiência**. Coleção: Justiça, Empresa e Sustentabilidade [vol. 1]. São Paulo: Revista dos Tribunais, 2011, pp. 52-65.

UNIÃO EUROPÉIA. Directiva 95/46/ce do Parlamento Europeu e do Conselho. Fonte: Jornal Oficial nº L 281 de 23/11/1995 pp. 0031 – 0050. Disponível em: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:PT:HTML. Acesso: 11 ago de 2013.

_____. Directiva 2002/58/CE do Parlamento Europeu e do Conselho. Fonte: Jornal Oficial nº L 201 de 31/07/2002 pp. 0037 – 0047. Disponível em: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:PT:HTML. Acesso em 11 ago de 2013.

_____.Fonte: Jornal Oficial nº C 161 de 06/06/2013 p. 0060 – 0063. Disponível em: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2013:161:0060:01:PT:HTML. Acesso em: 11 ago de 2013.

Patricia Martinez Almeida
profa.civil@gmail.com

Advogada, professora titular de Direito Civil e Processo Civil da Universidade Nove de Julho, especialista em Direito Constitucional com ênfase em Direitos Humanos pelo Centro de Pós-Graduação UNINOVE, mestranda em Direito pelo Programa de Mestrado da Universidade Nove de Julho.

Vladmir Oliveira da Silveira
vladmir@aus.com.br

Mestre e Doutor em Direito pela Pontifícia Universidade Católica de São Paulo (PUC-SP). Pós-doutor em Direito pela Universidade Federal de Santa Catarina - (UFSC). Coordenador e Professor Permanente do Programa de Mestrado em Direito da UNINOVE, Diretor do Centro de Pesquisa em Direito da mesma instituição. Presidente do Conselho Nacional de Pesquisa e Pós-Graduação em Direito - CONPEDI.