A PROTEÇÃO DE DADOS PESSOAIS NOS ESTADOS UNIDOS, UNIÃO EUROPEIA E AMÉRICA DO SUL: INTEROPERABILIDADE COM A PROPOSTA DE MARCO NORMATIVO NO BRASIL.

DATA PROTECTION IN UNITED STATES, EUROPEAN UNION AND LATIN AMERICA: INTEROPERABILITY WITH THE BRAZILIAN LEGAL FRAMEWORK PROPOSAL.

Rafael Ferraz Vazquez

RESUMO:

As características da sociedade da informação modificaram o comportamento da sociedade, adaptando conceitos como o de privacidade a essa nova realidade. Hoje em dia, as ferramentas tecnológicas existentes possibilitam a captação, processamento, compartilhamento e armazenamento de dados, sejam eles pessoais ou não, a níveis até então inimagináveis. Uma vez que tais atos ocorrem de maneira independente das fronteiras geográficas, as legislações de proteção de dados devem ser compatíveis entre si, caso contrário poderão representar um obstáculo à utilização dos avanços tecnológicos. É nessa realidade que o Brasil inicia o debate do seu Marco Normativo de Proteção de Dados Pessoais e Privacidade. Tendo em vista inciativa para a criação de legislação inovadora no marco legal brasileiro, fundamental é a análise comparativa internacional com legislações de proteção de dados sobre a matéria, em especial na América Latina, Estados Unidos e União Europeia, esta última tida como fonte de inspiração do anteprojeto brasileiro. A não compatibilidade da futura legislação brasileira com aquelas pré-existentes poderia significar, na prática, uma importante desvantagem mercadológica para empresas localizadas no Brasil. Por outro lado, a ausência de um nível de proteção de dados satisfatório leva a uma ineficácia na proteção de direitos como os de privacidade e intimidade, garantidos pela Constituição Brasileira.

PALAVRAS-CHAVE: Privacidade; Proteção de Dados; Diretiva; União Europeia; América Latina; Brasil; Estados Unidos; Internet; Cloud Computing; Pervasive Computing; Constituição

ABSTRACT:

The features of the information society modified the society's behave, and with it concepts such as privacy had to be adapted to this new reality. Today, the technological tools enable the gathering, processing, sharing and storing of data, including personal data, not foreseeable

some years ago. Once such acts are undertaken independently of the geographical boundaries, data protection legislations should be interoperable, otherwise may be seen as an obstacle for the use of the technology breakthroughs. It is in this new reality that Brazil opened the debate of its Privacy and Data Protection Brazilian Legal Framework. In light of this debate to approve a new Brazilian bill, it is important to analyze relevant pre-existing legislation, namely in Latin America, United States and European Union, the latter used as a model to the proposed Brazilian bill. The lack of interoperability of the future Brazilian with those from other countries could meant, in practice, a less favorable situation for those companies located in Brazil. On the other side, the lack of a satisfactory level of data protection would represent inefficiency in the protection of privacy and intimacy rights, guaranteed by the Brazilian Constitution.

KEYWORDS: Privacy; Data Protection; Directive; European Union; Latin America; Brazil; United States; Internet; Cloud Computing; Pervasive Computing; Constitution.

1 INTRODUÇÃO

A era da sociedade da informação foi alcançada devido a grandes avanços tecnológicos, ocorridos especialmente nos últimos 20 anos. A informação está, atualmente, no centro das atenções das atividades econômico-sociais.

Resultado de tais avanços, a ferramenta da navegação em nuvem (*cloud computing*) se tornou um padrão mundial quando o assunto é Tecnologia da Informação (TI). Avanços como esse levaram ao aumento exponencial na quantidade de informações coletadas, trocadas e processadas. Nesse verdadeiro oceano de informações, parte relevante se refere a dados considerados pessoais.

Não é de espantar que, em uma realidade onde os dados podem ser transmitidos e armazenados independentemente das limitações geográficas, crescente é a preocupação com a proteção do direito fundamental da privacidade, bem como com a sua vertente mais recente:a proteção de dados pessoais.

Embora de maneira um pouco mais lenta à tecnologia, é crescente o número de países que buscaram regular a proteção de dados pessoais. Atualmente, cerca de 90 países já possuem legislações específicas sobre o assunto, incluindo-se alguns países da América Latina. (GREENLEAF, 2012)

No entanto, apesar do Brasil estar entre os principais mercados de Tecnologia da Informação (TI), não existe no país legislação específica sobre proteção de dados pessoais. Essa ausência já foi observada pelas autoridade brasileiras, levando à criação do Marco Normativo de Privacidade e Proteção de Dados pelo Ministério da Justiça o qual encontra-se atualmente em discussão (BRASIL, 2012).

A criação de uma lei de proteção de dados já é tida como altamente relevante para a efetiva proteção dos direitos fundamentais dos cidadãos. Por outro lado, em razão da onipresente tecnologia, uma lei que venha a impor limites ao uso, por exemplo da navegação em nuvem, poderá impor maior fardo àquelas empresas que atuam a nível global e deverão respeitar diversas legislações nacionais na matéria. Constante é o pedido de empresas multinacionais por harmonização de leis que regulem o uso de tecnologias, chamando a atenção para a questão da interoperabilidade e o custo resultante de tais leis.

Enquanto na União Europeia encontramos um certo grau de uniformidade, a situação provavelmente não será a mesma na América Latina. A existência de relevantes diferenças entre as legislações na América Latina pode levar à uma menor atratividade para empresas que queiram atuar nesses países. (ERNST & YOUNG, 2012)

Assim, diante da necessidade de proteger os dados pessoais no Brasil e, ao mesmo tempo, criar um sistema interoperável com outros sistemas jurídicos alienígenas, o presente artigo analisará as legislações pertinentes para o futuro esquema jurídico brasileiro: América Latina, Estados Unidos e União Europeia.

2 CONCEITOS: PRIVACIDADE E DADOS PESSOAIS

Questão fundamental é entender claramente o que se está tutelando quando se fala em proteção de dados pessoais. Muitas vezes visto como sinônimos, os conceitos de privacidade e proteção de dados são diferentes entre si. Nesse sentido, a definição de privacidade é mais ampla que proteção de dados. (FISHER e FERRAZ, 2011) Como definido outrora, privacidade e proteção de dados são “gêmeos mas não idênticos” (HERT e SCHEREUDERS, 2001). Dessa forma, embora distintos, proteção de dados pessoais seria uma das vertentes do direito à privacidade.

Sendo uma maneira de efetivar a proteção à privacidade, a legislação sobre proteção de dados fornece os meios para que os cidadãos tenham conhecimento e controle sobre a coleta e processamento daquelas informações que os identificam (“dados pessoais”),

possibilitando a limitação desse processamento a uma série de condições de segurança. (KUNER, 2009)

Com os recentes avanços, cada vez mais o conceito de proteção de dados pessoais vem ganhando um caráter independente do conceito de privacidade. (MAÑAS, 2010) Tanto é assim que já é normal os legisladores regularem o direito à proteção de dados de maneira independente do conceito "geral" de direito à intimidade e privacidade. Consequentemente, a evolução tecnológica levou os países a entenderem que o direito da autodeterminação sobre seus dados pessoais poderia ser desvinculado do direito à intimidade (LÓPEZ, 2003).

3 IMPORTÂNCIA DOS DADOS PESSOAIS

A crescente preocupação com a proteção de dados pessoais por parte dos legisladores é, em grande parte, justificada. De maneira resumida, pode-se dividir os dados pessoais em duas categorias, aqueles referentes à consumidores e os demais dados referentes à empregados, usuários de internet sem relação de consumo etc.

A coleta de dados sobre consumidores têm sido objeto de grande interesse por parte de diversas empresas, em especial para oferecer publicidade comportamental (*behavioral advertising*). No entanto, informações sobre os consumidores sempre foram consideradas valiosas pelo setor privado. Segundo Doneda (BRASIL, 2011):

> *"Os dados pessoais dos consumidores sempre foram atraentes para o mercado. Com dados precisos sobre os consumidores é possível, por exemplo, organizar um planejamento de produtos e vendas mais eficiente, ou mesmo uma publicidade voltada às reais características dos consumidores, entre diversas outras possibilidades. Há pouco tempo atrás, o custo para se obter tais dados pessoais costumava restringir severamente a quantidade destas informações que eram efetivamente coletadas e utilizadas."*

Para obter tais informações, inúmeras ferramentas inovadoras, serviços, produtos e objetos são, hoje me dia, capazes de coletar e compartilhar dados relacionados aos usuários e seu cotidiano. O uso das informações obtidas por tais meios é chamado de computação pervasiva (*pervasive computing*).

Pervasive computing nada mais é do que a integração no cotidiano das pessoas e no seu ambiente que as circundam, de ferramentas de comunicação capazes de coletar informações durante todo o seu uso. (REINO UNIDO, 2006). Tais ferramentas são largamente usadas, e úteis, no monitoramento de atividades, sistemas de transporte inteligentes etc.

Exemplo recente do *pervasive computing* foi a utilização, em hospitais brasileiros, de etiquetas inteligentes aplicadas em remédios, ferramentas e outros objetos para facilitar a administração do hospital e evitar furtos indesejados. Entretanto, seu uso também foi estendido à roupa dos médicos, de maneira a controlar o horário dos profissionais. (G1, 2012) Sem atentar para outras discussões, pergunta-se quais seriam as medidas de proteção adotadas na salvaguarda dessas informações?

No entanto, essas mesmas ferramentas altamente úteis podem gerar uma verdadeira sociedade vigilante, onde as pessoas possuem quase a totalidade de suas informações como localização, compras, amizades e padrões de comportamento passíveis de ser recompiladas em uma base de dados. Como é de se imaginar, a crescente proliferação de microprocessadores em aparelhos, objetos e até roupas, cria uma grande preocupação sobre a proteção de dados resultante dos mesmos (ALEMANHA, 2006).

Uma segunda categoria de dados relaciona-se com o público em geral (não consumidores). Tais dados são comumente utilizados no cotidiano das empresas dos mais diversos setores, todas usuárias de tecnologia. É o exemplo de base de dados contendo informações sobre funcionários de uma companhia, instituições com históricos de saúdo de pacientes, lista de passageiros de avião, informações bancárias e muitas outras informações. A realidade, inclusive no Brasil, é que muitos desses dados são armazenados de maneira descuidada, e cada vez mais comum é a contratação de serviços de armazenamento virtual (*cloud computing)* sem a consciência sobre as garantias e características dos mesmos. Não é a toa que cresce o número de incidentes com vazamento de informações pessoais contidas em tais bases de dados.

4 A PROTEÇÃO DE DADOS PESSOAIS NO ÂMBITO INTERNACIONAL

Como visto, os conceitos de proteção de dados e privacidade podem ser diferenciados. Enquanto os direitos à intimidade e privacidade foram objeto de discussão internacional há inúmeras décadas, foi somente na década de 80 que se iniciou a discussão internacional sobre a proteção de dados pessoais. Um grande marco nesse debate foi a publicação do *OECD International Guidelines*. Anteriormente a tal publicação, houve no mundo movimentos muito pontuais de debater sobre o assunto. Resultado desses debates resultaram em algumas legislações, tal como a Lei do Land alemão de Hesse (1970), a sueca *Data Legen* 289 (1973), o *Privacy Act* norte-americano (1974) e a francesa *Informatique et Libertées* (1978), esta

última criando inclusive uma autoridade pública de proteção de dados, a Comissão Nacional de Informática e Liberdades (CNIL). (BRASIL, 2010)

Em 1981, o Conselho da Europa aprovou a Convenção 108 sobre a proteção de dados pessoais em processos automatizados. Essa Convenção reforçou o debate sobre o assunto no território Europeu, culminando em 1995 na aprovação da Diretiva 46/95, um verdadeiro marco regulatório o qual inspira até hoje, mais de 15 anos depois, a quase totalidade das legislações existentes sobre a matéria.

Em 1990, a Assembleia Geral da Organização das Nações Unidas (ONU) aprovou suas diretrizes sobre a matéria, as quais seguiram os princípios trazidos tanto pelo documento elaborado pela OECD como a Convenção 108. No entanto, o trabalho desenvolvido pela ONU possuía um foco mais humanitário. No mesmo sentido, em 2011, a Assembleia Geral da ONU aprovou o documento preparado pelo *UN special rapporteur* Frank LaRue sobre liberdades de expressão e opinião. Em seu relatório, voltado para o ponto de vista humanitário, foi afirmado que há uma necessidade em melhorar a proteção mundial em matéria de dados pessoais.

5 O EXEMPLO EUROPEU E O SEU FUTURO (DIRETIVA EUROPEIA n.95/46)

Sem dúvida alguma, 17 anos depois de sua aprovação, a legislação europeia é o grande exemplo quando o assunto é proteção de dados pessoais. A Diretiva 95/46 (“Diretiva de Proteção de Dados” ou simplesmente “DPD”) estabeleceu uma verdadeira pedra fundamental na expansão de leis sobre proteção de dados. Isso porque a implementação da DPD pelos países membros da Comunidade Europeia (“países membros”) levou inúmeros outros países a seguirem o seu exemplo e legislarem sobre o assunto de maneira quase idêntica à europeia.

Uma grande motivação para se inspirar na DPD é a proibição geral (com exceções) de exportar dados pessoais da União Europeia à países fora do Espaço Econômico Europeu (“EEE”) caso o país destinatário dos dados não ofereça um nível de proteção de dados equivalente àquele Europeu. Consequentemente, de forma a qualificar como país apto a receber dados privados inúmeros países optaram por reproduzir em suas legislações àquelas existentes na DPD, facilitando assim a sua aprovação pela Comissão Europeia e consequente recebimento de dados pessoais sem a necessidade de requerer autorizações a cada transferências.

No caso de transferências de dados pessoais da Europa para países considerados não adequados, a DPD estabelece um sistema de registro e autorizações pelas autoridades de proteção de dados. Para tal autorização algumas ferramentas foram criadas no âmbito europeu. A primeira delas são os Códigos de Conduta ("*Binding Corporate Rules")*implementados por uma empresa ou setor. Tal código deverá ser levado a registro na autoridade de proteção de dados do estado membro europeu exportador dos dados. Tal código será avaliado do ponto de vista do nível de proteção de dados, garantias fornecidas, e o seu caráter vinculante. Uma vez aprovado, todas aquelas empresas as quais aderiram ao Código de Conduta poderão receber dados europeus sem a necessidade de aprovação a cada transferência.

Uma segunda alternativa é o chamado acordo de porto seguro, criado no ano 2000 para possibilitar a transferência de dados mais facilitada entre a União Europeia e Estados Unidos (também considerado como país não-adequado). Desde a sua criação, mais de 3.000 empresas já aderiram ao porto seguro, o qual é regulado em solo americano pelo Federal Trade Commission (FTC). Embora tenha sido uma solução para facilitar a imensa quantidade de dados trocados entre esses dois territórios, opinião recente (WP 196) do Grupo de Trabalho do artigo 29 (criado pela DPD), considerou que esse acordo de porto seguro americano não fornece as garantias exigidas pela DPD para o tratamento de dados pessoais, especialmente porque a adesão das empresas ao porto seguro americano se dá após a implementação de uma auto regulação. Essa auto regulação, segundo o Grupo de Trabalho, não fornece proteção suficiente aos dados pessoais.

A terceira e última alternativa, largamente utilizada, são as chamadas cláusulas modelo. Tais cláusulas, já em sua terceira versão, são estabelecidas por meio de uma decisão da Comissão Europeia e são um verdadeiro modelo do contrato que deve ser celebrado e depositado nas autoridades de proteção de dados para que seja permitida a exportação dos dados pessoais. A atual versão é de 2010, estabelecida pela Decisão da Comissão de 5 de fevereiro de 2010, notificada sob o número C(2010) 593.

5.1 Aspectos Relevantes da DPD.

Sendo reproduzida de maneira recorrente em legislações estrangeiras, válida é a análise de algumas previsões importantes trazidas na Diretiva 95/46. Em primeiro lugar, cabe ressaltar que, por se tratar de uma diretiva (e não um regulamento europeu), a mesma necessitou implementação interna nos diversos países membro da União Europeia. Portanto, a

mesma não é diretamente aplicável a nível nacional, embora sirva de base para as leis nacionais.

Um dos conceitos mais importantes trazidos na DPD é o de dados pessoais, definido pelo seu artigo 2º como:

> *"qualquer informação relativa a uma pessoa singular identificada ou identificável («pessoa em causa»); é considerado identificável todo aquele que possa ser identificado, directa ou indirectamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, econômica, cultural ou social."*

Interessante é a prática atual de algumas empresas, com vistas a evitar a incidência da lei de proteção de dados, criar processos para tornar os dados autônomos, removendo aquelas informações que possibilitariam uma identificação da pessoa. Ainda sobre a definição de dados trazida, alguns dados mereceram atenção especial, sendo categorizados como dados especiais ou sensíveis, sendo aquelas informações relacionadas à "*origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, bem como o tratamento de dados relativos à saúde e à vida sexual."* (Artigo 8º DPD)

Outro aspecto importante é o âmbito de aplicação da DPD, segundo seu artigo 3º aplicável em três hipóteses: (i) Quando o responsável pelo tratamento esteja domiciliado na Europa; (ii) quando a legislação europeia seja aplicável segundo as regras do Direito Internacional Público; e (iii) se os meios para tratamentos de dados pessoais esteja localizado em território da União Europeia. A DPD, portanto, é aplicável também a cidadãos estrangeiros, uma vez que a nacionalidade não influi nos critérios de aplicação da mesma. Tal independência da nacionalidade é resultado da vontade legislativa de, sempre que possível, aplicar a DPD aos dados pessoais, buscando proteger uma maior quantidade de dados pessoais. Pode-se afirmar, por conseguinte, que o seu escopo de aplicação é bastante amplo.

Um último aspecto, fundamental para entender a estrutura europeia de proteção de dados, é o esquema de fiscalização e punição pelo descumprimento das regras de proteção de dados. Cada estado membro europeu, segundo a DPD, deve possuir uma autoridade de controle com total independência nas suas funções, a qual terá competência para investigar, intervir (inclusive em ações judiciais) e punir. As sanções pelo descumprimento foram deixadas para serem definidas a nível nacional de cada país da União Europeia, e geralmente são divididas por grau de gravidade da infração.

5.2 A reforma da DPD.

Embora ainda seja o exemplo máximo a ser seguido, a DPD não está isenta de problemas. Mais recentemente, em razão dos constantes avanços tecnológicos, alguns aspectos da legislação acabaram tornando-se obsoletos. Nas palavras de Viviane Reding (2010), vice-presidente da Comissão Europeia: "*Novos riscos necessitam melhores soluções legais*". Exatamente por tal razão que, a partir de 2011, a Comissão Europeia, com o apoio do Parlamento Europeu, vem debatendo para não apenas reformar, mas substituir a DPD por um novo Regulamento Europeu de proteção de dados pessoais (de implementação direta nos estados membros).

Em resumo, seriam três as razões para a elaboração de um novo regulamento sobre proteção de dados (UNIÃO EUROPEIA, 2011):

(a) Importantes diferenças de implementação da Diretiva 95/46 (DPD) entre os diversos estados membros europeus, gerando heterogeneidade nas leis de proteção de dados dos países europeus;

(b) aumento inimaginável no volume de transferência de dados, superando em muito a quantidade de dados para a qual a DPD havia sido imaginada; e

(c) rápido avanço tecnológico testemunhado nos últimos anos.

Soma-se a tais razões, outras trazidas pela doutrina como merecedoras de reforma. Entretanto, esses seriam aspectos negativos da DPD desde a sua criação, e não unicamente em razão dos avanços tecnológicos. As principais críticas versam sobre (ROBINSON, 2012):

- Objetivos de determinadas obrigações bastante obscuros ;

- altamente burocrática, não havendo previsão sobre "o que" se deve cumprir mas apenas "como";

- utilização da legislação em proteção de dados como meio de estabelecer um rígido controle ao acesso e processamento de dados;

- âmbito de aplicação confuso;

- Regras de transferência de dados incompatíveis com o fluxo global de dados atual.

Dessa forma, embora tenha colaborada de maneira fundamental para a proteção de dados na Europa e mundo, a DPD poderia ser melhorada em diversos aspectos.

Na proposta inicial da Comissão Europeia, já é possível notar algumas diferenças relevantes entre a DPD e o Regulamento proposto. Por exemplo, o âmbito de incidência da

lei, previsto no atual artigo 4(1) DPD, possivelmente será modificado, aplicando-se o critério de "oferecimento de produtos e serviços a residentes da União Europeia ou o monitoramento de suas atividades."

Outro aspecto da DPD a ser reformado seria a transferência internacional de dados para países fora do Espaço Econômico Europeu. Essa transferência atualmente é vista como ineficiente e burocrática. No novo Regulamento, para que tal exportação de dados ocorra, uma das três hipóteses deveria ocorrer:

1. haja um consentimento por parte do sujeito das informações de maneira clara e informada;

2. em caso de transferência entre empresas coligadas, haja a apresentação e registro de Códigos de Conduta Vinculantes por parte das empresas receptoras dos dados.

3. que o país de destino tenha um nível de proteção adequado ao da União Europeia. Será considerado adequado, aqueles países os quais submetam as suas legislações nacionais para "aprovação" por parte da Comissão Europeia.

Muito embora a discussão sobre a substituição da Diretiva 95/46 esteja em fase inicial, a proposta inicial da Comissão Europeia responde a muitas preocupações, especialmente do setor privado. Isso porque as empresas serão aquelas responsáveis por seguirem as obrigações trazidas e por isso veem nas regras de proteção de dados um fardo para os seus negócios multinacionais.

6 Estados Unidos.

O sistema americano de proteção de dados privados é fundamentalmente distinto ao sistema europeu. Tendo a privacidade seu fundamento na quarta emenda da Constituição Americana, a mesma somente passou a tutelar dados privados, e não apenas privacidade de lugares físicos, a partir do caso *Katz vs. United States*, em 1967, decidido pela Suprema Corte daquele país.

No entanto, desde a década de 80, a quarta emenda já não era suficiente (ILANA, 2011) para proteger o direito à privacidade frente às novas tecnologias, havendo a necessidade de criação de outros instrumentos além da aplicação da quarta emenda pelos tribunais americanos. Tal necessidade, cada vez mais crescente, foi solucionada de maneira pontual, acabando por criar nos Estados Unidos um esquema de proteção de dados segmentado por setores, tipo de dados e até estado.

Nos Estados Unidos, muitas de suas leis relacionadas à proteção de dados foram criadas exatamente com o objetivo de preencher lacunas legislativas que ameaçavam o direito a privacidade (MCNEIL, 2011). Alguns exemplos são: *Tax Reform Act* (PL 94-455), *The National Education Statistics Act* (PL 103-382), *The Fair Credit Reporting Act* (90-321) e o *Electronic Communications Privacy Act* (PL 99-508).

A proteção a nível estadual, por sua vez, também se dividem em setores, e a competência estatal para regular o assunto emana da própria constituição estadual, a qual pode ir além da proteção conferida pela Constituição Americana. Exemplo dessa disparidade entre estados são a Califórnia e Nova Jérsei. Embora ambos estados americanos possuam uma proteção considerada avançada no país, os maiores avanços ocorridos em Nova Jérsei são oriundos de reiteradas decisões judiciais sobre direitos da constituição estadual, diferentemente do que ocorre no estado da Carolina, onde avanços cocorreram por meio de leis específicas (MCNEIL, 2011).

O regime setorial americano não foi tido como modelo para nenhum outro país. A maioria dos países estrangeiros buscam desenvolver uma estrutura jurídica unificada sobre o assunto ("lei omnibus"), oposta à legislação americana a qual é altamente fragmentada.

Apesar dos problemas apontados, noticia-se que o congresso americano é muito reticente em criar uma legislação federal única sobre proteção de dados (KOURFF, 2010). Como consequência direta dessa passividade, a *Federal Trade Commission* (FTC), entidade governamental que supervisiona o comércio nos Estados Unidos, acabou por incentivar a auto-regulação e o uso de tecnologias em benefício da proteção de dados.

Vale ressaltar que a FTC é também a entidade responsável em solo americano por gerenciar o porto seguro com a União Europeia, estabelecendo parâmetros e fiscalizando o cumprimento de garantias por parte das empresas americanas para que possam participar do porto seguro. Como mencionado, foi recentemente considerado pelo Grupo de Trabalho do Artigo 29 da DPD que tais empresas participantes do porto seguro não protegem eficazmente os dados privados.

Assim, é cada vez mais evidente que a legislação americana, além de confusa e esparsa, não fornece um nível de proteção suficiente. O próprio FTC, em Março de 2012, concluiu que o nível de proteção de dados nos Estados Unidos não era suficientemente seguro e sugeriu ao Congresso americano a aprovação de uma legislação única (*omnibus*) em matéria de proteção de dados (UNITED STATES, 2012)

Esse talvez seja o primeiro passo para a criação de uma estrutura jurídica americana uniforme sobre proteção de dados. No entanto, tal legislação é capaz de sofrer forte oposição dos setores privados, já acostumados à flexibilidade da auto-regulação. Por outro lado, as mesmas empresas poderiam beneficiar-se de uma lei clara sobre os limites e a responsabilidade com relação aos dados processados. Ao mesmo tempo, os cidadãos além de beneficiarem de uma maior proteção de dados, seriam capazes de entender quais são os seus direitos, o que atualmente não ocorre.

Ainda na análise feita pelo FTC, é possível encontrar algumas recomendações que são bastante semelhantes àquelas feitas pela Comissão Europeia:

- privacidade por defeito (*Privacy by default*);

- possibilitar uma escolha consciente dos consumidores sobre compartilhamento de dados (*Opt-out*);

- transparência na coleta de dados.

Como se observa, nos Estados Unidos também existe naquele país a necessidade de maior adequação dos níveis de proteção dos dados privados. A estrutura atual é tida como confusa e desatualizada com relação às novas tecnologias (O *Stored Communications Act*, por exemplo, data de 1986). Por outro lado, os perigos são constantes e o vazamento de informações privadas vem se tornado cada vez mais frequente. Atualmente, cidadãos trafegam e compartilham dados sem o mínimo de claridade sobre seus direitos. Como constatado pela Comissão Europeia (UNIÃO EUROPEIA, 2011), nem sempre a auto-regulação é suficiente. Nesse sentido, embora um modelo auto-regulatório seja altamente atrativo para o mercado, há de se imaginar que as empresas permitirão o máximo de liberdade de forma a não prejudicar seus negócios. (SILVA, 2010). Tal postura torna-se perigoso a partir do momento em que o processamento de dados pessoais passa a ser um modelo de negócio em si mesmo.

Dessa forma, embora grandes empresas de tecnologia sejam americanas, a regulação sobre proteção de dados não evoluiu naquele país. Como resultado, empresas atuantes naquele território se veem prejudicadas em razão da complexidade resultante das diferenças entre as legislações estaduais; a incerteza sobre a responsabilidade jurídica a nível nacional e; a nível internacional, por não ser considerada equipara à legislação europeia (e muitas outras inspiradas nela) e consequentemente sujeita a maior burocracia para o recebimento de dados pessoais.

7 América do Sul

Apesar do Brasil não possuir legislação específica sobre proteção de dados, outros países na América Latina já aprovaram legislações consideradas pela União Europeia como suficientemente garantidoras na proteção de dados pessoais.

Argentina e Uruguai, por exemplo, buscaram adequar-se à legislação europeia e assim, permitir o fluxo de dados entre tais países, beneficiando as empresas localizadas em seus territórios, atraindo investimento de multinacionais europeias, para as quais a transferência de dados sem burocracia é altamente importante.

Há a crescente tendência em aprovar legislações em matéria de proteção de dados seguindo o modelo da DPD. Este é o caso de Nicarágua, Costa Rica, Colômbia, Peru e México, os quais aprovaram leis sobre proteção de dados seguindo "o modelo europeu". Uma análise inicial de tais legislações mostra que uma chancela da União Europeia é tida como provável, visto que claramente foram inspiradas na DPD. Por outro lado, o Chile, apesar de ter aprovado sua legislação posteriormente à Diretiva 95/46, não forneceria suficientes garantias à proteção de dados.

7.1 Países Considerados com Nível Adequado de Proteção pela UE.

7.1.1 ARGENTINA.

A Argentina foi o primeiro país da América Latina a receber a aprovação europeia para receber dados pessoais, outorga ocorrida em 2002. A proteção de dados pessoais na Argentina deriva da sua Constituição e é regulamentada pela Lei nº 25.326 sobre proteção de dados pessoais (“LPDP”) e do Decreto Regulamentar nº 1558/2001 (“Decreto”).

Enquanto a Constituição prevê o instituto do *habeas data* (Artigo 43.3), a mesma também eleva à categoria de direito fundamental o direito à proteção de dados. Por sua vez, a LPDP estabelece direitos e deveres, cria os órgãos de supervisão de proteção de dados e estabelece sanções em caso de descumprimento.

Embora seja inspirada na legislação europeia, a LPDP possui algumas diferenças relevantes. Ao definir o que seriam dados pessoais, a LPDP define que são informações que identifica ou tornam identificável uma pessoa física ou jurídica. Houve, portanto, a inserção da proteção de pessoas jurídicas no escopo de proteção de dados pessoais, o que não ocorre na legislação europeia. (VARELA, 2006) Com relação ao escopo de incidência da lei argentina, a mesma também diferencia do “modelo europeu” pois enquanto o artigo 4 DPD basicamente

prevê a aplicação das leis europeias em caso da empresa responsável pelo tratamento se localizar naquele território ou quando houver o uso de equipamentos em solo europeu; a lei argentina prevê a aplicação de suas leis quando os dados versarem sobre residentes em solo argentino, sejam eles nacionais ou não. (DELPECH, 2004)

Tal qual na legislação europeia, há a proibição de exportação de dados para países que não possuam um nível de proteção equivalente ao argentino. No entanto, não existe na legislação argentina a previsão de se utilizar as chamadas "cláusulas modelo" trazidas na DPD (cláusulas contratuais que obrigatoriamente devem constar nos contratos para exportação de dados pessoais). Tais cláusulas, assim como os códigos de conduta, são bastante úteis para facilitar a obtenção de aprovação da autoridade nacional do país europeu na hora de exportar dados para países sem o nível de proteção equiparado. Os códigos de conduta estão previstos na legislação argentina, embora esteja limitado a ser realizado por associações representativas de responsáveis ou usuários de banco de dados pessoais. No entanto, notável é a ausência das cláusulas modelo, largamente utilizadas na Europa.

Cabe ressaltar que a atual lei argentina é uma versão menos rígida de um projeto de lei apresentado e altamente criticado durante a sua proposição. Tal projeto, Projeto de lei 24,745 acabou sendo rejeitado pelo executivo daquele país em razão do padrão considerado alto para a obtenção do consentimento para processamento de dados e o seu compartilhamento.

Embora com um nível de proteção menor que o originalmente proposto, a atual legislação argentina, embora com a ressalva de que haveria necessidade de aguardar a interpretação e efeitos ao longo dos anos, foi aprovada pela Comissão Europeia como fornecendo um nível de proteção equiparado ao Europeu (UNIÃO EUROPEIA, 2002) e, portanto, dados pessoais oriundos da União Europeia já poderiam ser transferidos para aquele país sem maiores restrições.

7.1.2 URUGUAI.

Seguindo o exemplo pioneiro da Argentina na América Latina, o Uruguai também passou pelo "crivo" da Comissão Europeia, sendo classificado a partir de 2010 como país com normas de proteção de dados adequada para receber dados da União Europeia. Como não podia ser diferente, sua legislação é bastante semelhante àquela europeia e, consequentemente, à Argentina.

A constituição uruguaia não prevê o direito à proteção de dados, mas possibilita a inclusão de outros direitos fundamentais por meio de legislação inferior, na forma dos artigos 72 e 332. Tal previsão, como direito fundamental, é trazida pelo artigo primeiro da lei 18,331 sobre proteção de dados e a ação de Habeas Data. Tal lei é regulamentada pelo decreto 414/2009, que em seu preâmbulo, expressamente faz referência à Diretiva 95/46/EU (DPD), afirmando ser conveniente ajustar-se a tal legislação de direito comparado a qual é mais aceita do ponto de vista internacional. Embora não encontremos de maneira expressa tal afirmativa em outras legislações, parece ser exatamente este o espírito dos legisladores ao criarem normas de proteção de dados, seja na América Latina ou não.

Com relação às previsões existentes na lei 18,331, apesar de inspirar-se na DPD, vemos que alguma diferenças são encontradas. A definição de dados pessoais, por exemplo, é parecida com aquela argentina, visto que incluem dados das pessoas jurídicas: "*informação de qualquer tipo referida a pessoas físicas ou jurídicas determinadas ou determináveis"*. De maneira análoga, também há a classificação especial para os chamados "dados sensíveis".

Outra semelhança encontrada é a vedação de exportação de dados a países sem um nível equiparado de proteção de dados. Ao contrário da vizinha Argentina, a legislação uruguaia prevê a utilização de cláusulas contratuais tipo para a obtenção de autorização. Tal previsão consta de somente uma frase, semelhante à rápida previsão encontrada também na DPD.

As demais semelhanças trazidas para o sistema uruguaio são a criação de uma autoridade de proteção de dados, os princípios norteadores, e a implementação de um sistema de fiscalização e punição administrativa nos casos de descumprimento.

Como era de se esperar, a legislação uruguaia possui diversas semelhanças com a DPD, no entanto é quase um espelho da legislação argentina sobre a matéria. Como esperado, o legislador uruguaio inovou em questões pontuais e manteve a estrutura encontrada na DPD.

7.2 Países Com Legislação De Proteção De Dados Sem Nível De Proteção Equiparado ao da União Europeia.

7.2.1 CHILE.

A Constituição chilena prevê em seu Artigo 19(4) o direito à vida privada. Em 1999, o Chile aprovou a Lei 19.628 referente à "Proteção da Vida Privada" e no ano seguinte o Decreto 779/2000 que a regulamenta. Apesar de ser posterior à DPD, não houve por parte do Chile nenhuma inspiração na legislação europeia, sendo ainda nos dias de hoje considerada

como “inadequada” desde o ponto de vista Europeu. Tal inadequação, em outras palavras, significa que dados privados demorarão até 7 meses para serem transferidos para o Chile, enquanto que para a Argentina, país considerado adequado pela Comissão Europeia, a mesma transferência demorará um dia (ARRIETA, [?]).

Entre as críticas à atual legislação chinela, a mais recorrente é aquela sobre o seu silêncio com relação a itens essenciais para uma lei de proteção de dados, tais como:

- princípio de finalidade, ou seja, a relação direta entre a coleta e a utilização dos dados;
- claridade sobre o responsável pelos dados privados;
- informação a ser dada para o processamento dos dados;
- sanções em caso de infração;
- previsão sobre uma autoridade de controle de proteção de dados.

Não é por acaso que a legislação chilena passou por um processo de consulta pública o qual resultou em um projeto de lei tramitando no congresso desde 2008. Como esperado, o modelo desde novo projeto é a DPD, incluindo os seguintes aspectos:

- A criação de uma autoridade de proteção de dados;
- Vedação à exportação de dados a países sem o nível equiparado de proteção;
- Definições semelhantes à DPD.

É esperado, portanto, que o Chile venha a se tornar mais um país a legislar de maneira semelhante à europeia em matéria de proteção de dados pessoais, alterando a sua legislação atual.

7.2.2 PERU.

Um dos últimos países sul-americanos a aprovar uma legislação sobre proteção de dados foi o Peru, em 2011. Agora, além dos artigos 2 e 200 da constituição peruana há a lei 29.733 sobre proteção de dados pessoais, bem como algumas normas setoriais sobre o assunto. Tal legislação ainda carece de regulamentação, mas é noticiado que a implementação desse novo marco jurídico será fruto de uma cooperação direta com a agência de proteção de dados espanhola, AEPD.

Vale notar que tal esforço legislativo peruano não veio por acaso, mas sim em razão de compromissos internacionais firmados pelo Peru onde se exigia um esforço na proteção de dados. É o exemplo dos Acordos de Livre Comércio (ALC) com Canadá, União Europeia e a participação peruana no *Asian-Pacific Economic Cooperation* (APEC).

Com relação ao conteúdo da lei, a mesma já sofreu críticas de empresas de tecnologia, em especial com relação à falta de segurança jurídica oriunda de conceitos vagos e imprecisos. No entanto, não se nota grande diferença entre as definições da lei peruana e aquelas da Diretiva 95/46, embora seja perceptível a ausência de um detalhamento existente na DPD. Como exemplo, dados pessoais são definidos como aqueles que "identificam ou possam identificar", mas a DPD vai um pouco além, trazendo também uma lista de informações consideradas pessoais.

Outras semelhanças entre ambas as legislações são a criação de uma autoridade nacional de proteção de dados (Art. 32), a previsão da utilização de códigos de conduta (*Binding Corporate Rules*) por parte de empresas (Art. 31), o estabelecimento de níveis diferenciados de infrações (Art. 38) bem como os princípios aplicados à proteção de dados (Art. 4 a 11). Não houve, entretanto, menção expressa sobre as cláusulas-modelo mas deixou a possibilidade de previsão regulamentar sobre outras maneiras de exportação dos dados, desde que de observados os princípios norteadores da lei.

Como dito, tal lei ainda é carente de regulação inferior, o qual poderá não apenas esclarecer alguns conceitos trazidos pela lei 29.733 como também exercer papel fundamental na implementação de uma sistemática benéfica para aquelas empresas que lidam com dados privados.

7.2.3 MÉXICO.

De maneira igualmente recente, o decreto aprovando a Lei de Proteção de Dados Pessoais foi publicado em 5 de julho de 2010, e o seu correspondente regulamento em dezembro de 2011. A implementação de um esquema de proteção de dados privados passou, inclusive, por uma reforma constitucional, a qual incluiu a proteção de dados privados como um direito expressamente reconhecido por lei (artigo 6 e 16) bem como atribuindo competência ao congresso para legislar sobre o assunto (artigo 73).

Uma inovação criada pela legislação mexicana é a divisão dos dados pessoais em três categorias diferentes: patrimoniais, financeiros e sensíveis. Embora alardeado como inovação única, a própria legislação europeia, como visto, reserva atenção especial a determinados dados atribuindo-lhes caráter especial, são eles raça, sexo, opiniões políticas e outras elencadas no artigo 8 da Diretiva 95/46/EU. Tal divisão foi inclusive seguida por diversos países tal como Peru, Argentina e Uruguai.

A inspiração europeia também é uma constante na lei mexicana e está refletida na legislação mexicana de maneira clara nos seguintes aspectos: Existência de uma autoridade supervisora, definições utilizadas, sistema de infrações e a exigência de cumprimento de normas específicas para que seja possível exportar os dados. Com relação à definição de dados sensíveis, o legislador mexicano também inovou, classificando como dados sensíveis "aqueles dados pessoais que afetem a esfera mais íntima de seu titular."

Embora seu regulamento seja muito recente, a semelhança com a diretiva europeia e com as legislações argentinas e uruguaias levam a crer que o esquema legal mexicano seja considerado como suficientemente garantidor e assim, apto a receber dados da União Europeia.

7.2.4 COLÔMBIA.

Seguindo a tendência mundial, a Colômbia também aprovou uma legislação sobre proteção de dados pessoais. A nova legislação, segundo as normas constitucionais daquele país, deve ser aprovada pela corte constitucional. Tal aprovação é aguardada desde 2008.

A lei estatutária de proteção de dados colombiana, aprovada pelo congresso em 2007, também reflete o modelo da DPD. Em especial, semelhanças existem com relação à classificação de dados pessoais, a proibição de exportar dados a países sem o nível de proteção adequado, o estabelecimento de uma autoridade de proteção de dados (no caso será a própria Superintendência de Indústria e Comércio) e a previsão de sanções pelo descumprimento de normas de proteção de dados.

7.2.5 BRASIL.

Como já afirmado, o Brasil não possui uma lei específica de proteção de dados pessoais. Com relação à privacidade, a Constituição Federal Brasileira (CF) protege o direito à intimidade em seu artigo 5º inciso X, e o *habeas data* no inciso LXXII do mesmo artigo 5º. O Código Civil Brasileiro também prevê o direito à privacidade e o Código de Defesa do Consumidor traz, ainda que de forma muito breve, previsão sobre a necessidade de consentimento para coleta de dados do consumidor. Esse é, de forma bastante resumida, o esquema jurídico existente me matéria de proteção de dados.

Consequentemente, o ordenamento jurídico brasileiro não poderia ser considerado como suficientemente garantidor dos dados pessoais, diferentemente das leis de países como Argentina e Uruguai. Na prática, isso significa dizer que empresas localizadas no Brasil, e que importem dados da União Europeia, deverão receber a aprovação da autoridade de proteção

de dados do estado membro de origem dos dados. Para receber tal autorização, uma série de garantias vinculantes deverão ser fornecidas e depositadas na autoridade de proteção de dados.

Em especial, a empresa brasileira que deseja importar dados pessoais, deverá celebrar um contrato contendo a última versão das "cláusulas modelo", prevista pela Diretiva 46/95. Outra opção é a adoça de códigos de conduta empresariais (*binding corporate rules*) para que uma mesma empresa com presença nos dois territórios possa transferir dados pessoais entre as suas diversas sedes.

7.2.5.1 Marco Normativo da Privacidade e da Proteção de Dados no Brasil

Havendo uma clara necessidade de regular melhor a proteção de dados pessoais, o Ministério da Justiça iniciou a discussão sobre o tema publicando a proposta de “Marco normativo da privacidade e da proteção de dados pessoais no Brasil”. Como era de se esperar, o diálogo até o momento é altamente influenciado pela Diretiva 95/46 (DPD). As discussões atuais necessitam de uma maturidade maior, pois a criação de legislação nacional pode resultar em uma “importação” de aspectos que, embora existentes em outras leis, poderiam claramente ser melhor regulamentadas. Nesse sentido, é interessante notar que a proteção de dados relaciona-se com setores altamente tecnológicos, isto é, sujeito a evoluções frequentes. A própria Comissão Europeia, com relação à DPD já reconheceu defeitos existentes na DPD bem como a defasagem com relação aos avanços tecnológicos.

Sendo influenciado pela DPD, o anteprojeto traz conceito de dados pessoais idêntico àquele encontrado na DPD ("informação relativa a uma pessoa identificada ou identificável"), sendo também idêntica a categorização de certos dados como sensíveis. Outras semelhanças são a criação de uma autoridade de proteção de dados, nomeada como Autoridade de Garantia, a criação de códigos de boas práticas e a vedação da transferência de dados pessoais para países estrangeiros que não dispuserem de um nível de proteção adequado.

Sendo um anteprojeto, o mesmo sofrerá inúmeras modificações até a proposta a ser encaminhada ao congresso nacional. No entanto, cabe ressaltar que é inexistente no atual anteprojeto, menção sobre as cláusulas modelo. Tal ausência pode haver ocorrido pela atenção dada ao texto da DPD em si, e não pela sua aplicação prática ou recomendações de reforma feitas no âmbito europeu. Por outro lado, os códigos de boa-prática estão presentes no anteprojeto, de maneira bastante semelhante à DPD.

À luz da proposta inicial, é possível perceber que foram transpostos para o anteprojeto alguns dos problemas que levaram à proposta de reforma da diretiva europeia de proteção de dados. Entre os aspectos principais, é possível destacar que o anteprojeto possui o mesmo defeito encontrado na DPD, isto é, uma legislação que busca informar o "como fazer" e não qual o padrão a ser alcançado. Também não houve menção às clausulas contratuais modelo para a transferência internacional de dados, altamente importantes no âmbito de aplicação da DPD.

Vale ressaltar que esses dois aspectos constam na pauta principal da reforma da diretiva europeia e, uma vez que o anteprojeto brasileiro está claramente inspirado em tal diretiva, maior atenção deveria ser dada aos problemas existentes naquela legislação, existente há mais de 15 anos.

7.2.5.2 Marco Civil da Internet.

Outra iniciativa, em estágio avançado de discussão, é o Marco Normativo da Internet (Projeto de Lei 2.126/11). Tal projeto objetiva estabelecer "princípios, garantias, direitos e deveres para o uso da Internet no Brasil". Diversos aspectos, tal como neutralidade em rede, a responsabilidade dos provedores de internet como também a proteção de dados no ambiente virtual são tratados nesse marco normativo.

No projeto atual, está previsto que o usuário de internet tem direito à proteção de seus dados, devendo, por exemplo, constar expressamente cláusula a esse respeito em contratos celebrados pela internet. O projeto também prevê a vedação ao monitoramento dos dados pelo fornecedor de acesso à internet, dados estes altamente valiosos no emprego de publicidade comportamental.

Tal legislação é bastante limitada em matéria de proteção de dados, o que é uma escolha feliz de forma a evitar uma segmentação do assunto por diversas normas, o que tornaria o esquema jurídico complexo.

8 CONCLUSÃO

As novas tecnologias influenciaram conceitos como o de privacidade da sociedade atual. Informações que alguns anos atrás eram considerados de cunho pessoal, hoje em dia são compartilhadas online com milhares de pessoas, e pelos próprios indivíduos. Esses avanços acabaram por culminar na discussão de um aspecto específico da privacidade: a proteção de dados pessoais.

A sociedade da informação é cada vez mais global. E de maneira análoga é o funcionamento empresarial, existindo o mercado único global. Soluções tecnológicas fornecidas para empresas praticamente ignoram os limites geográficos, estabelecendo uma troca de informações em tempo real e independente do país ou continente.

No entanto, as leis continuam circunscritas aos territórios. Com a crescente atenção dada à proteção de dados pessoais, um potencial conflito entre tecnologia e leis de proteção de dados poderá frear a aplicação de diversos avanços em alguns territórios. Enquanto legisladores e cidadãos chamam a atenção para maiores garantias em matéria de proteção de dados, o setor privado demonstra preocupação com o custo de implementação prática de leis nacionais concomitantes a uma mesma atividade. Como resultado, recorrente é a chamada para a criação de sistemas de auto-regulação ou, pelo menos, de estruturas jurídicas compatíveis entre si e de fácil observância e respeito.

Atualmente, dois movimentos principais ocorrem com relação à regulamentação da proteção de dados. Um primeiro movimento é a criação de normas até então inexistentes em determinados países. O segundo é a reforma da estrutura jurídica existente, a qual já regulava a matéria em âmbito nacional ou regional.

Enquanto a reforma é discutida em territórios como Chile, Estados Unidos e União Europeia, países como Angola, México, Colômbia, Nova Zelândia e Coréia do Sul aprovaram leis nacionais de proteção de dados, todas tendo utilizado como base o modelo europeu.

O Brasil despertou, de maneira tardia, para a necessidade de implementação de uma lei de proteção de dados pessoais. Seguindo a tendência atual, a primeira proposta do Marco Normativo de Proteção de Dados e Privacidade tem como base a legislação europeia.

No entanto, e considerando que a própria Diretiva 95/46/EU encontra-se em um processo de reforma, tal fato deveria ser levado em conta. A utilização, de maneira quase fiel, de um modelo que, embora bem-sucedido, possui mais de 15 anos, poderá transpor no âmbito nacional inúmeros problemas já identificados nas legislações estrangeiras.

Além de se atentar para o modelo utilizado, outras questões são de fundamental relevância na discussão do anteprojeto de lei brasileiro. Entre tais questões está a compatibilidade com legislações vizinhas pré-existentes e os custos para o setor privado, responsável por cumprir não apenas com as obrigações a serem estabelecidas pelo legislador brasileiro, mas sim de diversos países devido ao chamado mercado único global.

Apesar das inúmeras questões a serem consideradas na criação de uma lei de proteção de dados pessoais, a sua ausência também é altamente prejudicial. Isso porque, além de não proteger eficazmente direitos constitucionais, a ausência de uma legislação impõe às empresas localizadas em território nacional processos burocráticos para que possam receber dados pessoais de países os quais já implementaram o modelo europeu de proteção de dados.

9 REFERÊNCIAS.

[?]. FTC Issues Final Report for Best Practices for Privacy Protection. Current Developments. *The Computer & Internet Lawyer*, v.29 n.6, Junho, 2012.

ALEMANHA. Bundesamt für Sicherheit in der Informationstechnik. *Pervasive computing : trends and impacts*. Federal Office for Information Security. Ingelheim : SecuMedia, 2006.

ARRIETA, R. (?) Chile y la protección de datos personales: Compromisos internacionales. *Expansiva UDP*. [?]

BRADSHAW, S.*et al.* Contract for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1662374>. Acesso em 15 de maio de 2012.

BRASIL. A proteção de dados pessoais nas relações de consumo: para além da informação credíticia. *Escola Nacional de Defesa do Consumidor*; coord. Danilo Doneda. Brasília: SDE/DPDC, 2010.

_____. Disponível em <http://www.governoeletronico.gov.br/noticias-e-eventos/noticias/governo-e-sociedade-discutem-anteprojeto-de-lei-sobre-protecao-de-dados-pessoais> Acessado em: 20/05/2012.

BUSINESS SOFTWARE ALLIANCE. BSA Global Cloud Computing Scorecard: A Blueprint for Economic Opportunity. Disponível em: <http://portal.bsa.org/cloudscorecard2012/assets/PDFs/BSA_GlobalCloudScorecard.pdf>. Acesso em: 15 de julho de 2012.

CARNEIRO, Rodrigo Borges *et al,* As informações pessoais em banco de dados e sua utilização em ações de marketing na internet, *Revista da Associação Brasileira de Propriedade Intelectual,* n.49, Rio de Janeiro, 2000.

DELPECH, Horácio Fernández. *Internet: su problemática jurídica*. 2. ed. Buenos Aires: Abeledo-Perrot, 2004.

EFING, A.C. GIBRAN, F. M. Banco de dados de consume como instrument para o Desenvolvimento da sociedade da informação. *Anais do XIX Encontro Nacional do CONPEDI realizado em Fortaleza - CE nos dias 09, 10, 11 e 12 de Junho de 2010*.

ESTADOS UNIDOS. FTC. *(2012). Protecting Consumer Privacy in an Era of Rapid Change: Recommendation For Businesses and Policymakers.* 2012.

FISCHER, P. FERRAZ VAZQUEZ, R.. Data transfer from Germany or Spain to third countries – Questions of civil liability for privacy rights infringement. *In* Cerrillo, A., Peguera, M., Peña, I.,Vilasau, M. (ed.)."Net Neutrality and other challenges for the future of the Internet*". Anais do 7th International Conference on Internet, Law & Politics*. Barcelona: Universitat Oberta de Catalunya, 11-12 July 2011. pp.311-340.

FISCHER, P. FERRAZ VAZQUEZ, R. "Online entertainment in cloud computing surroundings" *In* Cerrillo, A., Peguera, M., Peña, I.,Vilasau, M. (ed.)."Challenges and Opportunities of Online Entertainment *". Anais do 8th International Conference on Internet, Law & Politics*. Barcelona: Universitat Oberta de Catalunya, 09-10 July 2012. pp.329-357.

G1. Instalação de chip em jaleco de médicos gera polêmica no RJ. Disponível em: <http://g1.globo.com/rio-de-janeiro/noticia/2012/07/instalacao-de-chip-em-jaleco-de-medicos-gera-polemica-no-rj.html>. Acesso em: 21 de junho de 2012.

GILBERT, Francoise. EU Data Protection Overhaul: New Draft Regulation, *The Computer & Internet Lawyer*, v.29, n.3, Março 2012.

GREENLEAF, Graham. Global data privacy laws: 89 countries, and accelerating. *Privacy Laws & Business International Report*, Issue 115, Special Supplement, February 2012; Queen Mary School of Law Legal Studies Research Paper No. 98/2012. Disponível em: <SSRN: http://ssrn.com/abstract=200003>. Acesso em: 15 de julho de 2012.

HERT, Paul; SCHEREUDERS, Eric."*The Relevance of Convention 108. European Conference on Data Protection on Council of Europe Convention 108 for the protection of individuals with regard to automatic processing of personal data: present and future*". The Council of Europe (ed.) Reports of Data Protection Conference, p. 63-76, 2001.

KATTAN, Ilana. Cloud Privacy Protections: Why the Stored Communications Act Fails to Protect the Privacy of Communications Stored in the Cloud. *Vanderbilt J. of Ent. And Tech. Law.* Vol. 13(3) 617- 656, 2011.

KORFF, Douwe (ed.) *Comparative Study on Different Approaches to new Privacy Challenges, in particular in light of technological developments – Country studies*. Bruxelas: Comissão Europeia, 2010.

KUNER, Christopher. "*An international legal framework for data protection*", Computer Law & Security Review, v.25, 307- 317 pp., 2009.

_____. The European Commission's Proposed Data Protection Regulation:A Copernican Revolution in European Data Protection Law. *Bloomberg BNA: Privacy and Security Law Report*, v.11, 2012.

MAÑAS, José Luis Piñar (dir.), *El derecho fundamental a la protección de datos personales (LOPD): Protección de datos de carácter personal en Iberoamérica*. Valencia: Tirant Lo Blanch, 2005, pp. 19-36.

MCNEIL, Sonia. Privacy and the Modern Grid. *Harvard Journal of Law & Technology.*V.25 n.1, 2011.

MIRALLES, Ramón. Cloud Computing y protección de datos. *Revista de Internet, Derecho y Política,* n.11, 2010.

MOEREL, Lokke. Back to basics: when does EU data protection law apply. *International Data Privacy Law,* v.1 n.2, 2011.

OECD. *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Disponível em: <http://www.oecd.org/document/18/0,3746,en_2649_34223_1815186_1_1_1_1,00.html>. Acesso em: 20 de julho de 2012.

PERU. Peru se prepara para la proteccion de datos personales. Disponível em: <http://www.minjus.gob.pe/noticias/11-10-2011/peru-se-prepara-para-la-proteccion-de-datos-personales>. Acesso em: 20 de julho de 2012.

REDING, Viviane. *Privacy matters – Why the EU needs new personal data protection rules*. SPEECH/10/700. 2010.

REINO UNIDO, Parliamentary Office of Science and Technology. *Postnote*. N. 263, 2006.

ROBINSON, N. et al. (2012) *Review of the EU Data Protection Directive*. Disponível em: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/review_of_eu_dp_directive_summary.pdf. Acessado em 3 de Abril de 2012.

SILAVA, Rosane Leal. As tecnologias da informação e comunicação e a proteção de dados pessoais. *XIX Encontro Nacional do CONPEDI realizado em Fortaleza – CE nos dias 09, 11, 12 de Junho de 2010.*

SILVA NETO, A. M. *Privacidade na Internet: um enfoque jurídico*, São Paulo: Edipro, 2001.

UNIÃO EUROPEIA. Grupo de Trabalho do Artigo 29. Parecer nº 4/2002 sobre o nível de protecção dos dados pessoais na Argentina. Disponível em: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp63_pt.pdf. Acesso em: 05 de março de 2012.

_____. European Commission. *A comprehensive approach on personal data protection*. 2011

UNITED NATIONS. General Assembly, Human Rights Council, 17th Session. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression Frank La Rue. May 16, 2011. A/HRC/17/27.

VARELA, E. B. et al. The Right Of Privacy And Its Development In Argentina And Other Latin American Countries Vis-A-Vis New Technologies And Commercial Traffic Requirements, *Associação Brasileira de Direito de Informática e Telecomunicações* –ABDI, 2006.