

A PROTEÇÃO DE DADOS PESSOAIS NA INTERNET NO BRASIL: ANÁLISE DE DECISÕES PROFERIDAS PELO SUPREMO TRIBUNAL FEDERAL

PROTECTION OF PERSONAL DATA ON INTERNET IN BRAZIL: ANALYSIS OF THE SUPREME COURT JUDGEMENTS

Francieli Puntel Raminelli*

Letícia Bodanese Rodegheri**

RESUMO: As Tecnologias de Informação e Comunicação (TIC) estão cada vez mais inseridas no cotidiano dos indivíduos sendo, muitas vezes, ignorado o seu potencial ofensivo. Isso se mostra factível quando se trata da proteção de dados pessoais, que, se mal empregados, podem ser comercializados e causarem danos aos titulares. A União Europeia possui inúmeras diretrizes para a regulamentação do tema, as quais foram seguidas por outros países como, por exemplo, a Argentina. No Brasil, apesar da edição da Lei n.º 12.965, de 2014, ainda restam muitas questões não regulamentadas, cuja solução fica a cargo do Poder Judiciário, que as soluciona de acordo com o ordenamento jurídico existente no país. O presente trabalho objetiva, utilizando-se do método de abordagem dedutivo, apresentar o tema em sua perspectiva teórica, analisar a lei Argentina existente, como um marco referencial e, ao final, examinar o tratamento da matéria no Brasil, por meio de algumas decisões proferidas pelo Supremo Tribunal Federal. Para tanto, também foi empregado o método de procedimento monográfico (estudo de caso) juntamente com a técnica de pesquisa documental. Conclui-se ser necessária e emergencial a regulamentação da proteção aos dados pessoais no Brasil, devendo ser utilizadas as diretrizes já existentes em outros países como parâmetros.

PALAVRAS-CHAVE: Proteção de dados pessoais. Direito à Intimidade. Direito à Privacidade. Lei Argentina de Proteção de Dados. Jurisprudência do Supremo Tribunal Federal.

SUMÁRIO: Introdução. 1 A Tutela da Intimidade e dos Dados Pessoais na Internet. 2 A Proteção dos Dados Pessoais na América Latina: a Experiência Argentina. 3 O Tratamento dos Dados Pessoais no Brasil: Casos Concretos. Considerações Finais. Referências.

ABSTRACT: The Information and Communication Technologies (ICT) are increasingly embedded in daily life, but their offensive potential is often ignored. When the protection of personal data fails, the information can be commercialized and cause damage to the users. The European Union has numerous guidelines for the regulation of the subject, which were followed by other countries, such as Argentina. In Brazil, despite the enactment of the Law n.º 12.965/2014, there are still many unregulated issues, which are solved only through litigation, in accordance with the existing legal system in the country. Through a deductive method of approach, this research aims to present the theme in its theoretical perspective, analyzing the existing law in Argentina and examining the legal treatment in Brazil, with especial attention to Supreme Court decisions. In this intention, a study case method and a documental technique of research were adopted. The conclusion is that it is necessary to regulate the protection of personal data in Brazil, embracing the guidelines of other countries as parameters.

KEYWORDS: Protection of personal data. Right to Privacy. Argentinean Law on Data Protection. Supreme Court Judgments.

89

INTRODUÇÃO

* Mestre em Direito pela Universidade Federal de Santa Maria (UFSM), Rio Grande do Sul, com período de pesquisa e atuação com professora convidada na Universidade de Sevilla, Espanha. Professora da Faculdade de Direito da Universidade Federal de Santa Maria (UFSM) e da Faculdade de Direito de Santa Maria (FADISMA). Membro do Centro de Estudos e Pesquisa em Direito e Internet, registrado no Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq).

** Mestre em Direito pela Universidade Federal de Santa Maria (UFSM), Rio Grande do Sul.

A utilização das Tecnologias da Informação e Comunicação (TIC) impactam nas mais variadas searas da vida humana. Há a possibilidade de comunicação instantânea – texto, áudio e vídeo –, de recebimento e busca por informações, compras eletrônicas, emissão de documentos, entre outros. No entanto, na mesma medida em que as TIC favorecem que uma infinidade de ações seja realizada por meio da Internet, emergem conflitos e violações de direitos fundamentais, que requerem uma solução do Direito.

Por mais recente que sejam as inovações trazidas pela utilização da Internet, não se pode desconsiderar a criação de um ambiente em que há, em regra, ampla liberdade de expressão, rapidez na troca de informações e transposição de barreiras territoriais e temporais. Diante de características peculiares e totalmente diferentes daquelas com as quais o sistema jurídico estava habituado a interferir, tem-se visualizado a necessidade de edição de legislação específica para tutelar os direitos relacionados a esta utilização.

Verifica-se que as TIC influenciam diretamente na seara jurídica, de forma que a sua utilização apresenta impactos nas mais variadas áreas do Direito, dando-se destaque, no presente trabalho, à tutela de direitos fundamentais.

A grande questão a ser enfrentada consiste em verificar que a regulamentação da proteção à privacidade e, em específico, dos dados pessoais, já existe em vários países europeus – pioneiros na abordagem do assunto – e, também, na Argentina. Esse país da América Latina, vizinho do Brasil, há mais de quinze anos regulamentou a questão, já tendo, inclusive, recebido um certificado de segurança no tratamento de dados pessoais pela União Europeia. No Brasil, apesar da promulgação da Lei n.º 12.965/2014, que institui o Marco Civil na Internet e aponta a proteção de dados do usuário perante provedores, não existe uma legislação vigente acerca da proteção de dados pessoais, sendo que, apenas no ano de 2016, o anteprojeto de proteção de dados pessoais foi encaminhado à Câmara dos Deputados.

Diante deste cenário, o presente trabalho objetiva, utilizando-se do método de abordagem dedutivo, averiguar a proteção dos dados pessoais existente na Argentina para, em um segundo momento, examinar o tratamento que vem sendo conferido no Brasil, por meio de decisões proferidas pelo Supremo Tribunal Federal. Para a observação junto ao *site* do Supremo Tribunal Federal, empregou-se a técnica de pesquisa documental e o método de procedimento monográfico, sendo que a pesquisa versou sobre a existência de julgados contendo as seguintes palavras: “privacidade” e “internet”.

O artigo foi dividido em três tópicos centrais. Na primeira parte, abordou-se o direito à intimidade e à vida privada que, em um primeiro momento foi tratado como o “direito a estar só” e, posteriormente, como um direito de exigir prestações concretas do Estado, a exemplo do conhecimento, correção e determinação do uso das informações e dados pessoais. Na sequência, a análise centrou-se na legislação da Argentina, no que concerne à proteção de dados pessoais, presente na Lei nº 25.326 de 2000. E, por fim, o objeto de estudo recaiu sobre a realidade brasileira, por meio de casos práticos que demonstram como as lides relacionadas à proteção dos dados pessoais na Internet vêm sendo decididas no país.

1 A TUTELA DA INTIMIDADE E DOS DADOS PESSOAIS NA INTERNET

Atualmente, pode-se afirmar que se vive em uma Sociedade da Informação, fundamentalmente ligada à utilização das Tecnologias de Informação e Comunicação (TIC), conhecidas como o computador, o acesso à Internet, os telefones móveis, a televisão interativa, entre outros. Trata-se de uma época em que as pessoas detêm a capacidade de firmar um contato direto com uma “[...] gama crescente de dados consultados diretamente, o que lhes conferiu maior autonomia de escolha, pois a informática permitiu digitalizar as informações, armazená-las, tratá-las automaticamente, transportá-las e colocá-las à disposição do usuário final, o que antes não acontecia” (SILVA, 2010, p. 3907).

As TIC permitem que uma infinidade de informações e dados sejam lançados e difundidos na *web*, justamente por caracterizar-se como um ambiente em que qualquer pessoa pode, independentemente de barreiras temporais ou territoriais, nela expressar opiniões, comentários, críticas e, também, inserir dados pessoais. Trata-se de uma das principais características do meio, qual seja, a liberação da emissão, pois permitem a qualquer pessoa “[...] *consumir, produzir e distribuir informação* sob qualquer formato em tempo real e para qualquer lugar do mundo sem ter de movimentar grandes volumes financeiros ou ter de pedir concessão a quem quer que seja” (LEMOS; LÉVY, 2010, p. 25, grifo do autor).

A questão também pode ser abordada sob a perspectiva da existência de um “superinformacionismo”, caracterizado como a grande quantidade de informações que circulam na Internet, “sobre tudo e sobre todos”. Neste sentido, os cibernautas utilizam-se da rapidez com que as informações são transmitidas, da ampla liberdade (em regra não há filtros prévios à publicação) e do fácil acesso, pois é suficiente um computador com acesso à

Internet para que várias opções, matérias e argumentos sejam conhecidos e debatidos por uma infinidade de cidadãos.

A Internet constitui-se em um espaço aberto e propício ao fomento de debates relativos a temáticas outrora discutidas apenas de forma presencial. Assuntos como política, economia, relações sociais, liberdade, democracia, entre outros, estão em constante discussão no meio. Ao publicar conteúdo na *web*, o cibernauta não somente opta pelo assunto de seu interesse e emite uma opinião ou crítica, como também engaja e movimenta outros cidadãos na defesa de interesses e escolhas que, muitas vezes, apresentam reflexos fora da Internet.

A quantidade de informações disponível na *web* também se mostra como outra vantagem para os internautas, pois podem valer-se das notícias mais interessantes sobre um determinado assunto, selecioná-las, debatê-las e até mesmo contestá-las, criando um ambiente de discussão sobre o tema que acharem mais conveniente em relação ao meio ambiente.

No entanto, o grande desafio que se coloca à frente dos cidadãos é o controle dos dados pessoais que pode ser feito por empresas ou, até mesmo, pelos governos. Há possibilidade de verificação, por meio de um monitoramento *online*, de preferências artísticas, musicais, hábitos de vida, de viagens, operações financeiras, orientação sexual, crenças religiosas, entre outros. Pérez Luño trata que o cruzamento destes dados pode resultar na “síndrome do aquário”, porque os cidadãos vivem em uma casa de cristal, que pode ser constantemente observada e controlada (PÉREZ LUÑO, 2004, p. 96).

Diante da larga utilização da Internet e, conseqüentemente, das mais variadas implicações nas searas da vida humana, há a necessidade de tutela, de forma mais específica e direta, dos dados pessoais e do reconhecimento do direito à autodeterminação informativa no ambiente digital.

Interessa, em um primeiro momento, conceituar os dados pessoais como “[...] qualquer informação (numérica, alfabética, gráfica, fotográfica, acústica), independentemente do suporte (som e imagem), referente a uma pessoa identificada ou identificável” (CASTRO,

2005, p. 70). A Diretiva nº 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995¹ define, em seu artigo 2º, os dados pessoais, como sendo:

[...] 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, económica, cultural ou social (UNIÃO EUROPEIA, 1995).

Há uma variedade de tipos e classificações para os dados pessoais². Entre eles, mostra-se relevante a distinção entre dados em sensíveis e não-sensíveis. Por dados sensíveis, entende-se como os referentes à ideologia, religião ou crença, origem racial, saúde ou vida sexual. Por sua natureza distinta, devem ter especial proteção, a fim de evitar situações de discriminação como, por exemplo, a divulgação de dados relacionados à saúde de determinado indivíduo, que pode resultar em uma não contratação (área trabalhista). Têmis Limberger afirma que tais dados têm uma “[...] potencialidade maior de causar ofensa aos direitos fundamentais, não somente no tocante ao direito à intimidade, mas, especialmente ao princípio da igualdade” (LIMBERGER, 2007, p. 203).

Dados não-sensíveis são, portanto, aqueles não considerados como detentores de especial proteção por não violarem, diretamente, o princípio à igualdade. De acordo com a Diretiva nº 95/46/CE, do Parlamento Europeu e do Conselho, em se tratando de dados não sensíveis, é aplicado o artigo 7º, sendo suficiente o consentimento inequívoco para sempre

¹ A título ilustrativo há a Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, também relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrônicas (Diretiva “Privacidade e Comunicações Electrónicas”). Embora a diretiva conceitue os dados pessoais, amplia a proteção ao tratar, por exemplo, da segurança no tratamento dos dados, em que o fornecedor de serviços de comunicações eletrônicas é obrigado a garantir o acesso aos dados pessoais unicamente a pessoas autorizadas, proteger os dados pessoais contra destruição, perda ou alteração acidentais, garantir a aplicação de uma política de segurança relativa ao tratamento de dados pessoais, entre outras determinações (UNIÃO EUROPEIA, 2002).

² Exemplificando, os dados podem ser considerados dados públicos ou privados. Os primeiros podem ser entendidos como “[...] aqueles do conhecimento geral, fazendo parte do conhecimento e acervo da sociedade, como os que constam de cadastros à disposição do público e dos dados registrados em cartórios e repartições públicas, não cobertos pelo sigilo. Assim podem ser considerados dados públicos: nome, endereço, número de telefone, sexo, CPF, data de nascimento, profissão, identidade civil e/ou profissional, estado civil e filiação partidária” (VEIGA; ROVER, 2004). Para esses autores, dados privados, por sua vez, são os relativos à pessoa física ou jurídica que se mantêm na esfera privada dos cidadãos ou da empresa, não sendo, portanto, do conhecimento geral. Como exemplos, citam-se as informações confidenciais, sigilosas e estritamente pessoais, dentre as quais os atos da vida pessoal do cidadão, hábitos de consumo, preferências de lazer, comunicações realizadas, correspondência recebida e emitida (incluindo-se os *e-mails*), bem como as páginas da Internet com restrição de acesso (VEIGA; ROVER, 2004).

utilizados. Por outro lado, no caso de dados sensíveis, utiliza-se o artigo 8º, sendo necessário o consentimento explícito, ou seja, expresso e escrito (UNIÃO EUROPEIA, 1995).

A proteção dos dados pessoais, públicos ou privados, sensíveis ou não, está diretamente relacionada à tutela da intimidade e da vida privada dos indivíduos. Convém recordar que o direito à intimidade nasce, via de regra, com um aspecto negativo, qual seja, o direito a não ser molestado. Destaque-se, neste ponto, que o direito à intimidade foi mencionado, como o *right to privacy*, por Samuel Warren e Louis Brandeis, em um artigo acadêmico no ano de 1890, como um direito oponível em situações como “[...] violação de propriedade (*property*), violações da confiança (*breach of confidence*), violações do direito do autor (*copyright*) e também dos casos de difamação (*defamation*)” (LIMBERGER, 2007, p. 55). Nessa época, o direito à intimidade tem a conotação como o “direito a ser deixado em paz”, traduzindo-se claramente um direito de primeira geração, que prima pela liberdade.

Posteriormente, este direito evolui em direção a um aspecto positivo, qual seja, o direito a requerer prestações do Estado. Compõe uma visão atual da intimidade, que se entende como mais ativa e dinâmica, contemplando a possibilidade de conhecer, acessar e controlar as informações que concernem a cada pessoa (PÉREZ LUÑO, 2013, p. 119). Constitui-se em um período diretamente relacionado ao Estado Social, em que os cidadãos passam a poder exigir providências do Estado, período em que nasce o *habeas data*³.

Pérez Luño, na mesma esteira, trata que este direito a “estar só”, entendido como um direito à solidão, traduzindo-se em um conceito fechado e estático da intimidade, cedeu lugar a uma concepção ativa e dinâmica, em que a intimidade é tratada como a possibilidade de conhecer e controlar as informações concernentes à pessoa. Por isso, aborda a intimidade não como um estado de auto confinamento, mas como uma determinada relação com os outros, como uma qualidade social da pessoa (PÉREZ LUÑO, 2012, p. 91).

Decorrente desse aspecto positivo do direito à intimidade aborda-se a autodeterminação informativa como um direito fundamental com conteúdo próprio, que não se limita a garantir

³ Interessa salientar que Danilo Doneda, no artigo “Iguais mas separados: o Habeas Data no ordenamento brasileiro e a proteção de dados pessoais”, trata da experiência brasileira na adoção do *habeas data* como o primeiro país a constitucionalizar a garantia. No entanto, faz a crítica de que o instituto ainda não evoluiu a ponto de albergar as questões relacionadas com a utilização da Internet, limitando-se a permitir que o cidadão conheça diretamente os dados e, se necessário, requeira a retificação. Resume-se, portanto, ao binômico acesso/retificação, sem pensar em uma garantia que se adeque “[...] à maleabilidade e dinamicidade do fenômeno tecnológico” (DONEDA, 2008).

a vida privada e a intimidade⁴. Constitui direito do cidadão conhecer, corrigir e, também, determinar a quem, como, quando e de que forma os seus dados pessoais serão divulgados.

Catarina Sarmiento e Castro, ao tratar do conflito entre os direitos fundamentais e a segurança, especialmente após o atentado ocorrido em 11 de setembro de 2001, trata da autodeterminação informativa como um novo direito fundamental, relacionando o tratamento de informações com a informática (CASTRO, 2013, p. 07). Exemplificando, cita a experiência alemã, no ano de 1983, com a Lei do recenseamento geral, que reconheceu “[...] o direito do indivíduo à *proteção contra a utilização* dos seus dados pessoais, bem como o direito de este *determinar a utilização e divulgação* dos dados que lhe respeitam” (CASTRO, 2013, p. 11, grifos das autoras).

Percebe-se que a revolução propiciada pelo advento e difusão da Internet imprimiu um novo significado ao direito à intimidade. Por isso, o cidadão não tem apenas o direito de estar só, mas também a possibilidade de exigir prestações concretas, quer dizer, exigir informações, corrigi-las e, ainda, controlar sua utilização.

Interessante notar que a necessidade de proteção jurídica do cidadão origina-se na constatação de que os dados pessoais que circulam na *web* possuem um conteúdo econômico, ou seja, de que há a possibilidade de comercialização de tais dados. O direito à informação vem sendo, portanto, cada vez mais tratado como uma mercadoria, sob a qual incidem interesses econômicos. Isso decorre, em grande parte, dos fenômenos originados com a globalização e com a crescente importância destinada ao capital que faz com que, inclusive, seja reconhecido, de acordo com Maria Eduarda Gonçalves, um direito de propriedade sobre a informação (2003, p. 210).

Entretanto, a informação não deve ser considerada somente com um viés econômico, de modo que os cidadãos não sejam tomados como consumidores, atores ou produtores de informação, mas como cidadãos que demandam proteção estatal. Torna-se necessário regulamentar os direitos relacionados à Internet para que haja maior segurança na utilização

⁴ Em sentido contrário, Têmis Limberger cita a existência de uma tese negativa acerca da autodeterminação afirmativa constituir-se em um direito fundamental. A título ilustrativo, cita a posição de Erthard Denninger, que defende ser a autodeterminação informativa uma posição já estabelecida há anos, sendo completada por obra da jurisprudência. Para essa corrente, a autodeterminação constitui-se em uma faculdade de dispor dos dados pessoais decorrente da autonomia da conduta, ou seja, como um complemento, advindo da jurisprudência, do direito geral da personalidade que, na atualidade, sofre as consequências da relação entre a intimidade das pessoas e a elaboração eletrônica de dados (LIMBERGER, 2007, p. 105-106).

do espaço e, também, para que o direito à privacidade seja preservado, especialmente quando em conflito com outros direitos fundamentais.

No Brasil, a Lei nº 12.965/14, conhecida como Marco Civil da Internet, propõe-se a estabelecer princípios, garantias, direitos e deveres para o uso da Internet no Brasil (BRASIL, 2014). Acerca da proteção de dados, especificamente, prevê a garantia de proteção e privacidade aos usuários, dependendo, no entanto, da promulgação de lei específica, que ainda está em discussão. Assim, embora o Marco Civil da Internet represente um avanço brasileiro no pertinente ao ciberespaço, ainda é necessário um amadurecimento normativo (FORTES; BOFF; CELLA, 2014, p. 169), com a criação de novos regramentos e leis na matéria cibernética⁵. A lei de proteção de dados pessoais é um dos passos a ser dado neste sentido.

Interessa, para o presente estudo, apresentar a Lei de Proteção de dados da Argentina, país latino-americano próximo ao Brasil que, desde o ano 2000, já possui sólida regulamentação acerca da tutela dos dados pessoais. Este é o objetivo do tópico que segue.

96

2 A PROTEÇÃO DOS DADOS PESSOAIS NA AMÉRICA LATINA: A EXPERIÊNCIA ARGENTINA

No contexto da América Latina, a maior parte dos países ainda não regulamentou a matéria pertinente à proteção de dados pessoais. Em geral, existem apenas leis setoriais sobre o tema, como, por exemplo, a lei acerca da vida privada, no Chile⁶ e a lei sobre informações

⁵ Ressalte-se que em maio de 2016 foi editado o Decreto n.º 8.771, que regulamenta a Lei n.º 12.965/2014 (Marco Civil da Internet), para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações (BRASIL, 2016a). Apesar do avanço em regulamentar o tema, inclusive conceituando os dados pessoais no artigo 14, entende-se que a proteção aos dados pessoais ainda se mostra insuficiente, conforme se observa no decorrer do artigo.

⁶ Trata-se da Lei nº 19.628/99, que foi promulgada no dia 18 de agosto de 1999 e publicada no dia 28 de agosto do mesmo ano, divida, atualmente, em seis títulos e vinte quatro artigos. De acordo com o projeto, esta lei baseou-se em legislações da Espanha, França, Grã-Bretanha, Noruega e Argentina (CHILE, 1999). Mais informações sobre a Lei podem ser encontradas no *site* da Biblioteca Nacional do Congresso do Chile. Disponível em: <<http://www.leychile.cl/Navegar?idNorma=141599&buscar=19.628>>. Acesso em: 25 jan. 2016.

de caráter privado, no Paraguai⁷. Há alguns anos, países como Peru⁸ e México⁹ promulgaram leis específicas de proteção aos dados. No Brasil, desde 2010 é discutido o anteprojeto de lei (BRASIL, 2015a), que somente foi encaminhado à Câmara dos Deputados em maio de 2016 – Projeto de Lei n.º 5276/2016 (BRASIL, 2016b).

No entanto, dois países que já possuem legislação acerca do tema destacam-se: Argentina e Uruguai. Este último iniciou a regulamentação da matéria em 2004, com a Lei n.º 17.838, que tratava da restrição de dados para informações comerciais – além de estabelecer o *habeas data* (URUGUAY, 2004). Em 2008 essa proteção foi expandida com a promulgação da Lei n.º 18.331, tratando especificamente da proteção de dados pessoais e da ação de *habeas data* (URUGUAY, 2008). Em agosto de 2012, a Comissão Europeia, nos termos da Diretiva 95/46/CE, decidiu que a República Oriental do Uruguai possuía adequação do nível de proteção de dados pessoais no relativo ao seu tratamento automatizado¹⁰.

A Argentina, por sua vez, primeiro país latino-americano que editou uma lei de proteção de dados, recebeu certificação da União Europeia quanto ao nível de segurança no tratamento das informações¹¹, apresentando maior abrangência ao tratar do assunto em sua primeira lei sobre o tema, bem como o decreto que regulamenta e detalha a Lei. Em linhas gerais, a Lei de n.º 25.326/00 estabelece direitos e deveres, cria os órgãos de supervisão de proteção de dados e estabelece sanções em caso de descumprimento. Por esta “amplitude” na abordagem da matéria e o reconhecimento dado pela União Europeia acerca de sua segurança, tem-se que a Lei Argentina de Proteção de Dados é uma excelente referência existente na América Latina e pode ser um bom modelo para a regulamentação em outros países, motivo pelo qual será analisada com mais profundidade a seguir.

⁷ A Lei é a de n.º 1.682/01, que foi promulgada em 16 de janeiro de 2001. (PARAGUAI, 2001). Disponível em: <<http://www.senado.gov.py/leyes/index.php?pagina=leyes&id=1031>>. Acesso em: 25 jan. 2016. Referida Lei foi complementada (com artigos ampliados, modificados ou derogados) pela Lei n.º 1.969 de 2002. Disponível em: <http://www.redipd.es/legislacion/common/legislacion/paraguay/Ley_1969_de_2002.pdf>. Acesso em: 25 jan. 2016.

⁸ Trata-se da Lei n.º 29.733/11 (PERU, 2011). Disponível em: <<https://www.huntonprivacyblog.com/uploads/file/Ley%2029733.pdf>>. Acesso em: 25 jan. 2016.

⁹ Publicada no dia 11 de junho de 2002. (MÉXICO, 2002). Disponível em: <http://www.contasabertas.com.br/website/noticias/arquivos/1095_lei%20acesso%20info%20mex.pdf>. Acesso em: 25 jan. 2016.

¹⁰ Trata-se da diretiva 2012/484/EU. (UNIÃO EUROPEIA, 2012). Disponível em: <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:227:0011:0014:PT:PDF>>. Acesso em: 25 jan. 2016.

¹¹ (UNIÃO EUROPEIA, 2003). Decisão da Comissão Europeia. Disponível em: <http://ec.europa.eu/justice/policies/privacy/docs/adequacy/decision-c2003-1731/decision-argentine_en.pdf>. Acesso em: 25 jan. 2016.

A Lei nº 25.326, sancionada e promulgada no mês de outubro do ano 2000, possui o intuito de reger o direito à privacidade no pertinente aos dados pessoais do usuário. Este direito, que se encontra inserido entre os direitos de personalidade, tem como fundamento “[...] o direito de todo indivíduo de ser respeitado como pessoa e não ser prejudicado na sua existência e em sua dignidade¹²” (DELPECH, 2004, p. 279). Mais especificamente, tendo em vista o impacto das novas tecnologias, que facilitaram a coleta e o armazenamento de dados pessoais, tem-se que uma legislação que regulamente o tratamento de dados e proteja o cidadão é necessária, principalmente porque diz respeito a direitos protegidos genericamente nas Constituições¹³.

Neste sentido, em muitas ocasiões o direito à privacidade entra em conflito com o direito à informação, porque alguns dados, em respeito ao primeiro, devem ser protegidos e mantidos em segredo, podendo violar o direito à informação de outras pessoas. Em que pese serem ambos direitos reconhecidos como direitos fundamentais na maioria dos Estados, deve-se sempre objetivar um equilíbrio entre eles, evitando que a proteção de um interfira no outro (DELPECH, 2004, p. 279). É por este motivo que se encontra na Lei Argentina, por exemplo, a possibilidade de retificação, atualização ou supressão de dados, soluções que respeitariam tanto o direito à privacidade como o direito à informação. Entretanto, é importante ressaltar que de acordo com o caso concreto deve-se analisar a melhor solução, “acomodando e situando” direitos dentro de uma perspectiva aceitável (BAUZÁ, 2013, p. 55).

Os dados pessoais estão caracterizados na legislação argentina como “informação de qualquer tipo referida a pessoas físicas ou de existência ideal determinadas ou determináveis” (ARGENTINA, 2000). Além da mera classificação como “informações”, deve-se lembrar de que a combinação de dados pessoais permite a obtenção de um perfil muito preciso dos interesses e atividades de um indivíduo, sendo que estes dados podem ser utilizados para fins diversos, principalmente comerciais e publicitários. Ademais, surgem outros riscos, mais preocupantes, como é o caso de roubo de identidade, para fins criminosos, ou até mesmo perda de um possível emprego, devido a buscas prévias acerca do candidato pela empresa que deseja contratar (DOMÍNGUEZ, 2013).

¹² Este e outros trechos da doutrina de Horacio Fernandez Delpech, pesquisador argentino que analisa a relação entre o Direito e as Novas Tecnologias, bem como de outros autores de língua espanhola, são de livre tradução das autoras.

¹³ É o caso do Brasil, em que estão expressamente previstas como direitos fundamentais a intimidade, a vida privada, a honra e a imagem, sem definir, entretanto, o que seriam violações a esses direitos.

É diante deste contexto de utilização comercial (e também outros fins, em que se pode afetar a privacidade e a segurança) não autorizada pelos usuários que a existência de leis regulamentadoras ganha importância e se justifica. Como afirmou Sánchez Bravo (1998, p.53), ainda nos primórdios da Internet, a proteção de dados pessoais “[...] frente a possíveis abusos informáticos, dentro do âmbito da liberdade dos cidadãos, vem determinada pelas exigências próprias de um Estado de Direito como proteção, não só da intimidade, senão também dos direitos e liberdades públicas em sentido amplo [...]”.

A construção da República Argentina acerca do direito à privacidade e à proteção de dados pessoais iniciou-se com a inclusão do artigo 1071 “bis” do Código Civil¹⁴, que previa sanções àqueles que praticassem atos lesivos à intimidade alheia. A doutrina, na época, mostrou-se dividida acerca da eficácia da modificação, porque foi considerada por muitos como “[...] uma norma de regulamentação estéril” (DELPECH, 2004, p. 283). Quase duas décadas depois, com a reforma da Constituição da Nação Argentina de 1853-1860 em 1994¹⁵, incluiu-se expressamente a ação de *habeas data* como forma de amparo e proteção da intimidade e dos dados pessoais, o que também foi acolhido pela Constituição da Cidade de Buenos Aires.

Ainda, em dezembro de 1996, foi promulgada a Lei 24.766, que define sanções penais para os delitos de violação de segredos e para a ilegítima divulgação de informações de pessoas físicas ou jurídicas armazenadas em meios informáticos. Estes crimes, no entanto, aplicam-se a bases de dados não estatais e definem somente pena de multa quando o autor não for funcionário público – única pena possível tendo em vista que a Lei aplica-se apenas a funcionários não estatais (ARGENTINA, 1996).

Por fim, em outubro de 2000, foi sancionada a Lei 25.326, conhecida por Lei de Proteção de Dados Pessoais, sendo seu decreto promulgado em novembro de 2001. Possui como objetivo fundamental a proteção total de dados pessoais de bancos públicos ou privados destinados a fornecer informação¹⁶, com o fim de garantir o direito à honra e à intimidade das

¹⁴ Tal alteração ocorreu em outubro de 1975. (ARGENTINA, 2000).

¹⁵ Art. 43 [...] “Toda pessoa poderá propor esta ação para tomar conhecimento dos dados a ela referidos e de sua finalidade, que constem em registros ou bancos de dados públicos, ou os privados destinados a prover informações, e no caso de falsidade ou discriminação, para exigir sua supressão, retificação, confidencialidade ou atualização daqueles. Não poderá se afetar o segredo das fontes de informação jornalística” (SEPARATA, 2009). Livre tradução.

¹⁶ Da leitura da Lei e do Regulamento, depreende-se que não são somente os bancos de dados com o intuito de fornecer informações que estão submetidos à Lei 25.326/00, mas todos aqueles que formem arquivos, registros ou banco de dados que não sejam para uso exclusivamente pessoal (DELPECH, 2004, p. 287).

peças, consoante o art. 43 da Constituição Nacional da República Argentina (DELPECH, 2004, p. 285). Por ser uma lei nacional, tem alcance em todo território do país, além de proteger cidadãos argentinos e estrangeiros, dentro ou fora do país, e sempre que os dados estejam armazenados dentro do território argentino (ARGENTINA, 2000).

No pertinente à forma de coletar os dados, a Lei Argentina determina, em regras gerais, que estes devem ser determinados, certos, adequados e pertinentes de acordo com o âmbito e a finalidade para a qual foram colhidos. Somente podem ser captados de forma leal¹⁷ e legal¹⁸, não sendo possível utilizá-los para objetivos diversos dos informados aos titulares da informação, além de ser obrigatória a exatidão e atualização se necessário. Ainda, ao titular deve ser possível acessá-los, sendo imperativa a destruição dos dados quando não forem mais necessários ou pertinentes para os fins pelos quais foram recolhidos (ARGENTINA, 2000).

A Lei 25.326 prevê expressamente, em rol taxativo, quais são os dados considerados sensíveis e quais as exceções em que poderão ser recolhidos. Isto porque a regra é a da proibição do tratamento destes dados, que poderão ser objeto de recolhimento em apenas cinco casos¹⁹: quando forem de relevante interesse geral, autorizado por lei; quando usadas para fins científicos ou de estatística e os titulares não possam ser identificados; em relação às associações religiosas ou organizações políticas, que poderão ter um registro de seus membros; com relação a dados relativos a antecedentes penais e contravenções, que poderão ser utilizados por autoridades públicas competentes; e, por fim, estão permitidos o recolhimento e tratamento de dados em estabelecimentos de saúde públicos ou privados e dos profissionais que tratam ou trataram o indivíduo, ressaltando-se os princípios do sigilo profissional (ARGENTINA, 2000). Ainda, no mesmo artigo sétimo, há a previsão da proibição (no parágrafo terceiro) de registros ou bancos de dados sensíveis mesmo com a

¹⁷ O art. 6º da Lei indica quais informações obrigatoriamente devem ser prestadas ao titular da informação, quais seja: a finalidade do recolhimento e quem pode ser seu destinatário, a existência de arquivo, registro ou similar, o assunto e o responsável, o caráter obrigatório ou facultativo das respostas aos questionários, as consequências de proporcionar os dados, não proporcionar ou proporcioná-los sem exatidão e a possibilidade acerca de direitos de acesso, de retificação e de supressão dos dados (ARGENTINA, 2000).

¹⁸ O art. 5º da Lei estabelece a ilicitude de tratamento dos dados pessoais quando “o titular não houver prestado seu consentimento livre, expresso e informado” (ARGENTINA, 2000).

¹⁹ As exceções estão previstas no art. 7º (ARGENTINA, 2000).

autorização dos titulares da informação, ressalvando-se, por certo, as exceções acima previstas²⁰.

Verifica-se, expressamente, que a Corte Suprema de *Justicia de la Nación* Argentina aplica o disposto na Lei 25.326/00, a exemplo do seguinte julgado:

DERECHO DE ACCESO A LA INFORMACION PUBLICA - SUBSIDIO - PROTECCION DE DATOS PERSONALES - INTERPRETACION DE LA LEY
 Cuando el decreto 1172/03 (Anexo VII, Reglamento General del Acceso a la Información Pública para el P.E.N.), regula las excepciones al deber de proveer información, no determina de manera autónoma -en la materia que aquí interesa- lo relativo a los "datos sensibles" que fundamentan la restricción a aquel deber genérico, sino que se remite, lisa y llanamente, a lo normado en la ley 25.326, no pudiendo informarse lo relativo a "datos sensibles", siendo éstos los definidos por dicha ley en su art. 2º, por lo que el accionar de la demandada- quien se opone a brindar información acerca de subsidios sociales- constituye una pretensión de extender lo "sensible" más allá de los límites marcados por dicha norma, atribuyéndose una prerrogativa que solo compete al legislador. -Voto de los jueces Enrique S. Petracchi y Carmen M. Argibay y voto de la jueza Elena I. Highton de Nolasco- (ARGENTINA, 2014).

Neste caso, que se trata de um exemplo das diversas aplicações práticas da Lei Argentina de Proteção de Dados Pessoais, decidiu a Corte Suprema que não se deve confundir a proteção aos dados dos indivíduos, prevista expressamente na Lei, com as informações públicas, que devem ser publicizadas em casos de relevância pública e interesse social. Existindo na lei a previsão específica dos dados sensíveis, de ordem pessoal e que tratam especificamente de cidadãos em particular, não é possível que se confunda com as informações públicas, que tratam, na verdade, do dever de transparência dos Estados perante sua população.

Ainda que o intuito tenha sido o de respaldar a “proteção” de dados públicos por meio da Lei de Proteção de Dados Pessoais, que não possui esse objetivo, foi devido à especificidade da lei na definição e descrição dos dados pessoais sensíveis, que a Corte, com a simples indicação de artigo de lei, solucionou a questão. A Corte ressaltou, ademais, que a atividade legislativa cabe somente aos legisladores (Poder Legislativo) e a nenhum outro agente. Observa-se que, na realidade, a existência da lei cumpriu seu objetivo, protegendo os indivíduos, e não respaldando a violação de direito à informação pública.

²⁰ É a redação do art. 7º, 3: “Queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles. Sin perjuicio de ello, la Iglesia Católica, las asociaciones religiosas y las organizaciones políticas y sindicales podrán llevar un registro de sus miembros” (ARGENTINA, 2000). É interessante ressaltar que nas leis espanholas e chilenas sobre o tema, ainda que também seja proibido o tratamento dos dados sensíveis, são previstos como exceção os casos em que há o consentimento do titular (DELPECH, 2004, p. 288).

O tratamento dos dados pessoais, sensíveis ou não, impõe a adoção de medidas de segurança e dever de confidencialidade dos dados coletados. É o que apontam os artigos 8º, 9º e 10 da Lei 25.326/00 em relação ao responsável pelo banco de dados, sendo expresso que os dados se configuram como segredos profissionais, que somente poderão ser revelados mediante “[...] decisão judicial ou quando mediante razões fundadas relativas à segurança pública, a defesa nacional ou a saúde pública” (ARGENTINA, 2000). No pertinente aos direitos dos titulares dos dados, além dos direitos já elencados, podem-se citar os três que mais se destacam: o direito de informação (art. 13), o direito de acesso (art. 14) e o direito de retificação, atualização ou supressão (art. 16), todos com previsão expressa (ARGENTINA, 2000).

Uma questão interessante prevista na lei e no decreto é a obrigatoriedade de registro de todos os arquivos, registros bases ou banco de dados públicos ou privados destinados a fornecer informações. Tal registro deve ser realizado junto à Direção Nacional de Proteção de Dados Pessoais, órgão de controle vinculado ao Ministério da Justiça e dos Direitos Humanos, destinado a realizar a fiscalização do cumprimento da lei e a auxiliar os indivíduos para o pleno exercício de seus direitos e tem como principal objetivo justamente o controle junto os bancos de dados existentes (ARGENTINA, 2000).

É importante ressaltar que a Direção Nacional de Proteção de Dados Pessoais foi a responsável pela classificação e graduação das sanções impostas aos descumprimentos da lei, que foram divididas em infrações leves, graves e muito graves. Todas implicam em multa, cujo valor pode variar entre mil e cem mil pesos argentinos, a depender do caso. Ainda, a Lei prevê, no artigo 32, novas figuras penais, determinando como sanção três tipos de condutas: inserir ou fazer inserir dados sabidamente falsos em arquivos de dados pessoais; acessar de forma dolosa e ilegítima, violando os sistemas de confidencialidade, de determinado banco de dados; e revelar a terceiro segredo de banco de dados pessoais cujo segredo está obrigado a manter por força de lei (ARGENTINA, 2000).

Como se observa desta breve apresentação, a Lei Argentina de Proteção de Dados Pessoais regula os principais pontos relativos ao tema em seus quarenta e oito artigos²¹.

²¹ A Lei 25.326 foi modificada e complementada cinquenta e oito vezes, mas sua essência foi mantida, uma vez que as alterações na maioria são decretos, resoluções e disposições a fim de regulamentar alguns pontos. A única lei sancionada foi a de nº 26.343 de 2008, que incluiu o art. 47. Este artigo define o prazo de 180 dias para que os bancos e dados de informações creditícias eliminem informações acerca de dívidas já canceladas ou regularizadas pelos usuários (ARGENTINA, 2008).

Transcreveu-se apenas um julgado da Corte Suprema de Justicia de la Nación Argentina a fim de demonstrar que a Lei é utilizada pelo Judiciário para resolver os conflitos que demandam solução e, portanto, que as decisões são pautadas no texto legal, não ficando ao arbítrio do julgador.

Sendo referência na América Latina, os países vizinhos poderão utilizar-se desta Lei como uma diretriz para regulamentarem seus próprios Estados, que muitas vezes possuem maior número de internautas e, portanto, de cidadãos a ser protegidos.

Nesse sentido, verifica-se que o Brasil conta com mais de noventa e quatro milhões de internautas (CGI, 2014, p. 135) e, no entanto, ainda se discute a regulamentação sobre a proteção dos dados pessoais, cabendo ao Marco Civil da Internet – Lei 12.965/2014 – trazer um panorama geral do assunto. Com isso, os casos que chegam ao Judiciário não dispõem de lei específica para serem resolvidos, sendo necessário basear-se em normas gerais já existentes para solucionar as questões. Diante deste problema, analisar algumas decisões existentes sobre privacidade e proteção de dados no Supremo Tribunal Federal Brasileiro é o propósito do próximo título.

103

3. O TRATAMENTO DOS DADOS PESSOAIS NO BRASIL: CASOS CONCRETOS

No Brasil, a proteção dos dados pessoais não apresenta estrutura unitária, mas se constitui em uma série de dispositivos constantes na Constituição da República, Código Civil, Código de Defesa do Consumidor, entre outros. Na Constituição da República de 1988, garante-se a liberdade de expressão (artigo 5º, IX e artigo 220) e de informação (artigo 5º, XIV, XXXIII e XXXIV e artigo 220), bem como se consideram invioláveis a vida privada e a intimidade (artigo 5º, X), especificamente a interceptação de comunicações telefônica, telegráficas ou de dados (artigo 5º, XII), a proibição da invasão de domicílio (artigo 5º, XI) e de violação de correspondência (artigo 5º, XII). Há, ainda, a instituição do *habeas data* prevendo um direito genérico de acesso e retificação de dados pessoais (artigo 5º, LXXII) (BRASIL, 1988).

Acerca da proteção constante no Código Civil, limita-se aos artigos 20 e 21²², relativos aos direitos da personalidade (BRASIL, 2002). No Código de Defesa do Consumidor refere-se, via de regra, aos bancos de dados dos consumidores, conforme artigo 43 e seguintes (BRASIL, 1990).

Recentemente, o projeto de lei n.º 2.126/11 foi aprovado e convertido na Lei n.º 12.965/14, que trata sobre o Marco Civil da Internet do Brasil, construído de forma colaborativa pela população brasileira²³. Há, ainda, o anteprojeto sobre a proteção à privacidade e aos dados pessoais que, mesmo contando com participação popular em 2010 e em 2015²⁴, somente foi encaminhado ao Congresso Nacional em maio de 2016 e está aguardando pareceres do relator na Comissão de Constituição e Justiça e de Cidadania (CCJC), na Comissão de Trabalho, de Administração e Serviço Público (CTASP) e na Comissão de Ciência e Tecnologia, Comunicação e Informática (CCTCI) (BRASIL, 2016b).

Há três pilares que orientaram a construção do Marco Civil da Internet: neutralidade da rede, liberdade de expressão e privacidade dos internautas. Considerado a “Constituição da Internet” no Brasil, o Marco Civil abarcou alguns pontos que constam do projeto de lei sobre a proteção aos dados pessoais, mas ainda não regulamentou toda a matéria. Exemplificativamente, cita-se o artigo 3º, III que, ao tratar dos princípios em que a lei se baseia refere “proteção dos dados pessoais, na forma da lei” (BRASIL, 2014). Essa lei, no

²² “Art. 20. Salvo se autorizadas, ou se necessárias à administração da justiça ou à manutenção da ordem pública, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou a utilização da imagem de uma pessoa poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se se destinarem a fins comerciais. Parágrafo único. Em se tratando de morto ou de ausente, são partes legítimas para requerer essa proteção o cônjuge, os ascendentes ou os descendentes. Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma” (BRASIL, 2002).

²³ Para a realização da discussão do texto-base produzido pelo Ministério da Justiça foi criado um blog específico (MARCO, 2016), que recebeu, ao longo do processo, mais de 2,3 mil comentários, os quais resultaram no texto legislativo enviado pelo Poder Executivo ao Congresso Nacional em 2011 – Projeto de Lei n.º 2.126/11 (BRASIL, 2012a). No ano de 2016, o debate sobre o Marco Civil da Internet é reaberto, buscando-se novamente a participação popular para construir uma minuta de decreto que consolide os avanços da Lei. Trata-se de minuta contendo vinte artigos, divididos em quatro capítulos e que podem ser comentados pelos cidadãos em site vinculado ao Ministério da Justiça (BRASIL, 2016a).

²⁴ Sobre o debate realizado no ano de 2015: “O texto foi elaborado pela Senacon, em conjunto com a Secretaria de Assuntos Legislativos do MJ, após a realização de dois debates públicos, realizados via internet, um em 2010 e o segundo no primeiro semestre de 2015. No total foram mais de 2000 contribuições dos setores público e privado, academia e organizações não-governamentais. Durante os últimos cinco anos também foram realizadas inúmeras reuniões técnicas, seminários e discussões por diversos órgãos e entidades. Para a secretária Nacional do Consumidor, Juliana Pereira, a versão final do MJ amadureceu nos últimos cinco anos. [...] Para a análise das contribuições do debate público de 2015, a Senacon contou com o apoio do Comitê Gestor da Internet no Brasil e da UFMG. A proposta será encaminhada à Casa Civil” (MIGALHAS, 2015).

entanto, ainda está sendo discutida, o que resulta em uma lacuna jurídica no ordenamento brasileiro.

Por isso, em que pese a edição de uma lei para regular aspectos relacionados ao uso da Internet no Brasil, ainda há pontos que precisam ser solucionados com base na legislação já existente, por não serem abarcados pelo Marco Civil. Importante, portanto, verificar como têm sido julgados os processos que versam sobre direitos relacionados à proteção dos dados pessoais na Internet, razão pela qual foi realizado um levantamento junto ao *site* do Supremo Tribunal Federal. Na pesquisa, realizada durante o mês de dezembro de 2015, inseriram-se as palavras “privacidade internet” no mecanismo de busca relativo à jurisprudência²⁵.

A escolha recaiu sobre o Supremo Tribunal Federal por vislumbrar-se que a principal proteção existente atualmente no Brasil, no que se refere ao direito à intimidade, está contida na Constituição da República de 1988. Como ao Supremo cabe, de acordo com o disposto no artigo 102, *caput*, da Constituição da República, a guarda da Constituição (BRASIL, 1988), optou-se por realizar a pesquisa junto a este Tribunal que, em regra, direciona os entendimentos jurisprudenciais predominantes no país.

Encontraram-se cinco resultados para a busca em questão, sendo que dois tratam do reconhecimento da repercussão geral e os demais são julgados. Deve-se recordar que o instituto da repercussão geral está previsto no artigo 102, §3º, da Constituição da República de 1988, no que se refere à competência do Supremo Tribunal Federal para apreciar e julgar o recurso extraordinário. Deve ser demonstrada a repercussão geral “[...] das questões constitucionais discutidas no caso, nos termos da lei, a fim de que o Tribunal examine a admissão do recurso, somente podendo recusá-lo pela manifestação de dois terços de seus membros” (BRASIL, 1988).

O primeiro julgado que se refere ao reconhecimento da repercussão geral, datado em 22/03/2012, alude ao recurso extraordinário com agravo n.º 660.861, de Minas Gerais, contra acórdão que manteve, em recurso inominado, a condenação da empresa Google ao pagamento

²⁵ Com a finalidade de buscarem-se mais resultados para a pesquisa, inseriram-se as palavras “intimidade internet” no mecanismo de busca do *site* do Supremo Tribunal Federal que, no entanto, apresentou os mesmos casos de repercussão geral que os encontrados quando da busca para “privacidade internet”. A diferença consiste que, na pesquisa em que há o verbete “intimidade”, encontrou-se o julgado referente à Arguição de Descumprimento de Preceito Federal (ADPF) n.º 130/DF sobre que declarou não recepcionado pela Constituição de 1988 todo o conjunto de dispositivos da Lei federal n.º 5.250, de 9 de fevereiro de 1967 (BRASIL, 2009), bem como julgado sobre ofensa à intimidade e compensação por danos morais que, no entanto, não foi apreciado diante da ausência de prequestionamento, violações à Constituição da República não demonstradas e necessidade de reexame do conjunto fático-probatório (BRASIL, 2013a).

de indenização por danos morais, bem como a remoção da página reputada ofensiva, em virtude da criação, por terceiros, de conteúdo ofensivo no *site* de relacionamento *Orkut*. De acordo com o acórdão, foi declarada a responsabilidade objetiva do provedor, em razão do disposto no Código de Defesa do Consumidor, sendo descabida a alegação do Google, de que a criação da página considerada ofensiva e o conteúdo nela disposta seria de responsabilidade do criador do perfil (BRASIL, 2012b).

Também, a empresa alega que verificar, previamente, o conteúdo a ser publicado pelos internautas nas redes de relacionamento, consistiria em censura prévia e afronta aos artigos 5º, IV, IX, XIV, XXXIII e 220, §1º, §2º e §6º, todos da Constituição da República de 1988. De acordo com ela, restariam vulnerados a liberdade de expressão e o direito à informação. Diante da necessidade de verificar se há o dever, para a empresa, de fiscalizar o conteúdo publicado nos domínios eletrônicos sob sua responsabilidade e de retirar as informações reputadas ofensivas, sem a necessidade de intervenção do Poder Judiciário, foi declarada a repercussão geral da matéria, apta a atingir inúmeros casos (BRASIL, 2012b).

A decisão deve ser pautada pela incidência direta dos princípios constitucionais, com a finalidade de verificar a existência ou não de responsabilidade do provedor. Destaque-se que, por inexistir norma própria, necessária a declaração da repercussão geral, com a finalidade de encontrar o correto entendimento para o caso concreto e demais análogos.

O segundo julgado em que foi reconhecida a repercussão geral refere-se à publicação de informações sobre os funcionários, empregados e servidores vinculados ao município de São Paulo. De acordo com a Lei n.º 14.720/2008, regulamentada pelo Decreto n.º 50.070/2008, há a previsão da divulgação dos vencimentos dos servidores, mas sem a vinculação de seus nomes, de forma individualizada, a qual vem sendo realizada no *site* “De olho nas Contas”. O Município sustenta que a veiculação de dados dos servidores na Internet objetiva garantir transparência aos atos e condutas dos agentes públicos, conforme artigos 5º, XIV e XXXIII e 37, ambos da Constituição da República de 1988. Ressalta a não violação ao direito à intimidade, porque todas as informações divulgadas já constaram em leis anteriormente editadas e que, consoante o princípio da publicidade, a restrição do acesso a tais informações somente deve ocorrer de forma excepcional e quando imprescindível à segurança da sociedade e do Estado (BRASIL, 2011a).

Consoante o julgado, a repercussão geral deve ser conhecida, porque há conflito entre direitos da publicidade e proteção da intimidade sendo que, de acordo com a prefeitura de São

Paulo, somente deveria prevalecer o último “[...] quando a divulgação dos dados acarretarem prejuízo à privacidade e segurança do funcionário”. A prefeitura também sustenta a necessidade de pronunciamento do Supremo Tribunal Federal sobre a matéria, para que a questão seja uniformizada e aplicada a todos os municípios brasileiros (BRASIL, 2011a).

O reconhecimento desta repercussão geral demonstra a ocorrência de um dos mais frequentes conflitos entre direitos fundamentais: interesse público e direito à privacidade/intimidade. Destaque-se que a questão vem sendo debatida especialmente após a aprovação da Lei de Acesso à Informação (Lei n.º 12.527/2011), em que qualquer pessoa pode ter acesso a documentos e informações sob a guarda dos órgãos públicos, em todos os poderes e níveis de governo. Dentre os princípios norteadores da Lei está a publicidade e a transparência das informações como a regra e, o sigilo, a exceção, bem como que a informação deve ser repassada de forma ágil, transparente e com fácil compreensão. Além de regulamentar a forma e os prazos para os pedidos e atendimentos às solicitações, a Lei também prevê que a Administração Pública deve promover, por conta própria, a divulgação das informações, independentemente de requisição dos cidadãos (artigo 8º, da Lei n.º 12.527/2011) (BRASIL, 2011b).

Diretamente relacionado com o acesso de informações pelos cidadãos, o terceiro julgado, referente a um *habeas data*, objetiva o acesso às informações constantes de sistemas informatizados de controle de pagamentos de tributos junto ao SINCOR (Sistema de Conta Corrente da Secretaria da Receita Federal do Brasil). O recurso foi provido, por se vislumbrar a existência de direito subjetivo do contribuinte para conhecer as informações que lhe diga respeito em bancos de dados públicos ou de caráter público, conforme previsão do artigo 5º, LXXII, da Constituição da República de 1988 (dispõe sobre o *habeas data*) (BRASIL, 2015b).

De acordo com o julgado, as informações fiscais, constantes do SINCOR, conexas ao próprio contribuinte, se forem sigilosas, devem ser protegidas da sociedade em geral, e não de quem a elas se referem, por força da consagração do direito à informação do artigo 5º, XXXIII, da Constituição da República de 1988. Assim, o Estado violaria os princípios da razoabilidade e da proporcionalidade ao não permitir ao contribuinte o acesso a todas as informações fiscais inerentes aos seus deveres e ao cumprimento de suas obrigações tributárias. Extrai-se do voto do relator Ministro Luiz Fux que no ambiente virtual já se pode consultar, junto ao *site* da Receita Federal do Brasil, “[...] as informações decorrentes de

processamento de declarações, pagamentos de imposto de renda retido na fonte, entre outras informações que são cada vez mais controladas por este órgão”. E, portanto, basta permitir do acesso do contribuinte ao SINCOR pela mesma via eletrônica disponibilizada para o cumprimento de suas obrigações, uma vez que com a Constituição da República de 1988, “[...] o contribuinte deixou de ser objeto da tributação para tornar-se sujeito de direitos” (BRASIL, 2015b).

O quarto julgado encontrado na pesquisa realizada no *site* do Supremo Tribunal Federal refere-se a um pedido de *Habeas Corpus*, em que o paciente enviou comunicações criminosas, contendo injúria, desacato e incitação à prática de crimes, por meio de computador mantido em *lan house* e foi condenado pela prática dos crimes previstos nos artigos 155, 216 e 298, do Código Penal Militar. O pedido sustenta, entre outras matérias de ordem processual penal, que a condenação foi baseada em provas ilícitas, já que colhidas na *lan house* frequentada pelo paciente e que, por isso, haveria violação ao disposto no artigo 5º, XII, da Constituição da República de 1988 (BRASIL, 2012c).

No entanto, o pedido foi denegado, justificando-se não haver qualquer forma de violação à privacidade do paciente. Afirmou-se que o suposto autor dos delitos enviou panfletos *online* a diversos destinatários, tendo-se descoberto que eram enviados de determinada *lan house*. Durante a investigação criminal, o proprietário da *lan house* efetuou o reconhecimento por fotografia do autor, informou as datas e horários que frequentava o local – as quais coincidiram com as datas em que as mensagens foram enviadas –, bem como permitiu a análise do conteúdo do computador então utilizado (e também a realização de perícia), sendo encontradas as provas que identificavam o paciente como autor dos crimes (BRASIL, 2012c).

Sustenta-se, em suma, não ser necessária a autorização judicial para o acesso ao conteúdo constante nos computadores, tendo em vista a existência do prévio consentimento do proprietário dos aparelhos. Também, não era necessário o consentimento do paciente, porque o conteúdo já havia sido por ele publicado na Internet, não havendo qualquer violação à sua intimidade e vida privada. Foi, inclusive, o teor ilícito das publicações que ensejou a investigação criminal, de modo que a investigação realizada na *lan house* apenas propiciou o acesso a dados que permitiram identificar o paciente como o responsável pelo envio das mensagens (BRASIL, 2012c).

Ainda, retira-se do julgado que o paciente não apresenta direito em resguardar o sigilo sobre os dados registrados no computador existente na *lan house* e que, conseqüentemente, os identificaram como autor das comunicações ilícitas. O computador, pertencente a terceiro, poderia ser manuseado por qualquer outra pessoa que, inclusive, poderia entregá-los voluntariamente à autoridade policial e, nem por isso, seriam considerados como prova ilícita. Conclui-se que, em se tratando do acesso aos dados do computador que contou com o consentimento do proprietário, não há como se falar em violação ao direito de privacidade e nem em prova ilícita (BRASIL, 2012c).

Por fim, o quinto julgado encontrado refere-se a Agravo Regimental no Recurso Extraordinário n.º 756917, de relatoria do Ministro Luiz Fux, julgado em 29/10/2013 e que teve a repercussão rejeitada pelo Plenário do STF, sob a justificativa de que o dano moral, quando aferido pelas instâncias ordinárias, não revela repercussão geral apta a dar seguimento ao recurso extraordinário. Saliente-se que o julgado trata de ação de indenização por danos morais decorrente da publicação de fotografias sem a devida autorização. Ocorre que restou demonstrado, nas instâncias ordinárias, que as fotografias foram voluntariamente disponibilizadas pelos autores na Internet, permitindo-se o acesso irrestrito a todos os usuários da rede e, assim, ausência de violação à intimidade e à privacidade (BRASIL, 2013b).

Do exposto, verifica-se que há uma variedade de matérias que versam sobre conflitos entre direitos fundamentais ocorridos na Internet e, conseqüentemente, que demandam especial atenção por parte do Poder Judiciário. A normatização das condutas praticadas por meio da Internet, seja na área cível ou criminal, pode contribuir, assim como demonstrado na experiência da Argentina, facilitando a resolução de conflitos. Todavia, enquanto não há a aprovação do projeto de lei específico no que se refere à proteção de dados pessoais na Internet, necessário aplicar as regras até então existentes, atentando-se às particularidades de cada caso concreto.

CONSIDERAÇÕES FINAIS

O uso das tecnologias de informação e comunicação, há muitos anos inserido na sociedade, facilita e auxilia os indivíduos nas mais variadas tarefas do cotidiano. Entretanto, o uso diário e constante de meios informáticos para a realização das atividades mais comuns acaba, muitas vezes, por camuflar os riscos que estas tecnologias oferecem. O cidadão,

certamente, é a vítima mais contumaz das violações de direitos ocorridas por meio da Internet, principalmente no que tange aos direitos à privacidade e intimidade, porque, até sem ter ciência, suas informações podem ser coletadas, repassadas a terceiros e comercializadas.

No intuito de preservar tais direitos fundamentais, iniciaram-se regulamentações acerca da tutela dos dados pessoais dos usuários, tanto da Internet como de outros bancos de registros. Isto porque, de acordo com a classificação destas informações, as consequências para o titular podem ser malélicas, como a indevida utilização de dados sensíveis relativos a saúde, orientação sexual ou política, entre outros que podem, por exemplo, resultar em uma não contratação ou discriminação.

O principal marco regulatório do tema é da União Europeia, que há décadas trata desta proteção e concede a outros países certificados de adequabilidade no tratamento de dados. Na América do Sul, a Argentina mostra-se avançada nos estudos de proteção de dados pessoais, como se observa da análise da Lei 25.326 que, desde o ano 2000, regulamenta como são realizadas as coletas e armazenamento de dados pessoais, além de definir um controle destes registros pelo Estado e as condições para que sejam realizadas. Este trabalho utilizou-se da Lei Argentina de proteção de dados como referência, pois, além de ter sido o primeiro país sul-americano a regulamentar e defender seus cidadãos neste tema, possui uma grande proximidade com o Brasil, não apenas geográfica, mas também cultural e econômica. Assim, a Argentina é um exemplo a ser seguido, pois apesar de dificuldades de todas as naturezas, similares às brasileiras, está no mesmo patamar de outros países considerados vanguardistas no pertinente à proteção de dados.

No que concerne ao tratamento de dados pelo Estado Brasileiro, os avanços são recentes e ainda incipientes, contando-se apenas com a promulgação da Lei que institui o Marco Civil da Internet e o decreto que o regulamenta. O Projeto de Lei n.º 5276/2016, específico para o tratamento dos dados pessoais, apenas recentemente foi encaminhado ao Congresso Nacional e ainda não foi objeto de discussão entre os parlamentares. Por isso, os casos que tratam sobre o direito à intimidade e à privacidade, principalmente no que tange aos dados pessoais, são solucionados por meio das normas até então existentes. Em busca no *site* do Supremo Tribunal Federal, encontram-se apenas cinco casos que, certamente, poderiam ser resolvidos com maior facilidade se existisse uma regulação acerca do que configura ilegalidade no tratamento de dados pessoais, como se espelha da Legislação Argentina.

Deve-se destacar que não se vislumbra significativa quantidade de julgados junto à pesquisa realizada no *site* do Supremo Tribunal Federal pelas mesmas razões que fizeram com o que o mérito de alguns julgados descritos acima não fossem apreciados: falta de demonstração dos requisitos legais e constitucionais para o seu exame, bem como necessidade de análise fático-probatória, que não é feita pela Suprema Corte. Apesar dessa situação, a temática sob comento denota importância, especialmente diante da constatação de que cada vez mais cidadãos brasileiros utilizam esse meio de comunicação, cujas demandas judiciais e administrativas seriam melhor solucionadas se houvesse previsão legal para tanto, a exemplo da Argentina, e não dependessem da análise, de cada caso concreto, pelos tribunais brasileiros que, muitas vezes, é discricionária.

Portanto, apesar da relevância social do tema, que atinge milhões de brasileiros usuários da Internet, o Brasil ainda engatinha no sentido de regulamentar a proteção dos internautas. Resta aguardar a ação parlamentar na edificação da legislação, esperando-se que sejam seguidas as diretrizes Europeia e Argentina e, até que isto não ocorra, que o Poder Judiciário consiga atender às expectativas dos brasileiros.

111

REFERÊNCIAS

ARGENTINA. Código Civil de La República Argentina, de 30 de outubro de 2000. Disponível em: <http://www.oas.org/dil/esp/Codigo_Civil_de_la_Republica_Argentina.pdf>. Acesso em: 25 jan. 2016.

_____. Lei 24.766, de 30 de dezembro de 1996. Dispõe sobre a confidencialidade de informações e produtos que estejam legitimamente sob controle de uma pessoa e se divulgue indevidamente de maneira contrária aos usos comerciais honestos. Disponível em: <http://www.unlp.edu.ar/uploads/docs/dpi___ley_no_24_766.766.pdf>. Acesso em: 25 jan. 2016.

_____. Lei 25.326, de 30 de outubro de 2000. Disposições Gerais. Dispõe sobre Princípios gerais de proteção de dados, Direitos dos titulares de dados, Usuários e gestores dos arquivos, registros e bancos de dados, Controles, Sanções e Ação para a proteção de dados pessoais. Disponível em: <<http://www1.hcdn.gov.ar/dependencias/dip/textos%20actualizados/25326.010408.pdf>>. Acesso em: 25 jan. 2016.

_____. Lei 26.343, de 09 de janeiro de 2008. Acrescenta o art. 47 à Lei 25.326/00. Disponível em: < http://www.jus.gob.ar/media/33484/Ley_26343.pdf>. Acesso em: 25 jan. 2016.

_____. Corte Suprema de Justicia de la Nación Argentina. CIPPEC c/ EN M° DESARROLLO SOCIAL DTO 1172/03 s/AMPARO LEY 16986. C. 830. XLVI. REX26/03/2014T. 337 P. 256. Disponível em: <<http://sjconsulta.csjn.gov.ar/sjconsulta/documentos/verDocumentoById.html?idDocumento=7098041>>. Acesso em: 02 jun. 2016.

BAUZÁ, Marcelo. La protección de datos personales y su armonización com otros derechos y las politicas de e-gobierno. In: SÁNCHEZ BRAVO, Álvaro (Ed.). *Derechos humanos y protección de datos personales en el siglo XXI*. Sevilla: Punto Rojo, 2013.

BRASIL. Pensando o Direito. *MJ apresenta nova versão do Anteprojeto de Lei de Proteção de Dados Pessoais*. 21 out. 2015a. Disponível em: <<http://pensando.mj.gov.br/2015/10/21/mj-apresenta-nova-versao-do-anteprojeto-de-lei-de-protECAo-de-dados-pessoais/>>. Acesso em: 15 jan. 2016.

_____. Pensando o direito. *MJ abre novo debate público do texto que regulamentará Marco Civil da Internet*. 25 jan. 2016. Disponível em: <<http://pensando.mj.gov.br/2016/01/25/mj-abre-novo-debate-publico-em-torno-do-texto-que-regulamentara-o-marco-civil-da-internet/>>. Acesso em: 26 jan. 2016.

_____. *Constituição da República Federativa do Brasil*. Brasília: Senado Federal, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm>. Acesso em: 25 jan. 2016.

_____. Lei n.º 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Brasília, 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm>. Acesso em: 25 jan. 2016.

_____. Lei n.º 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, 1990. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8078.htm>. Acesso em: 25 jan. 2016.

_____. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Brasília, 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm>. Acesso em: 25 jan. 2016.

_____. Lei nº 12.527/2011, de 18 de novembro de 2011. Regulamenta o acesso a informações previsto no inciso XXXIII do artigo 5º, no inciso II do §3º do artigo 37 e no §2º do artigo 216, da Constituição Federal; altera a Lei n.º 8.112, de 11 de dezembro de 1990; revoga a Lei n.º 11.111, de 05 de maio de 2005, e dispositivos da Lei n.º 8.158, de 08 de janeiro de 1991; e dá outras providências. Brasília, 18 nov. 2011b. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 25 jan. 2016.

_____. Decreto n.º 8.771, de 11 de maio de 2016. Regulamenta a Lei no 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Brasília, 11 maio 2016. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8771.htm>. Acesso em: 2 jun. 2016a.

_____. Câmara dos Deputados. Projeto de Lei 5276/2016. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Disponível em: <<http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378>>. Acesso em: 19 jun. 2016b.

_____. Ministério da Justiça. Câmara dos Deputados começa a analisar Marco Civil da Internet. 29 mar. 2012a. Disponível em: <<http://portal.mj.gov.br/data/Pages/MJ7CBDB5BEITEMID85C774A3C34F4B12823E8661E839CABPTBRIE.htm>>. Acesso em: 25 jan. 2016.

_____. Supremo Tribunal Federal. Procedência da ação para declarar não recepcionado pela Constituição de 1988 todo o conjunto de dispositivos da Lei federal nº 5.250, de 9 de fevereiro de 1967. Partido Democrático Trabalhista (PDT) e Presidente da República e Congresso Nacional. Arguição de Descumprimento de Preceito Federal n.º 130/DF. Relator Ministro Carlos Britto. 30 de abril de 2009. Disponível em: <<http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=605411>>. Acesso em: 25 jan. 2016.

_____. Supremo Tribunal Federal. Negado provimento a Agravo Regimental no Recurso Extraordinário com Agravo. Google Brasil Internet Ltda. e Marcos Antonio Ruas Coelho Sobrinho. Agravo Regimental no Recurso Extraordinário com Agravo 764.388/Minas Gerais. Relator Ministro Teori Zavascki. 3 de setembro de 2013a. Disponível em: <<http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=4531718>>. Acesso em: 25 jan. 2016.

_____. Supremo Tribunal Federal. Acórdão de agravo provido para o reconhecimento da repercussão geral. Google Brasil Internet Ltda. e Aliandra Cleide Vieira. Repercussão geral no recurso extraordinário com agravo 660.861/Minas Gerais. Relator Ministro Luiz Fux. 22 de março de 2012b. Disponível em: <<http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=3058915>>. Acesso em: 25 jan. 2016.

_____. Supremo Tribunal Federal. Acórdão de agravo provido para o reconhecimento da repercussão geral. Município de São Paulo e Ana Marcia Andreu Lacambra. Repercussão geral no recurso extraordinário com agravo 652.777/São Paulo. Relator Ministro Ayres Britto. 29 de setembro de 2011a. Disponível em: <<http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=1902861>>. Acesso em: 25 jan. 2016.

_____. Supremo Tribunal Federal. Ordem denegada em Habeas Corpus. Efraim Santos da Costa e Superior Tribunal Militar. Habeas Corpus 103.425/Amazonas. Relatora Ministra Rosa Weber. 26 de junho de 2012c. Disponível em: <<http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=2541738>>. Acesso em: 25 jan. 2016.

_____. Supremo Tribunal Federal. Agravo regimental desprovido. Leonardo de Pinho Vieira, Marcus de Magalhães e Empresa Folha da Manhã S/A. Agravo regimental no Recurso Extraordinário com Agravo 756.917/São Paulo. Relator Ministro Luiz Fux. Julgado em 29 de outubro de 2013b. Disponível em: <<http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=4872875>>. Acesso em: 25 jan. 2016.

_____. Supremo Tribunal Federal. Recurso Extraordinário provido. Rigliminas Distribuidora Ltda. e União. Recurso Extraordinário 673.707/Minas Gerais. Relator Ministro Luiz Fux. 17 de junho de 2015b. Disponível em: <<http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=9487405>>. Acesso em: 25 jan. 2016.

CASTRO, Catarina Sarmiento e. *Direito da informática, privacidade e dados pessoais*. Coimbra: Edições Almedina, 2005.

_____. *O direito à autodeterminação informativa e os novos desafios gerados pelo direito à liberdade e à segurança no pós 11 de setembro*. Disponível em: <<http://www.buscalegis.ufsc.br/revistas/files/anexos/5544-5536-1-PB.pdf>>. Acesso em: 25 jan. 2016.

CGI.BR. Comitê Gestor da Internet no Brasil. *TIC Domicílios 2014*: Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros. Disponível em: <http://www.cgi.br/media/docs/publicacoes/2/TIC_Domicilios_2014_livro_eletronico.pdf>. Acesso em: 04 jan. 2016.

CHILE. Lei nº 19.628/99, de 18 de agosto de 1999. Dispõe acerca da proteção de dados de caráter pessoal. Disponível em: <<http://www.leychile.cl/Navegar?idNorma=141599>>. Acesso em: 25 jan. 2016.

DELPECH, Horácio Fernandez. *Internet: Su Problemática Jurídica*. 2 ed. Buenos Aires: Abeledo-Perrot, 2004.

DOMINGUÉZ, Ana Garriga. La protección de los datos personales en Internet: problemas actuales. In: SÁNCHEZ BRAVO, Álvaro (Ed.). *Derechos humanos y protección de datos personales en el siglo XXI*. Sevilla: Punto Rojo, 2013.

DONEDA, Danilo. Iguais mas separados: o Habeas Data no ordenamento brasileiro e a proteção de dados pessoais. *Cadernos da Escola de Direito e Relações Internacionais*, v. 09-2008. Disponível em: <<http://revistas.unibrasil.com.br/cadernosdireito/index.php/direito/article/view/444/422>>. Acesso em: 25 jan. 2016.

FORTES, Vinicius Borges; BOFF, Salette Oro; CELLA, José Renato Gaziero. O Poder da informação na sociedade em rede: uma análise jusfilosófica da violação da privacidade e dos dados pessoais no ciberespaço como prática de violação dos direitos humanos. In: ROVER, Aires José; SANTOS, Paloma Maria; MEZZARROBA, Orides (Orgs.). *Governo Eletrônico e inclusão digital*. Florianópolis: Conceito Editorial, 2014. p.157-174.

GONÇALVES, Maria Eduarda. *Direito da informação: novos direitos e formas de regulação na sociedade da informação*. Coimbra: Livraria Almedina, 2003.

LEMOS, André; LÉVY, Pierre. *O futuro da internet: em direção a uma ciberdemocracia planetária*. São Paulo: Paulos, 2010.

LIMBERGER, Têmis. *O direito à intimidade na era da informática: a necessidade de proteção dos dados pessoais*. Porto Alegre: Livraria do Advogado, 2007.

MARCO CIVIL DA INTERNET: *seus direitos e deveres em discussão*. Disponível em: <<http://culturadigital.br/marcocivil/>>. Acesso em: 25 jan. 2016.

MÉXICO. Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, de 11 de junho de 2002. Disponível em: <<http://www.sectur.gob.mx/wp-content/uploads/2014/01/LFTAIPG.pdf>>. Acesso em: 25 jan. 2016.

MIGALHAS. *MJ apresenta nova versão do anteprojeto de lei de proteção de dados pessoais*. 21 out. 2015. Disponível em: <<http://www.migalhas.com.br/Quentes/17,MI228770,81042-MJ+apresenta+nova+versao+do+anteprojeto+de+lei+de+protecao+de+dados>>. Acesso em: 25 jan. 2016.

PARAGUAI. Lei nº 1.682, de 16 de janeiro de 2001. Regulamenta as informações de caráter privado. Disponível em: <http://www.redipd.es/legislacion/common/legislacion/paraguay/Ley_1682_de_2001.pdf>. Acesso em: 25 jan. 2016.

PÉREZ LUÑO, Antonio Enrique. *Cibercidadani@ o ciudadani@.com?* Barcelona: Gedisa, 2004.

_____. *Los derechos humanos em la sociedad tecnológica*. Madri: Editorial Universitas, 2012.

_____. La pretección de los datos personales de carácter sanitario. In: SÁNCHEZ BRAVO, Álvaro (Ed.). *Derechos humanos y protección de datos personales em el siglo XXI*. Sevilla: Punto Rojo, 2013.

PERU. Congreso de La Republica. Lei nº 29.733 de 3 de julho de 2011. Disponível em: <<https://www.huntonprivacyblog.com/uploads/file/Ley%2029733.pdf>>. Acesso em: 25 jan. 2016.

SÁNCHEZ BRAVO, Álvaro. *La protección del derecho de la libertad informática en la Unión Europea*. Universidad de Sevilla: Sevilla, 1998.

SILVA, Rosane Leal da. As tecnologias da informação e comunicação e a proteção de dados pessoais. *Anais do XIX Encontro Nacional do CONPEDI*. Fortaleza, 09-12 junho de 2010. Disponível em: <[https://s3.amazonaws.com/conpedi2/anteriores/XIX+Encontro+Nacional+-+UFC-Fortaleza+\(09%2C+10%2C+11+e+12+de+junho+de+2010\).pdf](https://s3.amazonaws.com/conpedi2/anteriores/XIX+Encontro+Nacional+-+UFC-Fortaleza+(09%2C+10%2C+11+e+12+de+junho+de+2010).pdf)>. Acesso em: 25 jan. 2016.

UNIÃO EUROPEIA. Comissão das Comunidades Europeias. Decisão C(2003) 1731 da Comissão das Comunidades Europeias, de 30 de Junho de 2003. Relativa à proteção adequada dos dados pessoais na Argentina. Disponível em: <http://ec.europa.eu/justice/policies/privacy/docs/adequacy/decision-c2003-1731/decision-argentine_en.pdf>. Acesso em: 25 jan. 2016.

_____. Parlamento Europeu e Conselho da União Europeia. Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002. Relativa ao tratamento de dados pessoais e a proteção da privacidade no setor das comunicações eletrônicas.. Disponível em: <<http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:PT:NOT>>. Acesso em: 25 jan. 2016.

117

_____. Parlamento Europeu e Conselho da União Europeia. Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995. Relativa à proteção de dados das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: <<http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31995L0046&from=PT>>. Acesso em: 25 jan. 2016.

_____. Parlamento Europeu e Conselho da União Europeia. Diretiva 2012/484/UE do Parlamento Europeu e do Conselho, de 21 de Agosto de 2012. Relativa à adequação do nível de proteção de dados pessoais pela República Oriental do Uruguai no que se refere ao tratamento automatizado de dados. Disponível em: <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:227:0011:0014:PT:PDF>>. Acesso em: 25 jan. 2016.

URUGUAY, República Oriental del. Lei nº 18.331 de 18 de agosto de 2008. Disponível em: <<http://www.parlamento.gub.uy/leyes/ AccesoTextoLey.asp?Ley=18331&Anchor=>>>. Acesso em: 20 jan. 2016.

_____. Lei nº 17.838 de 1º de outubro de 2004. Disponível em: <<http://www.parlamento.gub.uy/leyes/ AccesoTextoLey.asp?Ley=17838&Anchor=>>>. Acesso em: 19 jan. 2016.

VEIGA, Luiz Adolfo Olsen da; ROVER, Aires J. Dados e informações na internet: é legítimo o uso de robôs para a formação de base de dados de clientes? In: ROVER, Aires José (Org.). *Direito e informática*. São Paulo: Monole, 2004, p. 27-40. Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/luizvaires-livro_aires.pdf>. Acesso em: 25 jan. 2016.

Submissão: 31/01/2016
Aceito para Publicação: 24/06/2016

