A TUTELA DA PRIVACIDADE NO CONTROLE DE DADOS PESSOAIS NO DIREITO BRASILEIRO

THE PRIVACY PROTECTION IN CONTROL OF PERSONAL DATA IN THE BRAZILIAN LAW

Joana de Moraes Souza Machado*

Recebimento em setembro de 2015.
Aprovação em dezembro de 2015.

Resumo: A sociedade contemporânea é marcada pelos avanços ocorridos na tecnologia de comunicação, possibilitando a socialização das informações. Estas passaram a ter um papel fundamental na vida das pessoas, considerando-se a sua visibilidade pela sociedade pós-industrial. No entanto, tal evolução acabou por invadir o cotidiano das pessoas e empresas, transformando-se inclusive, as formas de relacionamento. Nesse contexto, a privacidade passou a ser entendida não somente pelo aspecto do isolamento, mas também como direito à autodeterminação informativa. Todos os indivíduos devem ter o controle das informações acerca de si. No Brasil não há uma lei de proteção de dados pessoais, dificultando assim o controle destes dados. Este trabalho teve como objetivo apresentar argumentos criteriosamente sistematizados que sustem a efetiva tutela da pessoa frente ao tratamento de dados pessoais por agentes privados. Foi demonstrada neste estudo, a premente necessidade de controle das informações pessoais, no qual só se mostrará viável com o advento de uma legislação protetiva destes dados, que seja adequada à realidade do nosso país. Para alcançar os objetivos propostos, foi utilizada a técnica da pesquisa bibliográfica, com uso de doutrinas nacionais e alienígenas. Utilizou-se ainda a pesquisa documental, valendo-se de materiais que não receberam tratamento analítico, como artigos científicos, reportagens de revistas e documentos internacionais de proteção de dados pessoais.
Palavras-chave:Dados pessoais. Informação. Privacidade.

Abstract: Contemporary society is marked by advances in the communication technology, enabling the sharing of information. These now have a key role in people's lives, considering its visibility by post-industrial society. However, this development turned out to invade people's daily lives and businesses, turning even the forms of relationships. In this context, privacy came to be seen not only from the aspect of isolation, but also as a right to informational self-determination. All individuals should have control of the information about you. In Brazil there is no personal data protection law, thus making it difficult to control this data. This work aimed to present carefully systematized arguments that sustains effective protection of the person against the processing of personal data by private agents. It was demonstrated in this study, the urgent need for control of personal information, which will show if you only feasible with the advent of a protective legislation of this data, which is appropriate to the reality of our country. To achieve the proposed objectives, it used the technique of literature, using national and alien doctrines. It is also used to document research, making use of materials that have not received analytical treatment such as scientific papers, news magazines and international papers of personal data protection.
Keywords: Personal data. Information. Privacy.

INTRODUÇÃO

* Doutora em Direito Constitucional pela Universidade de Fortaleza – UNIFOR, Fortaleza-CE, Brasil. Mestre em Direito e Desenvolvimento pela Universidade Federal do Ceará – UFC. Professora Adjunta do Departamento de Ciências Jurídicas na Universidade Federal do Piauí – UFPI, Teresina-PI, Brasil. E-mail: joana.souza17@hotmail.com

O controle de dados pessoais na ordem jurídica nacional se apresenta de forma indireta. Não há, no Brasil, um marco regulatório específico de proteção de dados pessoais, mas tão somente previsões genéricas na Constituição Federal e leis especiais, que tratam apenas de forma superficial tal temática.

Afirma-se o direito do indivíduo de ter o controle sobre as suas informações pessoais que estejam em poder de bancos de dados públicos e privados, o que se consubstancia no poder de consentimento para o tratamento de dados. Por intermédio do consentimento e da autonomia da vontade se pode estruturar uma disciplina que harmonize os interesses conflitantes.

O panorama jurídico nacional atual não se mostra suficiente e satisfatório para uma efetiva tutela da privacidade informacional, posto que os instrumentos jurídicos disponíveis não tratam especificamente da tutela de dados pessoais, tendo em vista que a privacidade informacional tem um caráter muito mais especifico do que outros desdobramentos deste direito da personalidade.

A evolução tecnológica foi responsável pelo aumento das possibilidades de escolha do indivíduo, com reflexos diretos na personalidade, e mais especificamente na privacidade, imagem e identidade das pessoas. Com isso, o consentimento passou a ser um instrumento de escolha individual e de exercício da sua autonomia privada.

Nesse ensaio, analisar-se-ão os instrumentos normativos nacionais postos à disposição do indivíduo para a tutela de dados pessoais, com o objetivo de se verificar se os mesmos se mostram satisfatórios para uma efetiva proteção da privacidade informacional. Pretende-se, ainda, fazer um estudo crítico-reflexivo acerca do anteprojeto de lei de dados pessoais do Brasil, elaborado pelo Ministério da Justiça em colaboração com a Fundação Getúlio Vargas[1].

1 A PROTEÇÃO CONSTITUCIONAL E INFRACONSTITUCIONAL DE DADOS PESSOAIS NO BRASIL

A disciplina constitucional sobre a regulamentação da proteção de dados pessoais aproxima-se mais do modelo norte-americano do que do s*tandart*europeu. A legislação do direito *anglo-saxão* tinha como princípio que o que não era expressamente proibido seria permitido. Já o modelo *alemão*, firmava o entendimento de que toda a atividade de tratamento de dados pessoais seria proibida, se não fosse permitida expressamente.

[1]Anteprojeto de Lei de Proteção de Dados Pessoais no Brasil. Disponível em: http://www.portalmj.gov.br. Acesso em: 01 de jul.2014.

Ao tratar dos dados pessoais, o constituinte brasileiro dispôs sobre a dupla esfera do direito à intimidade. Como liberdade positiva e como liberdade negativa, ao tutelar a inviolabilidade do sigilo dos dados, no art. 5°, XII e o *Habeas Data*, no seu art. 5°, LXXII, respectivamente. No entanto, deixou uma lacuna relativamente aos contornos daquilo que representa o sigilo dos dados[2].

Muito se discutiu acerca do tratamento dispensado aos dados pessoais na Constituição Federal vigente. Para alguns autores, a disciplina constitucional sobre a matéria se fez de forma muito tímida, sem detalhar as etapas do tratamento de dados, mas tão somente a alguns dos seus aspectos. Porém, não seria tarefa do legislador constituinte detalhar a proteção de dados. Ficaria a cargo da legislação infraconstitucional e dos intérpretes do direito a função de regulamentar o sistema de proteção de dados pessoais.

Aproteção de dados pessoais decorre da tutela da privacidade, protegida em conjunto com a intimidade, no art. 5°, X da Constituição brasileira. No entanto, não se limita por esta, na medida em que há previsão de um leque de garantias constitucionais no ordenamento brasileiro extensível à matéria.

Nos dias atuais, o instrumento de maior relevância para a proteção de dados pessoais no Brasil é *Habeas Data*, criado pela Constituição de 1988 e regulamentado posteriormente pela Lei n. 9.507/97. Mais recentemente foi aprovada normatização que trata dos direitos e deveres dos usuários da internet, Lei n. 12.965/2014, denominada Marco Civil da Internet, que trata de forma genérica da proteção de dados pessoais. As duas legislações serão estudadas nos tópicos subsequentes.

Todavia, antes de adentrar a análise mais aprofundada destas normatizações, faz-se necessário tecer algumas considerações acerca do tratamento constitucional concedido aos dados. O sigilo de dados pressupõe coleta, armazenamento e elaboração de dados, mas não se trata da sua comunicação ou transferência a terceiros (SAMPAIO, 1998, p 548).

Ferraz Junior (1993, p.446) entende que entre as expressões "sigilo" e "dados" deve-se colocar a comunicação, ou seja, permite-se a coleta, o armazenamento, a elaboração e a comunicação a terceiros. No entanto, na forma como foi colocado pelo referido autor, a interpretação mais adequada não seria esta, isto porque o dispositivo constitucional em comento pretende proteger a inviolabilidade do segredo de dados, no qual se inclui a proibição de comunicação a terceiros, bem como a proibição de interceptação por quem quer que seja.

[2]SAMPAIO, José Adércio Leite. **Direito à Intimidade e à Vida Privada**: uma visão jurídica da sexualidade, da família da comunicação e informações pessoais. Belo Horizonte: Del Rey, 1998, p. 548

É preciso entender que no sentido usual, a expressão "dados" significa informações. Em sentido mais técnico, o termo "dados" implica aquela informação que passou por algum tipo de tratamento. Nesse sentido, o sigilo de dados diz respeito ao sigilo das informações tratadas de forma automatizada. Todavia, deve ter um perfil nominativo, para possibilitar identificar direta ou indiretamente o seu titular.

Em outras palavras, a inviolabilidade de dados diz respeito a sua não utilização de forma desleal, ou seja, sem o conhecimento e/ou consentimento do seu titular. Essa lealdade deve ser aferida após a ocorrência do fato, já que não se estabeleceu um regime de autorização, fazendo-se uma análise da adequação dos meios aos fins e dos fins ao direito[3].

Obviamente que, nem todo tratamento de informação precisa passar pelo consentimento do seu titular. Nos casos em que houver interesse social ou público relevantes em conflito, essas informações poderão circular, mas sempre se garantindo o núcleo essencial do direito à privacidade e à intimidade, como por exemplo, os dados sensíveis.

Observa-se que além da previsão constitucional existente no que se refere a dados, há diversas disposições esparsas, que podem ser encontradas no âmbito do direito civil, do direito processual e no direito penal, bem como disposições de perfil comercial e tributário. E mais, muitas destas normativas foram elaboradas em período anterior à Constituição de 1988, como por exemplo, a Lei n 7.232/84, que dispõe sobre a Política Nacional de Informática, prevendo a estruturação e exploração dos bancos de dados.

O Código de Defesa do Consumidor, Lei n. 8.078/90, assegurou ao consumidor no seu art. 43 o acesso às informações pessoais em cadastros, fichas e registros de dados e de consumo arquivados, limitando a permanência desses registros pelo prazo máximo de cinco anos ou até a prescrição da ação de cobrança (o que ocorrer primeiro).

O legislador consumerista demonstrou preocupação com o equilíbrio das relações de consumo, por meio da imposição de limites ao uso de informações de consumidores pelos fornecedores. O uso de informações por parte do fornecedor se mostra como fator de segurança, ou mesmo para desenvolver técnicas comerciais para incremento da sua atividade. No entanto, é necessário que se estabeleça limites, para que o consumidor não perca sua liberdade de escolha, assim como não seja discriminado com o uso destas informações.

Pela análise do Código de Defesa do Consumidor, anteveem-se alguns princípios de proteção de dados pessoais compatíveis com as relações de consumo, nos quais não convém aqui detalhar. Aplicam-se apenas as relações específicas, sem integrarem um sistema geral de

[3] SAMPAIO, Jose Adercio leite. op. cit, p. 505.

proteção de dados pessoais, muito embora sirvam como parâmetros para outras situações, que não sejam relações de consumo.

Pode-se citar o princípio da finalidade em nosso ordenamento, através da aplicação da boa-fé objetiva e da própria garantia da privacidade, pois os dados fornecidos pelo consumidor deverão ser utilizados somente para os fins que para os quais foram coletados[4].

2 O *HABEAS DATA* NO DIREITO BRASILEIRO

O *Habeas Data* é uma garantia criada pela Constituição de 1988, que influenciou legislações latino-americanas. A adoção do instituto por muitos países latino-americanos, ao fato de que na década de 1980, credita-se ao fim de alguns regimes ditatoriais que utilizavam as informações de modo excessivamente autoritário.

O problema naquela época, não estava apenas no uso das informações, mas sim no abuso à sua utilização. Diferentes organismos armazenavam informações sobre as pessoas, sobretudo os órgãos de segurança, que perseguiam os adversários[5].

Dessa forma, o instituto do *Habeas Data* foi criado em momento oportuno, no qual não se concebiam mais as violações perpetradas contra direitos da personalidade, sobretudo, contra o direito à privacidade e à intimidade das pessoas. Esse remédio constitucional teve como objetivo possibilitar ao cidadão o conhecimento direto de informações que lhe diziam respeito, bem como, se necessário retificar tais dados, em caso de incorreção ou inexatidão.

Pode-se afirmar que o *Habeas Data* é uma das ações que constituem o rol de instrumentos para garantia de direitos individuais e coletivos. A sua posição no ordenamento deve ser entendida como uma reação para consolidar as bases democráticas e evitar o retorno ao regime ditatorial, no momento em que a sociedade e o próprio ordenamento estavam se recompondo de um período de ditadura e diversas liberdades individuais vinham sendo suprimidas[6].

A doutrina discutia se o aparecimento do *Habeas Data* foi influenciado pelo pensamento jurídico europeu ou norte-americano, isto porque na época de suainauguração, no

[4]DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 339

[5]Com o advento do golpe militar de 1964, foi produzida farta documentação pelos órgãos de informação, que integram hoje o Centro de Referência das Lutas Políticas – Memórias Reveladas, criado em 2009 pela Casa Civil da Presidência da República, sob a coordenação do Arquivo Nacional. O banco de dados disponível no portal *Memórias Reveladas* oferece informações sobre as investigações e diligências policiais-militares, cassações de direitos, controle individual de pessoas, associações e organizações tidas como suspeitas, dentre outros assuntos. A disponibilização deste acervo constitui um marco na democratização do acesso à informação, bem como serve de instrumento de formação da cidadania. (REDE DE INFORMAÇÕES E CONTRAINFORMAÇÕES DO REGIME MILITAR NO BRASIL. Disponível em: http://www.arquivonacional.gov.br. Acesso em: 02 de jul. 2014).

[6] DONEDA, Danilo. op. cit. p. 332-333

Brasil, aqueles países já possuíam experiência na matéria. Todavia, Doneda[7] lembra que as consequências derivadas das tecnologias na América Latina se apresentam, de forma geral, defasadas e atenuadas em relação aos países desenvolvidos. Acrescente-se a isso, o fato de que naquela época faltava um modelo bem estruturado e claro para servir de exemplo, pois as experiências europeias se desenvolviam isoladamente.

O fato é que o modelo brasileiro se revela genérico, insatisfatório e lacunoso. Necessita de urgente regulamentação por legislação específica para a proteção de dados pessoais, com previsão expressa de que toda informação só possa ser objeto de tratamento para atingir a finalidade para a qual foi disponibilizada. As informações só poderão ser transmitidas a terceiros, com o expresso consentimento do seu titular. Acrescente-se a estes requisitos, a imposição de sanções civil, penal e administrativa pelo descumprimento das regras de proteção de dados.

Quando do surgimento deste remédio constitucional pela Constituição brasileira vigente, muito se questionou se realmente haveria necessidade de se criar uma nova garantia processual, para além do Mandado de Segurança. Até mesmo porque quando da entrada em vigor da Carta de 1988, entendeu-se que tal instituto seria imediatamente aplicável, uma vez que, na falta de norma regulamentadora, seria possível aplicar aquelas normas atinentes ao Mandado de Segurança.

Somente após nove anos da promulgação da Constituição de 1988, foi editada a chamada lei do *Habeas Data,* Lei n. 9.507/97 que passou a regular o direito de acesso às informações e disciplinar o rito processual desse remédio constitucional.

Após o advento da Lei n. 9.507/97, não só foi implementada a forma de obtenção dos direitos assegurados nas alíneas "a" e "b", do inciso LXXII, do art. 5°, como também foi delineado o procedimento do *Habeas Data, c*aso seja necessário o ingresso no poder judiciário.

Não obstante a importância deste instrumento processual para a tutela dos direitos à intimidade e à privacidade, ainda há comumente violações perpetradas contra a privacidade informacional, mais especificamente as informações pessoais constantes em bancos de dados. O remédio constitucional ora analisado somente se aplica quando o indivíduo deseja obter ou retificar informações a seu respeito. Na verdade, não permite ao seu titular qualquer controle sobre a manipulação e tratamento das informações que as empresas públicas ou privadas detenham a seu respeito.

[7] Ibidem, p. 328

É justamente nesse ponto que reside o problema acerca da privacidade informacional: a falta de controle do titular sobre essas informações. Esse fato é bastante corriqueiro no mundo globalizado em que se vive. Muitas vezes, o indivíduo disponibiliza seus dados às empresas privadas, que formam verdadeiros cadastros, com o objetivo de favorecer a celebração de contratos de consumo, ou a divulgação de seus produtos e serviços. Posteriormente, porém, essas organizações transmitem tais informações a outras empresas, sem o conhecimento e a autorização do seu titular,facilitando a lesão ou ameaça à sua intimidade e à sua privacidade.

O procedimento previsto na Lei do *Habeas Data* segue, em linhas gerais, segue o padrão da Lei do Mandado de Segurança, o que se justifica pela patente afinidade entre os dois institutos, implicando que nos casos omissos da Lei n. 9.507/97, deve-se aplicar a Lei do Mandado de Segurança – 12.106/09.

A criação de mecanismos como o *habeas data* para tutela das informações pessoais se mostra de pouca eficácia diante da realidade fática, isto porque dificilmente o cidadão exercerá algum controle sobre estas informações pessoais constantes nos chamados "dossiês digitais", denominação dada por Solove[8].

Deve-se entender que os problemas relativos à coleta, armazenamento e uso de informações por bancos de dados são totalmente diferentes daqueles que se referem à vigilância governamental, como naquela noção de sociedade de controle baseada na obra de George Orwell, em 1984. A metáfora do "Grande irmão" tem como objetivo o comportamento e controle social e não os danos causados pela utilização das informações.

O grande problema que se apresenta com os dossiês digitais é justamente a criação de perfis das pessoas, construídos a partir de informações, antes esparsas, com o objetivo de transmiti-las a outras empresas, isto é, desvirtuando a finalidade para a qual os dados foram disponibilizados, sem o conhecimento e autorização do seu titular.

Em outro sentido, Solove[9] esclarece que não se trata apenas da perda de controle das informações pessoais, nem tão pouco de um plano de dominação do "Grande Irmão". Para o referido autor, o problema é que o processo burocrático é descontrolado e o uso das informações tem efeitos palpáveis, considerando que os referidos dossiês digitais são utilizados por empresas e por governos para tomar decisões sobre indivíduos, que muitas vezes não têm ao menos conhecimento de tal fato.

[8]SOLOVE, Daniel. **The digital person:**Thechnology and privacy in the information age. New York: New York University Press, 2004. Kindle Edition. Ebook.
[9]Ibidem, p. 228-230

Nesse sentido, observa-se que os diversos mecanismos de tutela previstos na Constituição Federal, no Código de Defesa do Consumidor e na Lei 9.507/97 ainda são insuficientes para uma tutela efetiva da privacidade informacional. Necessário se faz, uma tutela específica deste direito, por meio de legislação de proteção de dados pessoais, com a criação de órgão de controle ou autoridade administrativa independente, a exemplo do que se tem nos países da União Europeia, conforme orientação da Diretiva 95/46/CE, bem como nos Estados Unidos, com a *Federal Trade Comission, q*ue exerce o papel de controle e fiscalização de dados pessoais.

Na verdade, o *Habeas Data* é um produto do seu tempo, criado para umanecessidade específica: a de obter, retificar ou fazer anotação de informação pessoal. Hoje, enfrenta o desafio de demonstrar sua aplicabilidade e eficácia, diante de novos recursos da tecnologia de informação e comunicação.

3 A IMPORTÂNCIA DO MARCO CIVIL DA INTERNET PARA PROTEÇÃO DE DADOS PESSOAIS

A Lei n. 12.965/2014, denominado Marco Civil da Internet, estabelece princípios, direitos e deveres para o uso da internet no Brasil.A estrutura destalei está pautada em três pilares: a neutralidade, a privacidade e a liberdade de expressão. Prevista no art. 3°, IV e no art. 6°, a neutralidade impõe que todo conteúdo trafegado pela internet deve ser tratado de forma igual, navegando na mesma velocidade. Esse princípio garante livre acesso a qualquer tipo de informação. Para que haja discriminação ou exceções à neutralidade, necessário se faz decreto presidencial, após consulta do Comitê Gestor da Internet.

Assim, as operadoras de telecomunicações não podem fazer distinção de tráfego baseadas em interesses comerciais. Deve-se garantir que os dados possam ser acessados sem qualquer distinção no que se refere à origem ou conteúdo, pois os provedores da internet não podem fixar valores extras para que usuários participem de determinados serviços, por exemplo[10].

A privacidade é mencionada no art. 3° e no art. 7°, I, quando estabelecem os direitos do usuário no acesso à internet. Textualmente se afirma a inviolabilidade da intimidade e da vida privada, bem como a sua proteção e indenização por dano material ou moral decorrente

[10] Recentemente, a operadora de serviços Velox e banda larga da Oi foi multada pelo Ministério da Justiça por infrações às normas de defesa do consumidor. Esta condenação foi motivada em razão do serviço navegador disponibilizado aos consumidores. Foi constatado que a Oi em parceria com a empresa britânica Phorm estava desenvolvendo um software chamado "navegador", que mapeava o trafego de dados do consumidor na internet, traçando o seu perfil de navegação. Estes perfis eram comercializados com anunciantes, agências de publicidade e portais da *web*. (Matéria publicada no dia 24 de jul. 2014. Disponível em: http://www.migalhas.com.br. Acesso em: 24 de jul. 2014).

de sua violação. Prevê ainda, no seu art. 8° que "A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet".

A privacidade das pessoas na era digital vem sendo há muito tempo ameaçada, no entanto, o governo brasileiro só passou a atentar para o fato após denúncias de espionagem dos EUA. Por esta razão, houve certa "urgência" na aprovação desta lei, somando-se a este fato, o evento NetMundial[11] realizado aqui no Brasil, em que a Presidente Dilma Rousseff pretendia utilizar a mencionada lei como "marca" da sua gestão no setor de tecnologia de informação.

Quando da aprovação da referida legislação, muito se discutiu se a liberdade de expressão não estaria sendo violada, diante de certas limitações impostas para a tutela da privacidade das pessoas. No entanto, percebeu-se que ambos os interesses (liberdade e privacidade) são direitos da personalidade preservados pela nova lei, embora passíveis de limitações. Afinal, nem mesmo a fundamentalidade de um direito o torna absoluto.

Conquanto a nova legislação aborde a temática da proteção de dados pessoais, não o faz de maneira detalhada e deixa a tarefa a cargo de ulterior lei específica. Ou seja, o legislador cuidou apenas de alguns aspectos da tutela dos dados pessoais. No art. 3°, III dispôs que a proteção dos dados pessoais é um dos princípios a ser observado para a disciplina do uso da internet. Garantiu a inviolabilidade e sigilo do fluxo de suas comunicações, no art. 7°, II. Também foi objeto de tutela a inviolabilidade das comunicações privadas armazenadas, salvo por ordem judicial.

No Marco Civil da Internet ficou assegurado no art. 7°, VIII, que os usuários da internet terão informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de dados pessoais, que somente poderão ser utilizados para as finalidades pelas quais foram coletados. Fica assegurado ainda no inciso VII "o não fornecimento a terceiros de seus dados pessoais, inclusive registro de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei".

Veja-se que o consentimento assume lugar de destaque em tal regulação, estando intrincada a autodeterminação informativa, no poder de controle que o indivíduo deve ter de informações que lhe dizem respeito. Tais dados só poderão sair da esfera de controle do seu titular com a sua autorização.

[11] O evento Netmundial foi realizado em São Paulo nos dias 23 e 24 de abril de 2014. Trata-se de encontro para discutir o futuro da Governança da internet. Mais informações: Disponível em: http://www.netmundial.br. Acesso em: 20 de jul. 2014.

Um dos pontos que chamou a atenção, independente de se ter uma legislação específica sobre proteção de dados pessoais, foi o direito à autodeterminação informativa, consubstanciada no controle das informações pessoais na internet, um direito garantido pela legislação em comento.

De fato, essa legislação não poderia ficar alheia à proteção de dados pessoais, muito embora não seja seu objetivo principal, no entanto, na ausência de legislação específica acerca desta matéria, o Marco Civil teve que antecipar algumas regras referentes ao tratamento de dados pessoais, até porque uma grande parte da utilização da w*eb* envolve a questão do uso de dados pessoais dos internautas.

Nesse sentido, observa-se que os s*ites* brasileiros utilizam os dados dos usuários de forma totalmente indiscriminada, não esclarecem nem informam de forma transparente o que acontecerá com as informações que lhes são solicitadas. Muitos *sites* de redes de lojas sequer informam que utilizam na sua política de segurança os chamados *Cookies,* ou quando informam não o fazem de forma clara e transparente.

Os denominados *Cookies s*ão arquivos no formato de texto, utilizados para armazenamento de dados, tendo como objetivo a personalização e otimização do usuário em determinado ambiente virtual, instalados de forma automática no disco rígido do computador do usuário no momento da visita àquela página virtual[12].

A questão gira em torno da relação dos *Cookies* com a privacidade. Na maioria das vezes, há o total desconhecimento por parte dos usuários que têm seus dados coletados e monitorados, situação que impossibilita o controle destas informações pelos seus titulares.

Nesse contexto, muito dificilmente o cidadão tem condições de perceber o risco que a coleta e o armazenamento de informações pessoais por empresas dotadas de meios sofisticados de tratamento de dados podem trazer para ele. Assim, o usuário deverá ser informado de forma clara e transparente acerca de todo o processo de tratamento de seus dados, pois somente ele terá o poder de autorizar a utilização destas informações.

De fato, a Lei n. 12.965/2014, denominada de Marco Civil da Internet revela-se como avanço, fixando um marco histórico e jurídico de utilização da *web* no Brasil. Aplica-se a todas as situações em que esteja em perigo a privacidade do usuário, mas também tendo sido respeitada a liberdade de expressão das pessoas como direito igualmente integrante da personalidade humana. No entanto, verifica-se que, mesmo com o advento desta lei, não se conseguiu resolver o problema da proteção dos dados pessoais.

[12]FOROUZAN, Behrouz A. **Comunicação de dados e redes de computadores**. Porto Alegre: Bookman, 2006, p. 854

4 O ANTEPROJETO DE LEI DE PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

O Brasil é o único país da América Latina[13] que não dispõe de uma legislação específica de proteção a dados pessoais, mas tão somente normatizações genéricas que, por sua própria natureza, não conseguiram tutelar de forma efetiva os direitos relacionados a dados pessoais, como a privacidade e a intimidade[14].

Dessa forma, percebe-se a ausência de proteção no que se refere a dados pessoais no Brasil, muito embora encontrem-se legislações que tratam superficialmente do tema, mas não da forma que a matéria merece. Por esta razão, a Secretaria de Assuntos Legislativos e o Departamento de Defesa do Consumidor do Ministério da Justiça, em colaboração com o Observatório Brasileiro de políticas Digitais do Centro de Tecnologia e Sociedade da Fundação Getúlio Vargas, tomando por base leis de abrangência internacional, como por exemplo, a Diretiva 95/46/CE, elaborou o anteprojeto de lei de proteção de dados pessoais – ALPDP[15], que passou de 30 de novembro de 2010 a 30 de abril de 2011 por debate público sobre a privacidade e a proteção de dados pessoais.

O objetivo central do anteprojeto é assegurar ao cidadão o controle e a titularidade sobre suas próprias informações, como forma de garantir a tutela do direito à privacidade informacional, bem como ao direito à intimidade. Note-se que, com os avanços na tecnologia de informação e comunicação, torna-se cada vez mais comum a obtenção e utilização de informações, sem o conhecimento do seu titular.

Em uma sociedade da informação como a que se vive atualmente, em que os dados representam um bem valioso, revelando-se como representação da própria personalidade do indivíduo, um regramento específico terá como principal beneficiário o cidadão, como titular dos dados pessoais, devendo ser considerado parte mais frágil nas relações que envolvem grandes organizações empresariais e o próprio Estado. Com o advento de uma regulação de proteção de dados, o indivíduo passa a ter maior segurança no que diz respeito ao tratamento adequado de tais informações, que compõem sua privacidade e intimidade.

---

[13] O Chile possui, desde 1999, legislação nesta matéria – Lei 19.628/99. Disponível em http://www.sernac.cl/leyes/comppendio/docs_compendio/ley19628.pdf. Acesso em: 15 de jun. 2014. Na argentina, a Lei 25.326/2000. Disponível em http://www.jus.gob.ar/datos personales.aspx. Acesso em: 15 de jun. de 2014. No México a legislação de proteção de dados pessoais surgiu em 2010 – *Ley federal de Protección de DatosPersondelosParticularesales em Posesión de los particulares.* Disponível em: http://www.ifai.org.mx/. Acesso em 15 de jun. de 2014.

[14] A Lei de proteção de dados chilena tem características especificas que a difere das demais legislações dos países vizinhos. Foi fortemente influenciada pela lei espanhola. Destacando-se a ausência de uma autoridade de garantia, pois cabe ao interessado o recurso à justiça ordinária, bem como identifica-se ainda, uma ausência de responsabilidade objetiva do gestor dos dados.

[15] Anteprojeto de Lei de Proteção de Dados Pessoais no Brasil. Disponível em: http://www.portalmj.gov.br. Acesso em: 01 de jul.2014.

Merece destaque a natureza principiológica dada ao anteprojeto de lei de proteção de dados pessoais, com influência das Diretivas da União Europeia, sobretudo da Diretiva 95/46/CE. A proposta de lei traz como base a previsão de dez princípios para a proteção de dados pessoais, tais como: finalidade, necessidade, livre acesso, proporcionalidade, qualidade de dados, transparência, segurança física e lógica, boa-fé objetiva, responsabilidade e princípio da prevenção.

Tem como objetivos específicos, conforme o art. 1°: garantir e proteger, no âmbito do tratamento de dados pessoais, a dignidade e os direitos fundamentais da pessoa, especialmente os referentes à liberdade, igualdade e privacidade pessoal e familiar, isto porque toda pessoa tem direito à proteção de seus dados pessoais.

Logo no 4°, o legislador pretendeu estabelecer alguns conceitos-chave para uma melhor compreensão do texto em análise, como por exemplo, o de dado pessoal, tratamento, bancos de dados, dados sensíveis e outros, como se veem:

> Art. 4° Para os fins da presente lei, entende-se como:
> I – dado pessoal: qualquer informação relativa a uma pessoa identificada ou identificável, direta ou indiretamente, incluindo todo endereço ou número de identificação de um terminal utilizado para conexão a uma rede de computadores.
> II – tratamento: toda operação ou conjunto de operações, realizada com ou sem auxilio de meios automatizados, que permite a coleta, armazenamento, ordenamento, conservação, modificação, comparação, avaliação, organização, seleção, extração, utilização, bloqueio e cancelamento de dados pessoais, bem como seu fornecimento a terceiros por meio de transferência, comunicação ou interconexão.
> III – bancos de dados: todo conjunto estruturado de dados pessoais, localizado em um ou vários locais, em meio eletrônico ou não.
> IV – dados sensíveis: dados pessoais cujo tratamento possa ensejar discriminação por parte do titular, tais como aqueles que revelem origem racial ou étnica, as convicções religiosas, filosóficas ou morais, as opiniões políticas, a filiação sindical, partidária ou a organizações de caráter religioso, filosófico ou político, os referentes à saúde e à vida sexual, bem como os dados genéticos.

Entende-se que o conceito de dados sensíveis se apresenta como um dos mais importantes para a discussão desta temática, considerando o efeito devastador que o tratamento e utilização de tais dados podem trazer para o seu titular, sobretudo quando utilizados para fins discriminatórios. Como se pode perceber, as grandes organizações têm se utilizado de bancos de dados cadastrais para construir verdadeiros perfis das pessoas, sem qualquer critério de classificação e, com isso decidir com quem desejam contratar.

Sem contar no âmbito trabalhista, em que os empregadores buscam a todo custo, devassar toda a vida de um potencial colaborador, com o objetivo de reduzir as chances de "erro" na escolha. Todavia, essa intromissão na vida privada das pessoas só seria possível se fosse com o seu consentimento, que na maioria das vezes, nem elas mesmas têm o conhecimento de tal fato.

Essa invasão na privacidade informacional dos indivíduos traz efeitos absolutamente maléficos à sua personalidade, considerando que se trata de informações que só dizem respeito à própria pessoa, ao âmbito mais reservado possível, como os dados referentes à convicções religiosas, filosóficas, políticas, bem como orientações sexuais e aquelas atinentes à saúde da pessoa.

O anteprojeto ora em discussão estabelece que nenhuma pessoa será obrigada a fornecer dados sensíveis, ficando proibida a formação de bancos de dados que contenham informações que, direta ou indiretamente, revelem dados sensíveis, salvo disposição legal expressa, respeitados os direitos de personalidade, especialmente a garantia à não discriminação, conforme o c*aput d*os arts. 20 e 21.

No entanto, a referida proposta de normatização prevê algumas hipóteses em que serão admitidos o tratamento de dados sensíveis, como por exemplo, se o titular houver dado o seu consentimento livre, informado e por escrito, sempre que este tratamento for indispensável para o legítimo exercício das atribuições legais ou estatutárias de seus responsáveis (art. 21, §1, inciso I).

Nesse sentido, o anteprojeto de lei de proteção de dados pessoaisbusca resgatar direitos valiosos à personalidade, como a privacidade informacional que, não obstante seja tutelada de forma genérica pela nossa Lei Maior, necessita de uma atenção especial por parte do legislador infraconstitucional, considerando os avanços na tecnologia de informação e comunicação ocorridas nos últimos anos.

Verifica-se que o anteprojeto de lei teve uma preocupação especial com o consentimento, enfocando o poder do indivíduo de exercer um controle absoluto das informações que lhe dizem respeito. Cabe apenas ao indivíduo, o direito de autorizar a utilização dos seus dados pessoais. A esse respeito, o anteprojeto de lei utiliza as palavras-chave consentimento e autorização. O consentimento para o tratamento de dados pessoais é um dos pontos mais sensíveis desta temática. Por intermédio dele, o direito civil tem a oportunidade de estruturar, a partir da autonomia da vontade, uma disciplina capaz de harmonizar os efeitos deste consentimento com os demais interesses em jogo[16].

Enquanto expressão da autonomia da vontade, o consentimento deve ser interpretado como uma manifestação da escolha individual. As possibilidades de escolhas do indivíduo têm reflexos diretos nos direitos da personalidade, considerando que vários destes direitos dependem de certa forma da autonomia da vontade.

[16] DONEDA, Danilo. op. cit., p. 371.

O Capítulo III do anteprojeto em discussão trata dos requisitos para o tratamento de dados pessoais, que somente pode ocorrer após o consentimento livre, expresso, e informado do titular, podendo ser dado por escrito ou por outro meio que o certifique (art. 9°).

As pessoas que realizam o tratamento de dados pessoais têm o dever de informar de maneira clara e explícita ao titular dos dados: a finalidade para a qual os seus dados estão sendo coletados e de que forma serão tratados; a identidade e o domicilio do responsável pelo tratamento; a natureza obrigatória ou facultativa do fornecimento de dados; os sujeitos para os quais os dados podem ser comunicados e os seus direitos, em particular a possibilidade de se negar a fornecer tais dados e sobre seu direito de acesso e retificação dos mesmos (art. 11).

Em alguns casos, o consentimento poderá ser dispensado, segundo o que dispõe o art. 13 do anteprojeto de lei, como por exemplo, quando for necessário à execução de obrigações derivadas de um contrato no qual é parte o titular, assim como também para execução de procedimentos pré-contratuais requeridos por este, ou para o cumprimento de uma obrigação legal por parte do responsável

O consentimento pode ser dispensado, ainda, conforme prevê o art. 13, IV quando se estiver diante de tratamento de dados para fins estatísticos. Nessa hipótese especifica, deve-se tomar cuidado, pois atualmente há pesquisas comportamentais tendo por base dados coletados dos indivíduos com informações dissociadas.

Essa metodologia utiliza dados coletados durante a utilização de s*ites* pelo usuário, por meio dos chamados *Cookies*, permitindo traçar perfis de grupos específicos, que podem levar ao cruzamento de dados. Essa análise estatística do comportamento virtual das pessoas pode levar a influenciar a coletividade e os hábitos dos usuários, tais como: o horário em que acessam determinado s*ite,* as páginas mais acessadas, os serviços mais utilizados e outros dados que podem ser relevantes quando não dissociados.

Por outro lado, o titular dos dados pessoais poderá se recusar a revelá-los, exercendo assim, o seu poder de autodeterminação, o que na maioria das vezes o faria ficar de fora daquela relação negocial, impossibilitando-o do acesso a determinados bens e serviços. Por esta razão, Rodotá[17]o considera um "mito", pois a sua utilização como instrumento para a tutela dos dados pessoais deve ser verificada a partir de sua concreta aplicação.

Tome-se como exemplo, uma pessoa que pretende adquirir um bem, financiado por instituição financeira, deverá preencher um cadastro. No entanto, não lhe convém responder a

[17]RODOTÁ, Stefano. **Elaboratorielettronici e controllosociale**. Bologna: Il Mulino, 1973, p. 45-51.

certas questões, por envolver dados considerados sensíveis. Tal circunstância faz com que a instituição financeira não aceite contratar, por faltar informações pessoais, consideradas relevantes para as organizações empresariais. Na verdade, o indivíduo não tem muita opção, ou ele aceita a conceder todas as informações necessárias para a celebração do contrato ou não poderá adquirir o bem.

Vê-se que aqui não se está tratando do consentimento negocial, mas sim de consentimento para tratamento de dados pessoais, que é bem mais especifico do que aquele concedido para a celebração de contratos, por exemplo. Assim, entende-se que não se revela adequado caracterizar o consentimento como sendo de natureza negocial. Se assim o fosse, dificultaria ou mesmo impossibilitaria a tutela dos dados pessoais, como atributo da personalidade. O consentimento para tratamento de dados pessoais está diretamente vinculado a elementos da própria personalidade, todavia não dispõe destes elementos, já que assume a natureza de um ato unilateral, quando concede autorização para tratamento de dados pessoais.

Verifica-se, portanto, que o consentimento poderá assumir o papel de instrumento da autodeterminação, sendo um aspecto da tutela da personalidade, bem como poderá desnudar-se em fator de legitimação para que os dados sejam utilizados por terceiros. Todavia, não se pode interpretar esta última hipótese como de natureza negocial, mesmo que possa parecer que o indivíduo que autoriza o uso de dados por terceiros, o faria em troca de alguma vantagem, até porque acarretaria a utilização de esquemas proprietários para o tratamento destes dados.

Outra questão que merece especial atenção é aquela referente à comunicação e interconexão dos dados pessoais. Com a evolução nas tecnologias de informação e comunicação, esta prática passou a ser corriqueira nas grandes organizações empresariais. Atualmente, revela-se muito comum, empresas que disponibilizam ou até comercializam dados pessoais com o absoluto desconhecimento dos seus titulares.

O anteprojeto de lei de proteção de dados estabeleceu que a comunicação ou interconexão dos dados pessoais só é possível com a permissão do seu titular, sendo tal consentimento revogável a qualquer tempo, conforme o art. 28, c*aput* e § 1° do mesmo dispositivo. Note-se a importância que foi dada ao consentimento pelo legislador, considerando que a proteção de dados pessoais está diretamente ligada à personalidade, por intermédio da privacidade e intimidade das pessoas.

No entanto, entende-se que na prática não se revela fácil o cumprimento do requisito do consentimento para quaisquer formas de tratamento de dados pessoais, diante dos recursos que a tecnologia coloca à disposição, principalmente das grandes organizações. Por exemplo,

o indivíduo disponibiliza seus dados pessoais ao preencher cadastro em uma empresa privada. Meses depois, uma instituição financeira, de posse do cadastro desta pessoa, entra em contato para oferecer empréstimos e cartões de crédito, por ter tido acesso a estas informações, que contribuíram para a constituição de um dado perfil de interesse daquela empresa.

Entende-se ainda que a possibilidade de "comercialização de dados pessoais" só se afiguraria como possível, havendo previsão expressa na lei de proteção de dados pessoais, o que não consta no anteprojeto ora em análise, nem tão pouco nas legislações que serviram de base para elaboração de tal proposta de lei. Somente a lei poderia restringir direitos relacionados a proteção de dados pessoais, como faz o Código Civil brasileiro, quando possibilita, excepcionalmente, o uso da imagem da pessoa, quando autorizada por ela ou quando necessária à administração da justiça, conforme o art. 21.

Ao término do tratamento, os dados pessoais deverão ser cancelados quando deixarem de ser necessários ou pertinentes à finalidade pela qual foram coletados. Todavia, o legislador previu a possibilidade de os dados serem cedidos a terceiros, desde que destinados a finalidades análogas àquelas para as quais foram colhidos. No entanto, necessita do consentimento do titular.

Insta destacar que toda entidade privada que realize tratamento de dados pessoais, que tenha mais de duzentos empregados deverá indicar um responsável pelo tratamento de dados pessoais, que deverá zelar, de forma independente, pela observância das disposições da presente lei (art. 34, c*aput* e§1°).O responsável pelo tratamento de dados terá como funções: atuar como correspondente imediato da Autoridade de Garantia; orientar os demais funcionáriosa respeito das práticas a ser tomadas em relação à proteção de dados pessoais e; manter uma relação dos tratamentos de dados pessoais realizados pela empresa que sejam acessíveis aos seus titulares que o requisitarem.

O responsável pelos dados pessoais nas empresas com mais de duzentos funcionários deverá passar por um treinamento acerca da legislação de proteção de dados, muito embora não haja previsão para este feito, já que muitas vezes as pessoas que manuseiam estas informações são absolutamente leigas na matéria. Note-se ainda, que este processo se mostra como lento, não logrando êxito, tão logo a lei for aprovada e entrar em vigor, pois deverá passar por um processo de conhecimento e adaptação por parte daqueles que realizam tratamento de dados pessoais.

Não se compreende com base em que o legislador estipulou esse limite de empregados para que uma determinada empresa tenha um responsável pelos dados pessoais manuseados. Tal exigência não se revela adequada em razão do tipo de bem que se pretende

tutelar, devendo-se incluir, todas as empresas com atuação no âmbito eletrônico, independente do número de colaboradores, considerando ainda as consequências advindas do tratamento dos dados pessoais.

Pela análise do anteprojeto, verifica-se ainda que a Autoridade de Garantia foi diversas vezes citada, mas importa saber, o que mesmo significa esta autoridade? Quais as suas funções e o seu papel na proteção de dados pessoais? Do ponto de vista prático, a referida autoridade contribuirá de forma positiva para proteção de dados pessoais?

Nos dias atuais, a vida das pessoas envolve uma troca continua de informações, com um grande fluxo de dados, com isso, se atribui importância especial à proteção de dados pessoais. Esta evolução é bastante visível em outros países, sobretudo naqueles que integram a União Europeia. A legislação sobre proteção de dados pessoais fixa regras sobre as modalidades de tratamento, concretizando-se em poderes de intervenção.

Estes poderes de controle e intervenção não devem mais ser atribuídos somente aos interessados diretos, isto porque como ensina Rodotá[18], devem ser confiados também a uma autoridade independente, envolvendo uma responsabilidade pública específica.

A legislação italiana, mais especificamente o Código em matéria de tratamento de dados pessoais – Decreto Legislativo n° 196, de 30 de junho de 2003, previu expressamente a figura do Garante, no seu art. 153 e 154. Dispôs inicialmente que, o Garante atuará com plena autonomia e independência de juízo e de valoração. Formado por um órgão colegiado, constituído por quatro membros, sendo dois eleitos pela Câmara dos Deputados e dois pelo Senado da República com voto limitado. Os membros deverão ser escolhidos entre pessoas com notória competência nas matérias do direito ou da informática[19].

Vê-se que a legislação italiana se preocupou logo em fixar regras para a nomeação dos membros que comporão o órgão colegiado, da forma mais democrática possível, demonstrando-se dessa forma, a caraterística basilar de um órgão independente e autônomo, sem subordinação a nenhum dos poderes.

A ideia de uma Autoridade de Garantia partiu desde o advento da Diretiva 95/46/CE, em que impôs aos países-membros da União Europeia, a obrigatoriedade de sua instituição,

[18]RODOTÁ, Stefano. **A vida na Sociedade de Vigilância**. A privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Trad. Danilo Doneda e Luciana Doneda. Rio de Janeiro: Renovar, 2008, p. 199.

[19] O Art. 153 do Código em matéria de Proteção de Dados Pessoais estabelece que: ”1. Il Garante opera in piena autonomia e conindipendenza de giuduzio e divalutazione. 2. Il Garante e’ organocollegialecostituito de quatro componenti, elettiduedallaCamera dei deputatu e duedalSenatodelllaRepubblica com voto limitadto. I componenti sono sceltitrapersonecheassicuranoindipendenza e che sono espertidiriconosciutacompetennza dele materiedeldiritto o dell’informatica, garantindo lapresenzadientramblelequalificazioni”. Disponível em: http://www.parlamento.it/parlam/leggi/deleghe/03196dl.htm. Acesso em: 20/04/2014.

passando a ser uma caraterística marcante do modelo europeu. No entanto, posteriormente foi adotado por outros países, que não integram a União Europeia, como Argentina, Austrália, Canadá, Japão.

O recurso à um órgão de fiscalização e controle, dotado de independência é uma prática bastante comum nos Estados democráticos. O ente estatal, não tendo mais condições de arcar com a responsabilidade pela fiscalização dos diversos serviços públicos postos à disposição do cidadão, bem como pela necessidade de se regular determinadas áreas do mercado, cria órgãos de controle e fiscalização.

Pode-se citar como exemplo no Brasil, as chamadas agências reguladoras[20], tais como: Agência Nacional de Telecomunicações – ANATEL; Agência Nacional de Petróleo – ANP; Agência Nacional de Energia Elétrica – ANEEL; Agência Nacional de Saúde Complementar – ANS; Agência Nacional de Vigilância Sanitária – ANVISA; Agência Nacional de Aviação Civil – ANAC, dentre outras.

Não se pretende afirmar que o órgão que compõe a Autoridade de Garantia seja uma agência reguladora, mas tão somente demonstrar as semelhanças entre ambas, já que têm funções de órgão controlador e fiscalizador[21].

O Anteprojeto de Lei de proteção de dados pessoais no Brasil prevê no seu art. 38, a figura da Autoridade de Garantia:

> Art. 38. É criado o Conselho Nacional de Proteção de Dados Pessoais, com autonomia administrativa, orçamentária e financeira, com a atribuição de atuar como Autoridade de Garantia quanto à proteção de dados pessoais, cuja estrutura e atribuições serão estabelecidas em legislação especifica.

O referido dispositivo se limitou a prever a criação do órgão e suas principais características, deixando para outra legislação a sua estrutura e atribuições. Entende-se que esta lacuna configura uma falha grave, considerando que o Brasil já inicia tardiamente a tutela

[20] As agências reguladoras surgiram quando da instituição das autarquias de controle, consideradas autarquias sob regime especial, tendo como prerrogativas: a) poder normativo técnico; b) autonomia decisória; c) independência administrativa e; autonomia econômico-financeira. O poder normativo indica que estes órgãos recebem a delegação de editar normas técnicas de caráter geral, retratando um poder regulamentar mais amplo. Já a autonomia decisória significa que os conflitos administrativos se desencadeiam e se dirimem através dos próprios órgãos da autarquia. A independência administrativa refere-se ao fato de que alguns dos seus dirigentes têm investidura a termo, sendo nomeados para prazo determinado, como por exemplo, um cargo em comissão, não obstante a investidura por prazo certo. Por fim, a autonomia econômico-financeira demonstra que estas autarquias têm recursos próprios, recebendo dotações orçamentárias para gestão por seus órgãos. (CARVALHO FILHO, 2009, p. 454-457).

[21] Em Parecer elaborado pelo escritório de advocacia Patrícia Peck Pinheiro Advogados – PPP, localizado na cidade de São Paulo- SP, como contribuição para redação do Anteprojeto de Lei de proteção de dados pessoais, destacou que o Brasil optou por um modelo arrojado, adotando um sistema que possui componente legislativo delineado os dogmas e a conduta esperada daqueles que praticarem o tratamento de dados e, que por seu turno, criará um conselho controlador e fiscalizador, similar a de uma Agência Reguladora, como o objetivo de resolução de conflitos, impasses e aplicação penalidades sem a necessidade de se recorrer ao judiciário. (PINHEIRO, Patrícia Peck. Disponível em: http://www.culturadigital/dadospessoais. Acesso em: 01 de jul. 2014).

específica de dados pessoais. Deixar para regular posteriormente esta estrutura significa atrasar mais ainda a concretização deste direito integrante da personalidade humana.

Defende-se nesteensaio, que o legislador brasileiro fixe desde logo a forma de criação deste órgão, bem como os membros que o integrarão, a exemplo do que fez a legislação italiana, que de modo mais democrático, decidiu que os membros fossem eleitos pela Câmara dos Deputados e Senado Federal, com mandato fixo, tornando legítimo o papel dos membros que irão compor a Autoridade de Garantia independente.

É importante frisar que uma das características basilares da Autoridade de Garantia é a sua independência, devendo afastar o máximo possível a possibilidade de ingerência ou subordinação dos poderes estatais constituídos. Por esta razão, é indispensável a criação de mecanismos que resguardem tal perfil, no momento da nomeação de seus membros, limitando a discricionariedade de sua escolha, com requisitos mais objetivos.

A constituição deste órgão que atuará como Autoridade de Garantia é de extrema importância para a efetiva proteção dos dados pessoais, como direito integrante da personalidade humana. Por esta razão merece do legislador uma atenção especial.

O que se defende é que a tutela dos dados pessoais seja efetiva, considerando-se o estágio atual da tecnologia, bem como a dimensão jurídica internacional desta temática, tendo como centro de preocupação do ordenamento jurídico a pessoa humana.

O anteprojeto de lei prevê ainda no seu art. 41, as sanções administrativas a ser imputadas em hipótese de infrações das normas previstas na lei, tais como: multa; bloqueio dos dados pessoais; dissociação dos dados pessoais; proibição do tratamento de dados pessoais; suspensão temporária de atividade e; proibição de funcionamento do banco de dados. Tais sanções serão aplicadas pela Autoridade de Garantia, podendo ser aplicadas cumulativamente, conforme o caso.

No entanto, causa estranheza o legislador não ter previsto nenhuma sanção criminal no referido projeto, havendo assim o risco de redução da eficácia, tendo em vista o tipo de sanção sofrida por aquele que a descumprir.

A autoridade de Garantia deverá impor ainda, de oficio ou a pedido da parte, as medidas coercitivas que considere necessárias para reverter efeitos danosos que a conduta infratora tenha causado ou para evitar que esta se produza no futuro novamente, fixando ainda, multa diária por dia de descumprimento, conforme o art. 43, c*aput,* do referido anteprojeto de lei.

Por fim, o anteprojeto trata da possibilidade de os responsáveis pelo tratamento de dados pessoais, individualmente ou por meio de organizações de classe, formularem códigos

de boas práticas, estabelecendo as condições de organização, regime de funcionamento, procedimentos aplicáveis, normas de segurança e demais formas de garantia para as pessoas, com respeito aos princípios e normas de proteção de dados. Os códigos de boas práticas deverão passar pelo crivo da Autoridade de Garantia, que poderá não aprová-lo se estiverem em desacordo com as disposições legais e regulamentares sobre a matéria.

Constata-se, por fim, que a efetividade do direito à privacidade informacional depende, em certa medida, de uma ação positiva por parte do Estado, isto porque o poder público tem o dever de implementar medidas administrativas e legislativas, necessárias à concretização deste direito tão valioso da personalidade humana.

CONCLUSÃO

A proteção dos dados pessoais revelou-se como tema de grande importância, diante das inovações tecnológicas nas áreas da informação e comunicação ocorridas nas últimas décadas. Esta matéria está intimamente intrincada com a tutela da privacidade, que restou ameaçada pelo advento da denominada "sociedade da informação".

Buscou-se neste trabalho contribuir para a compreensão da necessidade de proteção dos dados pessoais para uma efetiva tutela da privacidade informacional, em face das novas investidas tecnológicas, considerando o contexto social, econômico e político que aí se instaurou.

A relação entre privacidade e informação, diante dos avanços tecnológicos no mundo globalizado é muito próxima. Hoje, o que de fato interessa é a privacidade informacional, consubstanciada no direito do indivíduo ter o absoluto controle sobre os seus dados.

O controle por parte do cidadão revela-se de difícil implementação, tendo em vista a rapidez e a maleabilidade das informações. Observa-se a necessidade de se adotarem medidas legislativas acerca da proteção de dados, pois as normas existentes postas à disposição do cidadão não são suficientes e adequadas para uma efetiva tutela.

O Brasil é o único país do Mercosul a não possuir legislação acerca desta matéria, o que demonstra a fragilidade do direito à privacidade informacional nos dias atuais, em face das novas investidas tecnológicas.

O anteprojeto de lei de proteção de dados pessoais revela a grande influência sofrida pela legislação europeia, sobretudo, a Diretiva 95/46/CE. No entanto, demonstrou-se a preocupação em se utilizar como exemplo uma normatização, que apesar de ser paradigmática no assunto, reflete a realidade de países que compõem a União Europeia. Ou seja, não revela a

realidade de um país em desenvolvimento, com fortes desigualdades sociais e um histórico de corrupção como o Brasil.

Por fim, a fragilidade do direito à privacidade nos dias atuais, especialmente no Brasil, é clara diante dos recursos utilizados para a coleta, armazenamento e tratamento de dados pessoais. Defende-se assim, a imediata regulamentação especifica desta matéria, por entender que os instrumentos normativos existentes não são suficientes e adequados pa tutela efetiva.

REFERÊNCIAS

ASCENSÃO, José de Oliveira. **Direito da Internet e da sociedade da informação**. Rio de Janeiro: Forense, 2002.

BARROSO, Luís Roberto. A viagem redonda: habeas data, direitos constitucionais e provas ilícitas. In: WAMBIER, Teresa Arruda Alvin (coord.). **Habeas Data.** São Paulo: RT, 1998, pp.202-221.

BENJAMIN, Antônio Hermann. **Código Brasileiro de Defesa do Consumidor comentado pelos autores do anteprojeto**. Rio de Janeiro: Forense, 1997.

BRASIL. **Constituição da República Federativa do Brasil**. Brasília, DF, 1988.

_____. Lei n. 12.965, de 23 Abrilde 2014.**Estabelece princípios, garantias, direitos e deveres para uso da internet no Brasil**. Brasília, DF, 2014.

_____. Lei nº 10.406, de 10 de janeiro de 2002.**Institui o Código Civil.** Brasília, DF, 2002.

_____. Lei 9.507/97, de 12 de novembro de 1997. **Regula o direito de acesso a informações e disciplina o rito processual do *habeas data*.**Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L9507.htm. Acesso em: 06 de abril de 2014.

_____. Lei nº 9.986, de 18 de julho de 2000.**Dispõe sobre a gestão de recursos humanos das Agências Reguladoras e dá outras providências.** Brasília, DF, 2000.

_____. Lei n. 8.078, de 11 de setembro de 1990. **Institui o Código de Defesa do Consumidor**.Brasília, DF, 1990.

BUENO, Cassio Scarpinella. Habeas Data. In: Fredie Didier Jr. (Org.). **Ações Constitucionais**. Salvador: Podivm, 2012.

CARVALHO FILHO, José dos Santos. **Manual de Direito Administrativo**. Rio de Janeiro: Lumem Juris, 2009.

CASTELLS, Manoel. **A galáxia da Internet**: Reflexões sobre a internet, os negócios e a sociedade. Trad. Maria Luiza Borges. Rio de Janeiro: Zahar, 2003.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

_____. Um código para proteção de dados pessoais na Itália. In: **Revista Trimestral de Direito Civil**. Ano 4. Vol. 16, out-dez, 2003.

DOTTI, René Ariel. A liberdade e o direito à intimidade. In: **Revista de Informação Legislativa**: Brasília. Ano 17, n. 66, abr./jun. 1980.

FERRAZ JUNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites a função fiscalizadora do Estado. In: **Cadernos de Direito Constitucional e Ciência Política**. São Paulo: Revista dos Tribunais, 1993.

FOROUZAN, Behrouz A. **Comunicação de dados e redes de computadores**. Porto Alegre: Bookman, 2006.

FOUCAULT, Michel. **Vigiar e punir**. Petrópolis: Vozes, 1988.

GERMAN, Cristiano. **O caminho do Brasil rumo à era da informação**. São Paulo: Fundação Konrad Adenauer, 2000.

GUERRA, Sidney. **O direito à privacidade na internet**: uma discussão da esfera privada no mundo globalizado. Rio de Janeiro: América Jurídica, 2004.

ITÁLIA. **Codice in matéria diprotezione dei datipersonali**. Decreto legislativo 196, de 30 de agosto de 2003. Disponível em: http://www.parlamento.it/parlam/leggi/deleghe/03196dl.htm. Acesso em: 20/04/2014.

LEONARDI, Marcel. **Tutela e privacidade na internet**. São Paulo: Saraiva 2012.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONUBR). **Direito à privacidade na era digital**. Disponível: http://www.onu.org.br/20013. Acesso em 01 de julho de 2014.

PERLINGIERI, Pietro. **Perfis do Direito Civil**. Trad. Maria Cristina de Cico. Rio de Janeiro: Renovar, 2007.

PINHEIRO, Patricia Peck. **Parecer- Contribuições para redação do Anteprojeto de Lei de Proteção de Dados Pessoais**. Disponível em: http://www.culturadigital/dadospessoais. Acesso em: 01 de jul. 2014.

PINTO, Paulo Mota. A limitação voluntária do direito à reserva sobre a intimidade da vida privada. **Revista Brasileira de Direito Comparado**. Publicação do Instituto de Direito Comparado Luso-Brasileiro: Rio de Janeiro, 2002.

RODOTÁ, Stefano. **A vida na Sociedade de Vigilância**. A privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Trad. Danilo Doneda e Luciana Doneda. Rio de Janeiro: Renovar, 2008.

_____. **Elaboratorielettronici e controllosociale**. Bologna: Il Mulino, 1973.

SAMPAIO, José Adércio Leite. **Direito à Intimidade e à Vida Privada**: uma visão jurídica da sexualidade, da família da comunicação e informações pessoais. Belo Horizonte: Del Rey, 1998.

SOLOVE, Daniel J. **The digital person:**Thechnology and privacy in the information age. New York: New York University Press, 2004. Kindle Edition. Ebook.

_____.**A Taxonomy of Privacy**. University of Pennsylvania Law Review, Vol. 154, No. 3, p. 477, January 2006; GWU Law School Public Law Research Paper No. 129. Disponível em: <http://ssrn.com/abstract=667622>. Acesso em 16/03/2013.

UNIÃO EUROPÉIA. Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995. Jornal Oficial n° L281, de 23/11/1995. Disponível em: http:www.eur-lex.europa.eu. Acesso em: 28/01/2014.