Excelentíssima Senhora Deputada Bruna Furlan (presidente)
Excelentíssimo Senhor Deputado Orlando Silva (relator)

D. Comissão Especial Destinada a Proferir Parecer ao Projeto de Lei n. 4.060, de 2012, do Deputado Milton Monti, que dispõe sobre o Tratamento de Dados Pessoais e dá outras Providências, e apensados.

Ref. Parecer Técnico encaminhado pela Professora Livre Docente de Direito Civil da Faculdade de Direito de Ribeirão Preto/USP, Dra. Cíntia Rosa Pereira de Lima

1 Introdução

O objeto desse parecer técnico é a análise sobre o tema "**Modelo Regulatório: órgão, agência e autorregulamentação",** a partir do convite que nos foi feito pelo E. Deputado Orlando Silva (PCdoB) requerimento 13/17, deferido pela E. Deputada Bruna Furlan (PSDB).

"Regular" é conciliar os interesses econômicos, públicos e sociais. Nesse sentido, uma legislação sobre proteção de dados não busca frear o desenvolvimento econômico. Ao contrário, assim como outras leis setoriais, denominadas como microssistemas jurídicos, esse Projeto de Lei pretende consolidar um sistema de proteção de dados para viabilizar a inserção do Brasil no capitalismo informacional, no qual a propriedade das coisas foi substituída pelo controle das informações; um modo revolucionário (global e interconectado) de estruturação do mercado e circulação dos produtos e serviços; e, por fim, a substituição do predomínio dos bens rivais (*rivalrousness*) para o predomínio dos bens e serviços não rivais (*nonrivalrousness*), muitos desafios são apresentados para os aplicadores do direito.

Zygmunt Bauman[1] distinguiu o capitalismo "pesado", caracterizado pelo modelo fordista, cujos objetivos eram volume da produção e definição de tarefas para otimizar os resultados, com um apego a fronteiras (limites), sempre firmes e impenetráveis; do capitalismo "leve", que ao contrário, não há fixação de fronteiras tão rígidas e as tarefas não estão bem definidas.

Neste contexto, quanto à proteção dos dados pessoais, uma preocupação constante é sobre seu *enforcement,* pois se os dados são enviados à distância ignorando limites geográficos, é viável que um dado coletado em um país que tenha um modelo de proteção seja enviado para outro que não ofereça a mesma tutela, o que na prática fomentaria os denominados "paraísos dos dados pessoais".

Para evitar esse efeito, a legislação comunitária europeia (hoje o Regulamento Geral 279/2016; antes também a Diretiva 46, de 1995) estabeleceu um critério para o dado ser enviado para países que não fazem parte da União Europeia, qual seja, o nível adequado de proteção de dados. De maneira que se um país não satisfaça tal

[1] *Modernidade Líquida.* Tradução de Plínio Dentzien. Rio de Janeiro: Jorge Zahar, 2001. pp. 75 – 77.

critério, a ser oficialmente reconhecido pela União Europeia, ficará à margem do capitalismo informacional.

Esse é, portanto, outro motivo que justifica a adoção de uma lei de proteção de dados que represente um nível de proteção de dados pessoais semelhante ao europeu, para que as empresas brasileiras possam competir em igualdades de condições no capitalismo informacional.

Para tanto, não basta adotar uma legislação sobre o tema, mas o modelo regulatório deve ser eficiente. Na América Latina, o Uruguai foi o primeiro país a ter o reconhecimento europeu sobre a adequação do modelo de proteção de dados adotado naquele país, que criou uma agência reguladora para fiscalizar e fazer cumprir a lei uruguaia de proteção de dados, ou seja, a *Unidad Reguladora y de Control de Datos Personales (URCDP),* órgão da *Agencia para el Desarrollo del Gobierno de Gestión Electronica y la Sociedad de la Información y del Conocimiento (AGESIC)*.

Preliminarmente, cumpre-nos destacar que o Projeto de Lei n. 4.060 de 2012, de autoria do E. Deputado Milton Monti, *data venia*, apresenta um sistema de proteção de dados tímido e dissonante com o nível assegurado e exigido por outros países.

Ademais, o Projeto de Lei n. 6.291 de 2016, de autoria do E. Deputado João Derly, *data venia*, traz como objeto apenas a vedação do compartilhamento de dados pessoais dos assinantes de aplicações de internet, por meio da sugerida alteração do Marco Civil da Internet, Lei n. 12.965, de 23 de abril de 2014.

Parece-nos mais completo o sistema de proteção de dados desenhado no Projeto de Lei n. 5.276-A, de 2016, que é de autoria do Poder Executivo pelas razões explicitadas nesse parecer.

2 Análise do Projeto de Lei n. 4.060, de 2012 (do Sr. Milton Monti)

Quanto ao aspecto conceitual, cumpre destacar a diferença entre "privacidade" e "dados pessoais". A diferença entre esses dois conceitos é clara e já está pacificada nas legislações estrangeiras, pois se tratam de direitos de personalidades autônomos. Assim, não é tecnicamente adequado estabelecer correlação entre dados pessoais e "liberdade, privacidade, intimidade, honra e imagem", mesmo porque estes direitos são assegurados na Constituição Federal e tutelados pelo Código Civil.

Por exemplo, a *Convenção Europeia sobre Direitos Humanos e Liberdades Fundamentais* - art. 8º - assegura o direito à privacidade.[2] No mesmo documento, porém em outro dispositivo, garante-se o direito à proteção dos dados pessoais (art. 7º da Carta).[3]

Por fim, Stefano Rodotà[4] destaca uma diferença importante entre o direito `a privacidade cuja tutela é estática e negativa. Enquanto a tutela dos dados pessoais estrutura-se a partir de regras sobre o tratamento de dados, poderes de intervenção, entre outros, por isso, a tutela é dinâmica, ou seja, surge com a coleta dos dados e permanece com eles durante a circulação e armazenamento.

No art. 1º deste PL n. 4.060, de 2012 (do Sr. Milton Monti), faz-se uma correlação perigosa, *in verbis:* "[...], particularmente em relação a sua liberdade, privacidade, intimidade, honra e imagem". A sugestão seria alterar a redação para não estimular qualquer confusão entre esses conceitos. O objeto dessa lei é assegurar a

[2] "ARTICLE 8 - Right to respect for private and family life - 1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

[3] Article 7 - Respect for private and family life - Everyone has the right to respect for his or her private and family life, home and communications.

[4] Tra diritti fondamentali ed elasticità della normativa: il nuovo codice sulla *privacy.* In: *Europa e Diritto Privato,* fasc. 01, pp. 01 – 11, Milão: Giuffrè, 2004. p. 03.

proteção dos dados pessoais, estabelecendo regras para sua coleta, tratamento, utilização, entre outras atividades, afim de assegurar o pleno desenvolvimento do ser humano.

No art. 6º , inc. IV deste PL n. 4.060, de 2012 (do Sr. Milton Monti), novamente se incorre na confusão entre tutela dos dados pessoais e dados de domínio público, ou seja, a dicotomia entre público e privado é irrisória quando se trata de proteção de dados pessoais. Neste sentido, Giusella Finocchiaro[5] destaca que determinado dado pessoal, ainda que não seja privado, é objeto de tutela pela legislação sobre proteção de dados pessoais. Portanto, conclui que a definição de dado pessoal não faz referência direta nem indireta à privacidade. Em suma, o objeto do direito à privacidade é diverso do objeto do direito à proteção dos dados pessoais. O primeiro é assegurar o resguardo de parcela de sua vida privada; o segundo, por sua vez, é proteger os dados e as informações (ainda que de conhecimento público) de serem objeto de tratamento em desacordo com as regras e códigos de condutas. Desta forma, sugere-se eliminar esse inciso, pois as regras de tratamento de dados podem incidir sim sobre dados públicos.

Art. 7º, inciso I do PL n. 4.060, de 2012 (do Sr. Milton Monti), não leva em consideração o uso das tecnologias para reidentificação, por isso, o conceito de dado pessoal proposto não está ajustado com os padrões internacionais, o que fatalmente comprometerá o reconhecimento da adequação do nível de proteção de dados brasileiro. Neste sentido, parece-nos mais adequado adotar o conceito proposto no PL N. 5.276-A: "*dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos quando estes estiverem relacionados a uma pessoa*;".

Art. 7º, inciso VII do PL n. 4.060, de 2012 (do Sr. Milton Monti), destacam-se os perigos da utilização do termo "bloqueio", termo evitado pelo PL n.

[5] *Privacy e protezione dei dati personali:* disciplina e strumenti operativi. Bologna: Zanichelli, 2012. p. 36 – 37.

5.276-A (art. 52, inc. VII), a nosso ver, de forma mais acertada, pois pode gerar confusão com a medida ora em discussão no STF (ADI n. 5.527, rel. Min. Rosa Weber e ADPF n. 403, rel. Min. Edson Fachin) sobre a possibilidade ou não de bloqueio de aplicações por determinação judicial. Dessa forma, melhor seria utilizar a expressão "suspensão" como o faz o PL apresentado pelo Executivo.

Esse mesmo problema pode surgir do **Art. 13 do PL n. 4.060, de 2012 (do Sr. Milton Monti),** melhor seria direito à oposição ao registro, por exemplo.

Art. 14 do PL n. 4.060, de 2012 (do Sr. Milton Monti), este artigo não está de acordo com o padrão internacional de proteção de dados na medida em que viabiliza a circulação de dados pessoais, de maneira transfronteiriça, sem a ciência e o consentimento expresso do titular para tal finalidade. Em outras palavras, ainda que o titular de dados conceda o seu consentimento para o tratamento de dados, poderá desconhecer que esse mesmo dado pode vir à circular, livremente, inclusive, abrindo margem para a sua venda para terceiros. Sugere-se, exigir o consentimento livre e expresso para que se possa compartilhar dados do mesmo grupo econômico, segundo o entendimento consolidado a partir do caso WhatsApp e Facebook.

Art. 15, parágrafo único do PL n. 4.060, de 2012 (do Sr. Milton Monti), estabelece o sistema ***opt out,*** o que nos parece prejudicial e contrária à regra em que se exige o consentimento livre, expresso e prévio do titular dos dados, inclusive regra estabelecida na legislação vigente (art. 7º, inc. VII do Marco Civil da Internet). Assim, a coleta, o tratamento e o envio de dados pessoais somente podem ser autorizados previamente pelo titular dos dados.

Art. 18 do PL n. 4.060, de 2012 (do Sr. Milton Monti), apenas menciona os vícios de dolo e coação, enquanto o art. 9º, §3º do PL 5.276-A elenca outros vícios do consentimento também, portanto, parece-nos mais completo.

Arts. 19 e 20 do PL n. 4.060, de 2012 (do Sr. Milton Monti), restringem o direito do titular apenas o "bloqueio", ou seja, o direito à oposição à coleta, ao tratamento e ao envio dos dados pessoais. Entretanto, os direitos dos titulares dos dados assegurados vão além do direito à oposição, devem ser assegurados também: o direito ao acesso, à correção, e etc., todos mencionados no art. 18 do PL 5.276-A.

TITULO II – DA TUTELA FISCALIZATORIA E SANCIONATORIA - Arts. 21, 22 e 23 do PL n. 4.060, de 2012 (do Sr. Milton Monti), este projeto estabelece como sistema preferencial a autorregulamentação, estruturada a partir de "Conselhos de Autorregulamentação" instituídos pelas entidades representativas dos responsáveis pelo tratamento de dados pessoais.

Esse sistema (preconizado no art. 23 do PL n. 4.060) assemelha-se muito com o CONAR, uma sociedade sem fins lucrativos com sede em São Paulo e duração ilimitada.[6] Cabe destacar que esse órgão foi criado de maneira espontânea (e não por determinação legal) sob o temor de que o governo sancionasse uma lei para estabelecer uma espécie de análise prévia do conteúdo publicitário. Assim, para evitar a interferência do Estado, o CONAR foi fundado para coibir publicidade enganosa e abusiva afim de tornar esta intervenção desnecessária. Esta sociedade civil criou o ***Código Brasileiro de Autorregulamentação Publicitária***[7]. Muito embora o CONAR não faça parte da administração pública indireta e não tendo seus poderes e atribuições definidas em lei, o CONAR recebe denúncias de consumidores, de autoridades e de associados sobre violação do Código e aplica sanção administrativa, porém sem coerção legal.

Não nos parece adequado, s.m.j., que esse modelo seja estabelecido para o sistema fiscalizatório e sancionatório quanto à proteção dos dados pessoais por diversas razões. Primeira, a descentralização não é conveniente em um setor tão sensível que é a

[6] FADEL, Marcelo Costa. Breves Comentários ao Código de Auto-Regulamentação Publicitária do CONAR. *In: Revista do Direito do Consumidor,* vol. 50, abril – junho de 2004. pp. 153 – 170. p. 155.
[7] Disponível em: < http://www.conar.org.br/>, último acesso em 27 de novembro de 2015.

proteção de dados pessoais, pois fomentaria incertezas e insegurança no que diz respeito às regras e padrões éticos exigidos. Segunda razão, o próprio CONAR não tem poder de polícia, o que, caso seja criado esse conselho de autorregulamentação, poderá enfraquecer o sistema de proteção, tornando-o pouco eficaz na medida em que os titulares dos dados pessoais, para exercerem seus direitos deveriam recorrer necessária e exclusivamente ao Poder Judiciário, o que demandaria tempo e dinheiro. Não sendo, tão pouco, conveniente ao Judiciário que já está assoberbado pela quantidade das demandas (se considerarmos o volume de dados na sociedade informacional esses números aumentariam exponencialmente podendo até mesmo inviabilizar a eficiência do provimento jurisdicional). Terceira razão, não é totalmente confiável um sistema, no qual o ente que fiscaliza é composto por representantes fiscalizados. Em outras palavras, para a efetividade do sistema de proteção de dados, essa entidade deve ter absoluta independência funcional e autonomia financeira para que possa tomar decisões imparciais.

Entretanto, **no PL n. 5.276-A, há uma proposta a nosso ver mais interessante que é justamente a corregulação**, ou seja, essas entidades representativas dos responsáveis pelo tratamento de dados pessoais poderão elaborar "Códigos de Boas Práticas", submetidos ao órgão competente para avaliza-las. Um sistema que centraliza e confere maior segurança, pois estas regras são apreciadas por um único órgão imparcial.

3 Análise do Projeto de Lei n. 5.276-A, de 2016 (do Poder Executivo)

O Projeto de Lei n. 5.276-A, de 2016, é resultado de um longo processo democrático em que o texto foi submetido a consulta pública, período em que diversas entidades puderam colaborar lapidando e aprimorando conceitos técnicos, garantindo

princípios e direitos importantes, e, o mais relevante: preocupando com a efetividade do sistema de proteção de dados brasileiro.

Art. 2º do PL n. 5.276-A, de 2016 (do Poder Executivo): pelos mesmos argumentos antes expostos, não se deve confundir os conceitos de "dados pessoais" e "privacidade". Portanto, o *caput* deste artigo destaca, como fundamento da proteção de dados, a privacidade. Entretanto, como demonstrado *supra,* o dado ainda que público é objeto de proteção quando relativo a uma pessoa determinada ou determinável. Por isso, nem sempre a proteção de dados está fundada na tutela da privacidade, razão pela qual, a privacidade pode ser um dos fundamentos como os demais elencados nos incisos, em especial no inc. III do referido artigo; e não é "o fundamento" e nem o mais importante. Sugere-se a supressão da expressão "o respeito à privacidade e".

Art. 4º , inc. II do PL n. 5.276-A, de 2016 (do Poder Executivo), as regras de proteção de dados pessoais devem incidir também nas atividades jornalísticas, artísticas, literárias ou acadêmicas. Atualmente, por exemplo, o Regulamento Geral europeu de Proteção de Dados Pessoais (279/2016) não estabelece essa exceção de maneira absoluta. No art. 85 desse Regulamento, por exemplo, enfatiza a necessidade de conciliar a proteção de dados com as atividades jornalísticas, artísticas, literárias ou acadêmicas. Em outras palavras, a lei de proteção de dados se aplica, mas desde que não afete a liberdade de expressão para estas finalidades. Por exemplo, para uma reportagem coletar, tratar e disseminar dados pessoais requer-se o consentimento do titular. Ademais, no art. 89 desse Regulamento, fica estabelecido o princípio da minimização para a coleta, o tratamento e o compartilhamento de dados pessoais ainda que para fins de interesse público, científico, histórico e estatístico.

Assim, tendo em vista os inconvenientes e a falha do sistema de proteção de dados que tal exceção pode gerar, o melhor seria excluir o inc. II do art. 4º.

Art. 4º , § 3º do PL n. 5.276-A, de 2016 (do Poder Executivo), há uma confusão conceitual entre proteção de dados e privacidade novamente, sugere-se trocar a palavra "privacidade" por "proteção de dados".

Art. 5º , inciso IV, do PL n. 5.276-A, de 2016 (do Poder Executivo), o conceito de anonimização é, demasiadamente, complexo porque não é jurídico; antes, envolve conhecimentos tecnológicos. Nesse sentido, caberá ao órgão competente estabelecer critérios para se definir os padrões tecnológicos que assegurem a anonimização. Por isso, sugere-se fazer tal ressalva ao final do inciso: "segundo critérios e padrões técnicos a serem estabelecidos pelo órgão competente".

Art. 5º , inciso XII, do PL n. 5.276-A, de 2016 (do Poder Executivo), pelas mesmas razões, sugere-se a ressalva ao final do inciso: "segundo critérios e padrões técnicos a serem estabelecidos pelo órgão competente".

Art. 11, § 3º, do PL n. 5.276-A, de 2016 (do Poder Executivo), sobre o tratamento de dados para fins de investigação criminal e inteligência, defesa nacional, nos termos do art. 4º do PL n. 5.276-A, não se aplicaria a lei de proteção de dados pessoais. Entretanto, no art. 11, §3º, inciso III, autoriza o tratamento de dados sensíveis sem o consentimento do titular para pesquisa de investigação criminal. Parece-nos contraditório, se o próprio texto da lei exclui de seu âmbito de aplicação esta hipótese, não caberia regulamentá-la. Desta forma, sugere-se a compatibilização das normas.

Art. 13, § 3º, do PL n. 5.276-A, de 2016 (do Poder Executivo), novamente há uma confusão conceitual entre "dados pessoais" e "privacidade", sugere-se alterar a redação para *"[...], sem prejuízo do órgão competente poder solicitar ao responsável relatório de impacto à proteção de dados [e não como está à privacidade] referente aos riscos [...]"*.

Art. 32 do PL n. 5.276-A, de 2016 (do Poder Executivo), o mesmo ocorre no art. 32, sugere-se substituir "privacidade" por "proteção de dados pessoais": "[...] relatórios de impacto de proteção de dados e poderá [...]".

Em linhas gerais, dos 56 artigos do PL 5.276-A, 29 mencionam a atuação do órgão competente, sem contar os parágrafos e incisos, o que resultaria em aproximadamente 65 referências à atuação deste órgão. Em outras palavras, a criação e a atuação dessa entidade é fundamental para a efetiva proteção dos dados pessoais no Brasil. Portanto, é pacífico o entendimento de que este órgão deva ser criado, com autonomia financeira e independência institucional e que seja centralizado. Não seria adequado o modelo de autorregulação pelas razões acima expostas. O que se discute é o formato dessa entidade: órgão ou agência reguladora?

4 Modelo regulatório: órgão, agência e autorregulação

A *Convenção de Estrasburgo,* de 28 de janeiro de 1981, conhecida como *Convenção n. 108,* teve por objetivo a disciplina da matéria com vistas à efetiva proteção dos dados pessoais de todo ser humano independentemente do local de sua residência, para tanto foi idealizado a criação de um órgão independente e autônomo para fiscalizar e zelar pelo cumprimento das regras sobre proteção de dados. Vinte anos depois da *Convenção n. 108,* o importante papel desse órgão foi amplamente discutido, o que determinou a emenda desta *Convenção* em 2001, para acrescentar regras mais específicas e detalhadas sobre a atuação daquele órgão[8]. Em suma, concluiu-se pela obrigatoriedade

[8] Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows. Disponível em: < https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168008c2b8>, acessada em 20 de novembro de 2015.

de cada país signatário em criar uma *Authority,* bem como algumas missões desta entidade. Uma das missões é a colaboração com outras *Authorities* de outros países para que seja eficaz a proteção dos dados pessoais, isto é, a missão de estabelecer mecanismos de *enforcement* para as leis nacionais de proteção de dados.[9]

Com destaque o art. 8º da *European Charter of Fundamental Rights*, ao citar a proteção de dados pessoais como direito fundamental, ressalta a criação de uma autoridade.[10]

Em 1995, a Diretiva n. 46 estabeleceu um modelo de proteção de dados pessoais para ser transposta pelos Estados-membros, prevendo, no art. 28, a criação de uma entidade independente com a missão precípua de controlar e fiscalizar a aplicação da lei de proteção de dados. E essa entidade foi mantida no atual *Regulamento Geral de Proteção de Dados* (279/2016), arts. 51 a 59.

Desta forma, é interessante analisarmos a experiência de alguns países que já tem um órgão responsável pela efetividade dos respectivos sistemas de proteção de dados para se poder chegar a uma conclusão para o Brasil.

Na Itália, a *Autorità Garante della Privacy e dei Dati Personali* é um órgão da administração pública direta, porém independente, composto por dois deputados e dois senadores (eleitos para um mandato de sete anos não renovável e não indicados), favorecendo o mais amplo debate e priorizando candidatos, que detêm notório saber em direito e informática, muito embora não haja nenhuma especificação profissional. Não nos parece o modelo mais aconselhável no Brasil, porque se nota uma forte influência

[9] LIMA, Cíntia Rosa Pereira de. *A imprescindibilidade de um órgão independente para a efetiva proteção dos dados pessoais no cenário futuro do Brasil.* Tese de Livre Docência Apresentada à Faculdade de Direito de Ribeirão Preto. Ribeirão Preto, 2015. 487 fls.

[10] Disponível em: < http://www.europarl.europa.eu/charter/pdf/text_en.pdf>, último acesso em 27 de novembro de 2015.

institucional, sendo essa a maior crítica a esse modelo, pois compromete a imparcialidade uma vez que o órgão público fiscaliza a si próprio.

Na França, a *Commission Nationale de l'Informatique et des Libertés* (CNIL) tem a missão de proteger os dados pessoais mediante a fiscalização pelo correto cumprimento da lei francesa de proteção de dados. A Lei *Informatique et Libertès* no Capítulo III (arts. 11 a 21) estabelece os deveres, a composição e o funcionamento desse órgão. As missões institucionais da CNIL podem ser sintetizadas como: informar, proteger, regulamentar, aplicar sanções, controlar e fiscalizar, bem como compreender e antecipar as inovações tecnológicas para que seja garantida tanto a eficácia da proteção dos dados pessoais, quanto à adoção de padrões tecnológicos e administrativos de segurança.

Esse órgão apresenta uma composição mais extensa do que a *Autorità Garante* italiana (composta de 04 membros). A CNIL é composta por 17 comissários, dentre os quais: quatro parlamentares (dois deputados e dois senadores); dois membros do *Conseil Économique, Social et Environnemental;* seis representantes dos tribunais superiores (dois conselheiros do Estado, dois da *Cour de Cassation* e dois da *Cour des Comptes)*; o Presidente da *Assemblée Nationale* e o Presidente do Senado; e três personalidades serão indicadas por decreto. Estas personalidades são especialistas com notável saber em informática.

Esses membros tem um mandato de cinco anos ou até quando durar o mandato político quando for o caso. E o Presidente da CNIL é eleito pelos seus conselheiros. Atualmente, a Presidente da CNIL é Isabelle Falque-Pierrotin, que também assume a presidência do *WP29*[11]. Além destas fiscalizações, a CNIL tem poder regulamentar através de deliberações em diversos temas como aqueles referentes à geolocalização, Internet, dados sanitários, financiários e etc. Por fim, destaca-se o papel

[11] Este é o grupo de trabalhos instituído pelo art. 29 da Dir. 95/46/CE, vide cap. 2.

da CNIL na resolução de conflitos administrativamente, assegurando o contraditório e ampla defesa, cabendo recurso ao Conselho de Estado.

Na Espanha, a *Agencia Española de Protección de Datos (AEPD)* foi criada pelo Decreto Real n. 428 de 26 de março de 1993. Posteriormente, em 13 de dezembro de 1999, sobreveio a Lei Orgânica n. 15, com a finalidade de adequar as atribuições deste órgão ao Direito Comunitário Europeu, especificamente, no Título VI (arts. 35 a 42). Essa entidade é um órgão independente e especializado cuja missão precípua é zelar pelo cumprimento das disposições da Lei Orgânica de Proteção de Dados e garantir o direito de informação, de acesso, de retificação, oposição e cancelamento dos dados, tida como a autoridade de controle máxima quanto à proteção de dados pessoais. Nos termos do art. 35 da LOPD, é um ente de direito público, com personalidade jurídica própria e com plena independência, regida pelo Estatuto Próprio que é o referido Decreto Real n. 428, de 26 de março de 1993, ainda em vigor naquilo que não contraria os dispositivos da LOPD. Posteriormente, este Decreto Real foi ratificado em 17 de outubro de 2008 pelo Decreto Real n. 1665. As atribuições desse órgão estão expressamente descritas no art. 37 da LOPD, que podem ser sintetizadas como controle e vigilância, autorização, informação, investigação, sanção e regulação.

Quanto à estrutura, a AEPD é presidida pelo Diretor indicado por Decreto Real dentre os membros do *Conselho Consultivo* (art. 36 da LOPD). Assim, a AEPD é composta por vários órgãos, quais sejam: o *Conselho Consultivo* (art. 38 da LOPD), com nove membros, entre os quais, um deputado, um senador, um representante da Administração Central designado pelo Governo, um representante da Administração Local indicado pela Federação Espanhola dos Municípios e Províncias, um membro da Academia Real de História por ela indicado, um especialista na matéria indicado pelo Conselho Superior das Universidades, um representante dos usuários e consumidores

indicado como prevê o regimento, um representante da Comunidade Autônoma[12] e um representante do setor dos bancos de dados privados, cada qual com mandato de quatro anos; o *Registro Geral de Proteção de Dados*; a *Inspeção de Dados*; e a *Secretaria*, todos descritos no Estatuto da AEPD (Decreto Real n. 428, de 26 de março de 1993).

O *Privacy Commissioner* canadense é definido como "*ombudsman*" ("ouvidor") que é um membro do Parlamento (*House of Commons* e Senado), cuja competência se restringe, exclusivamente, à proteção dos dados pessoais e privacidade, como por exemplo, direito de acesso à informação, investigação, publicação de informativos e promoção de *findings* sobre determinados temas relacionados à sua esfera de atuação. A crítica desse modelo é a falta de poder de polícia e, por isso, no Canadá já se está promovendo a ampliação dos poderes desse órgão para garantir um nível adequado de proteção de dados.

Nos Estados Unidos, a *Federal Trade Commission* tem exercido uma função semelhante à das agências acima mencionadas, no que diz respeito à fiscalização e controle dos princípios de proteção de dados denominados *Shield*. Além disso, o *FTC* tem recomendado ao Congresso leis sobre o tema e também monitora as práticas das empresas, bem como tem aplicado multas sempre na defesa dos consumidores.

Quanto à estrutura, o *FTC* é composto por cinco *Commissioners* indicados pelo Presidente e confirmados pelo Senado, com mandato de sete anos, sendo que durante este período estes não podem ser removidos da função a menos que tenham sido ineficientes ou negligentes em suas funções. Dentre suas funções estão: a investigatória, regulatória e decisória.[13]

[12] A agência da Comunidade de Madrid é a única agência autônoma espanhola. Vide: ONTOSO, Rosa Maria García. Protección de Datos en las Comunidades Autónomas. *In:* REILLY, Marcelo Bauzá; MATA, Federico Bueno de. (coord.) *El derecho en la sociedad telemática.* Santiago de Compostela: Andavira, 2012. pp. 215 – 230. p. 221.

[13] SOLOVE, Daniel J. and Hartzog, Woodrow. The FTC and the New Common Law of Privacy (August 15, 2013). v. 114 *In: Columbia Law Review, pp.* 583-676 (2014); Disponível em:

Na Argentina, a Lei n. 25.326, de 04 de outubro de 2000, denominada "*Ley de Protección de los Datos Personales*", disciplina a proteção de dados neste país. No art. 29 dessa lei, criou-se a *Dirección Nacional de Protección de Datos Personales*, atribuindo-lhe as seguintes funções: a) de auxiliar e assessor as pessoas que solicitarem dentro do escopo da lei; b) de estabelecer normas e regulamentos sobre proteção de dados; c) de manter um repertório com informações de todas as bases de dados, arquivos e registros que coletam e tratam dados pessoais; d) fiscalizar a observância dessa lei, podendo, para tanto, solicitar autorização judicial para ter acesso a equipamentos, locais e programas de tratamento de dados; e) solicitar informações de entidades públicas e privadas sobre as respectivas atividades de coleta, armazenamento e tratamento de dados pessoais; f) impor sanções administrativas quando houver violação a esta lei; g) ingressar como querelante em ações penais, cujo objetivo seja a imposição de sanção penal por violação a esta lei; e h) controlar o cumprimento dos requisitos e garantias que os agentes, responsáveis pela coleta e pelo tratamento de dados, devam adotar.

Quanto à estrutura, esse órgão atua no âmbito do Ministério da Justiça e Direitos Humanos, porém com autonomia e independência. É presidido por um Diretor indicado pelo Presidente da República e aprovado pelo Senado, com mandato de quatro anos. A crítica que se faz a esse sistema é o comprometimento da sua imparcialidade tendo em vista ser um órgão público e que deverá, também, fiscalizar o Ministério a que faz parte.

3.1 Órgão competente e do Conselho Nacional de Proteção de Dados e da Privacidade

SSRN: http://ssrn.com/abstract=2312913 or http://dx.doi.org/10.2139/ssrn.2312913. Acesso em: 15 de agosto de 2014. p. 608.

No Brasil, a agência reguladora é um ente da administração pública indireta, constituída na modalidade de autarquia de regime especial. Muito embora seja um órgão independente, está vinculada ao Ministério competente para tratar da respectiva atividade. Seus integrantes tem um mandato fixo (de três a quatro anos) o que lhes garante maior segurança em sua atuação. Consoante as atribuições estabelecidas no art. 53 do PL 5.276-A, ***parece-nos imperiosa a criação de uma agência reguladora federal para a proteção de dados pessoais como defendemos na tese de Livre Docência defendida na Faculdade de Direito de Ribeirão Preto da Universidade de São Paulo (2016)***.

Assim, tendo sido apresentado o PL 5.276-A pelo Poder Executivo, é plenamente viável a criação desse órgão, que pode vir posteriormente através de um decreto. Entretanto, ***o mais aconselhável seria a não vinculação desse órgão a nenhum Ministério para assegurar a sua completa independência e autonomia como já afirmamos na referida tese, sendo que tais prerrogativas devem ser garantidas em lei***. A vantagem deste modelo é a independência em relação ao Poder Público, ou seja, as agências têm plena autonomia político-administrativa e econômico-financeira, fundamentais para o melhor exercício das funções atribuídas.

Quanto à estrutura, o Diretor da agência seria eleito dentre os membros do conselho consultivo, com mandato de 02 (dois) anos, podendo ser eleito por mais um mandato. E o Conselho Consultivo seria o *Conselho Nacional de Proteção de Dados Pessoais e da Privacidade,* previsto no art. 54 do PL n. 5.276-A, caracterizado por ser multissetorial, favorecendo a participação de diversos setores da sociedade.

Por fim, cabe destacar que o PL 5.276-A estabelece um **modelo de corregulação**, pois os arts. 50 e 51 estabelecem a possibilidade de elaboração de normas deontológicas, ou seja, "Códigos de Boas Práticas" pelos responsáveis pelo tratamento de dados pessoais a serem apreciados e chancelados pelo órgão competente, mantendo a centralização dessa importante função, favorecendo a segurança jurídica.

Quanto ao custeio das agências reguladoras, importante ressalvar que o seu **custeio** não pode vir da aplicação das multas. Estas quando aplicadas, assegurados o contraditório e a ampla defesa, não devem ser destinadas à manutenção do órgão para evitar qualquer interesse financeiro por parte da agência quanto à aplicação desta sanção. O ideal seria a lei já estabelecer que estes valores deveriam ser destinados às políticas públicas sobre proteção de dados pessoais e às pesquisas científicas nessa área.

Assim, a lei deveria criar uma agência reguladora em nível federal, estabelecendo uma tarifa a ser paga pelas empresas, que tratam dados pessoais conforme uma porcentagem do capital de cada empresa.

Era o que nos cabia destacar. Desde já parabenizando a Comissão Especial de Tratamento de Dados Pessoais, na pessoa da Excelentíssima Presidente, Deputada Bruna Furlan (PSDB) e do Excelentíssimo Relator, Deputado Orlando Silva (PCdoB), que assumiu destemidamente a árdua tarefa de sintetizar um projeto de lei de tamanha complexidade.

Desde já nos colocamos à disposição para os esclarecimentos que, por ventura, forem necessários.

Ribeirão Preto, 02 de junho de 2017.

Cíntia Rosa Pereira de Lima

Professora Livre-Docente em Direito Civil
Faculdade de Direito de Ribeirão Preto
Universidade de São Paulo