PARECER Nº , DE 2017

Da COMISSÃO DE ASSUNTOS ECONÔMICOS, sobre o Projeto de Lei do Senado nº 330, de 2013, do Senador Antonio Carlos Valadares, que *dispõe sobre a proteção, o tratamento e o uso dos dados pessoais, e dá outras providências*, sobre o Projeto de Lei do Senado nº 131, de 2014, de autoria da Comissão Parlamentar de Inquérito da Espionagem (CPIDAESP), que *dispõe sobre o fornecimento de dados de cidadãos ou empresas brasileiros a organismos estrangeiros*, e sobre o Projeto de Lei do Senado nº 181, de 2014, do Senador Vital do Rêgo, que *estabelece princípios, garantias, direitos e obrigações referentes à proteção de dados pessoais.*

Relator: Senador **RICARDO FERRAÇO**

I – RELATÓRIO

Chegam para exame desta Comissão os Projetos de Lei do Senado (PLS) **nº 330, de 2013**, do Senador Antonio Carlos Valadares; **nº 131, de 2014**, de autoria da Comissão Parlamentar de Inquérito da Espionagem (CPIDAESP); **e nº 181, de 2014**, do Senador Vital do Rêgo, os quais tramitam em conjunto após a aprovação dos Requerimentos nº 992 a 998, ambos de 2014.

Diante da aprovação desses requerimentos, os projetos foram encaminhados para o exame da Comissão de Ciência, Tecnologia, Inovação, Comunicação e Informática (CCT), da Comissão de Meio ambiente, Defesa do Consumidor e Fiscalização e Controle (CMA), desta Comissão de Assuntos

Econômicos (CAE) e, após, seguirão para a instrução da Comissão de Constituição e Justiça (CCJ) e, então, deliberação pelo Plenário desta Casa.

Perante a CCT e a CMA, as matérias foram relatadas pelo então Senador Aloysio Nunes Ferreira, atualmente no exercício do cargo de Ministro de Estado das Relações Exteriores. Seu relatório legislativo, perante a CCT, concluiu pela apresentação de uma Emenda Substitutiva, adotada em parecer unânime daquela Comissão, inclusive incorporando diversas emendas apresentas por outros parlamentares.

Novamente relator da matéria perante a CMA, o hoje Chanceler Aloysio Nunes Ferreira opinou pela aprovação do PLS 330, de 2013, nos termos do substitutivo de sua lavra aprovado na CCT, e, ainda, pela declaração de prejudicialidade das demais proposições apensadas.

Importante destacar que as matérias foram instruídas por duas audiências públicas, com a presença de especialistas, representantes da sociedade civil e do governo federal, realizadas em 02/12/2014 e, novamente, em 18/08/2015.

Por fim, em 14/07/2016, foram apresentadas a Emenda nº 32 e as Subemendas nºs 1 e 2 à Emenda nº 31-CCT-CMA, de autoria da senadora Marta Suplicy.

É o que se tem a relatar.

II – ANÁLISE

Nos termos do art. 99, do Regimento Interno do Senado Federal (RISF), compete à Comissão de Assuntos Econômicos (CAE) opinar sobre "aspecto econômico e financeiro de qualquer matéria que lhe seja submetida" (inc. I) e também sobre "proposições pertinentes aos problemas econômicos do país" (inc. III).

Inicialmente, entendemos não haver qualquer vício de constitucionalidade, juridicidade e regimentalidade, o que será mais propriamente analisado quando da oitiva pela Comissão de Constituição e Justiça desta Casa.

Ainda assim, temos que a **iniciativa legislativa** seja adequada, uma vez que compete à União legislar privativamente sobre direito civil (art. 22, inc. I, da Constituição Federal), entre os quais se insere o direito à personalidade, e concorrentemente sobre responsabilidade por dano ao consumidor (art. 24, inc. VIII).

No mais, pelo conteúdo proposto, não se verifica violação à reserva de iniciativa em razão de propositura parlamentar da matéria. Também a opção pela **espécie normativa** de lei ordinária compatibiliza-se com o espectro constitucional, não havendo ferimento a cláusula de reserva de lei complementar ou de emenda constitucional reformadora na normatização do tema ora em análise não havendo qualquer ofensa em relação às limitações formais ao processo legislativo infraconstitucional.

Quanto ao mérito, reconhecemos a importância ímpar do projeto.

As matérias ora em apreciação versam sobre temática das mais relevantes atualmente, tendo em vista a sociedade informacional em que vivemos. O dado pessoal, para muito além da discussão de fundo constitucional, é hoje considerado um dos mais importantes ativos para o exercício da atividade empresarial. E não somente isso: um elemento fundamental até mesmo para a concretização de políticas públicas, dado o elevado grau de informatização e sistematização do Estado brasileiro, em todos os níveis federativos.

Vivemos hoje uma economia maciçamente baseada em dados (*data driven economy*), em que informações sobre todos os aspectos das relações humanas, inclusive da personalidade dos indivíduos, estão sendo coletados, armazenados e processados como nunca antes fora possível. A todo momento, pessoas, conscientemente ou não, oferecem a um número crescente de empresas – com tecnologia adequada – dados sobre quem são, o que estão fazendo, onde estão, sobre o que falam ou com quem interagem.

E, movida pelo interesse de descobrir cada vez mais informações sobre o indivíduo e com maior grau de precisão, o financiamento a novas tecnologias de processamento de dados tem permitido uma evolução a passos largos: algoritmos extremamente sofisticados já são capazes de interpretar dados a ponto de compreender e catalogar opiniões e preferências pessoais. Máquinas estão ficando “inteligentes”, aptas a solucionar problemas complexos e realizar tarefas básicas com significativo grau de autonomia e precisão – não

por outra razão, a pauta da empregabilidade humana face à evolução tecnológica já é habitual na mídia e no meio acadêmico.

Esse contexto explica porque algumas das companhias que mais têm valor de mercado, hoje, ao redor do mundo, têm como principal ativo os dados de seus consumidores, superando setores tradicionais da economia.

Ora, através dessas informações e com a tecnologia necessária, uma empresa é capaz de traçar cenários comportamentais e identificar traços psicológicos reveladores da personalidade humana. A privacidade, então, se torna um divisor de águas, porque a mitigação em torno de sua proteção viabiliza manipulações sociais em larga escala. Por isso, o uso indevido desses dados pode representar uma grave violação dos preceitos constitucionais que garantem a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas.

Há décadas, a comunidade internacional tem-se mobilizado em discussões sobre a preservação da privacidade e da intimidade de seus cidadãos, justamente em razão da exposição pessoal decorrente do consumo irrefreável de produtos e serviços a partir da tecnologia digital.

Nesse sentido, o Conselho de Direitos Humanos da Organização das Nações Unidas (ONU) já reconheceu, desde 1966, a proteção de dados pessoais como um elemento fundamental da privacidade, ao consagrar esse tema como um direito previsto no artigo 17, do Pacto Internacional sobre Direitos Civis e Políticos. Posteriormente, essa norma foi complementada pelo Comentário Geral nº 16, da Compilação de Instrumentos Internacionais de Direitos Humanos[1], que é taxativo quanto à necessidade de proteção dos dados pessoais face ao avanço tecnológico.[2]

[1] Disponível em: http://www.refworld.org/docid/453883f922.html.

[2] "A coleta e a manutenção de informações pessoais em computadores, bancos de dados e outros dispositivos, seja por autoridades públicas ou entidades privadas, devem ser reguladas por lei. Medidas eficazes devem ser tomadas pelos Estados para garantir que as informações relativas à vida privada de uma pessoa não cheguem às mãos de pessoas que não são autorizadas por lei a recebê-las, processá-las e usá-las, e nunca serão usadas para fins incompatíveis com o Pacto."

O assunto progrediu em torno de discussões especialmente voltadas para o fluxo transnacional dos dados, na medida em que a tecnologia da informação cumpria seu desiderato: eliminar fronteiras.

Em 1990, a Organização das Nações Unidas adotou, através de sua Assembleia Geral, a Resolução nº 45, contendo as "Diretrizes para a regulação de arquivos computadorizados de dados pessoais". São, ao todo, 10 princípios: (i) legalidade e equidade; (ii) exatidão; (iii) finalidade específica; (iv) acesso a pessoa interessada; (v) não discriminação; (vi) exceções facultativas; (vii) segurança de dados; (viii) fiscalização e sanção; (ix) fluxos transfronteiriços de dados; e (x) âmbito de aplicação[3].

Na esteira desse movimento internacional, a então Comunidade Europeia editou, em 1996, a Diretiva nº 46[4], com o propósito de regular o processamento de dados pessoais no âmbito da União Europeia. Cumpre destacar que essa norma fora recentemente sucedida pela Regulação Geral de Proteção de Dado (*GDPR*[5]), adotada em abril de 2016, que entrará em vigor a partir de maio de 2018. Sua matriz reside no conceito em torno da robustez do direito à privacidade, presente em diversos tratados sobre direitos humanos.

Em março de 2012, a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) publicou suas "Diretrizes que regem a proteção da privacidade e dos fluxos transfronteiriços de dados pessoais"[6]. Referido documento consagrou, também, princípios de regulação de dados pessoais, com o objetivo de sugerir a harmonização das legislações nacionais de seus membros em matéria de privacidade, a saber: (1) limitação de coleta; (2) qualidade dos dados; (3) definição da finalidade; (4) limitação de utilização; (5) cópia de segurança; (6) abertura; (7) participação do indivíduo; e (8) responsabilização.

Ainda em 2012, a Organização dos Estados Americanos (OEA), através de seu Comitê Jurídico Interamericano, editou uma "Proposta de

[3] Disponível em: http://www.un.org/documents/ga/res/45/a45r095.htm.
[4] 95/46/EC.
[5] General Data Protection Regulation
[6] Disponível em: http://www.oecd.org/sti/ieconomy/15590254.pdf.

Declaração de Princípios para Privacidade e Proteção de Dados Pessoais nas Américas", em sua 80ª Sessão Ordinária na Cidade do México.

O que se nota é que disposições sobre privacidade, proteção da honra e da dignidade pessoal, liberdade de expressão e associação e o livre fluxo de informações são encontradas nos principais sistemas de direitos humanos do mundo. Sua matriz normativa, via de regra, têm sido normas constitucionais: daí a necessidade de se analisar a questão sob a ótica defensiva dos direitos fundamentais.

Por outro lado, não há dúvida quanto à importância do dado pessoal para o desenvolvimento econômico global. O progresso tecnológico, as novas relações de mercado e consumo, o redesenho da escala mundial de produção estão intimamente ligados ao tratamento de dados, inclusive pessoais.

O desafio à frente, portanto, no que diz respeito à edição de um marco regulatório protetivo, é precisamente equilibrar, através da construção de um texto propositivo e sensato, os interesses sociais e os interesses econômicos, que de forma alguma podem se antagonizar. Pelo contrário, por definição, devem ser interesses absolutamente compatíveis e complementares entre si.

Não somente isso: busca-se, ainda, harmonizar o interesse público e o privado, seja estimulando o uso racional e eficaz das informações, inclusive pelo Estado, seja preservando direitos e garantias fundamentais do cidadão.

A questão perpassa vários cenários de preocupação, não se limitando a divagações sobre os limites do tratamento de dados, nem quais seriam os procedimentos mais justos de coleta. Existe uma inquietude permanente entre os especialistas acerca da efetiva segurança dos dados armazenados, tanto sob o viés da responsabilidade civil de agentes privados, como públicos, uma vez que o marco regulatório ora proposto aplicar-se-á, em grande parte, também, sobre o Estado.

Aliás, a coleta, o armazenamento e o tratamento desses dados, quando realizados pelos setores públicos, deve ser ainda mais proximamente monitorado, face a inescapabilidade do cidadão quanto à coleta e o uso públicos de seus dados, e diante das ameaças em torno da segurança e preservação desses dados.

Apenas para que se tenha a dimensão social dos riscos, em 2016, foi criada a identidade única na Índia, o *Aadhaar*, um número composto por 12 dígitos, disponibilizado pelo Governo indiano, que registra a identificação pessoal, a partir de dados biométricos e demográficos de mais de 1 bilhão de indianos. O órgão responsável pela coleta e armazenamento desses dados é a recém-criada Autoridade de Identificação Única da Índia, vinculada ao Ministério de Eletrônica e de Tecnologia da Informação. Até agora, mais de 99% da população indiana com mais de 18 anos foram cadastrados com essa identificação única, tornando-o o maior sistema de identificação biométrica de que se tem notícia. Isso significa, em termos práticos, que o Governo indiano possui a maior base de dados biométricos do mundo, sendo inevitavelmente um alvo permanente para a atuação de criminosos cibernéticos.

Noutro giro, especialistas em segurança da informação têm revelando, através da mídia, casos emblemáticos de vazamento de dados: em 2015, por exemplo, cerca de 191 milhões de registros de informações pessoais de eleitores americanos foram expostos na internet, armazenados em um banco de dados – com erros de configuração – contendo 300 *Gigabytes* de informações, sem nenhum indício do responsável pela falha de segurança. Os dados revelavam um grande número de atributos dos eleitores, como nome completo, endereço residencial, e-mail, número de identidade, número de eleitor, sexo, data de nascimento, número de telefone, filiação partidária e histórico de votação desde 2000.

Mais recentemente, um caso similar foi levado ao Judiciário: segundo noticiado pela imprensa, uma empresa americana, especializada em análise de dados, fora contratada por um Partido político daquele país, em 2016, mas não teria zelado pela segurança da base de dados contendo informações sobre mais de 60% da população nacional. Valendo-se de armazenamento na nuvem, a empresa não teria protegido a base de dados com senha, permitindo que informações de mais de 198 milhões de eleitores estivessem acessíveis publicamente. Em razão do episódio, a companhia está sendo processada, perante a Corte de Justiça da Flórida, em uma ação em que se pede indenização de 5 milhões de dólares a título de danos coletivos.

O que se constata, na verdade, é que episódios de falha de segurança de dados são frequentes e progressivos. E essa não é a única preocupação, pois, de um lado, se há falhas na proteção e dados armazenados, nada impede que haja desvirtuamento na coleta e no tratamento. Esse cenário

exige do Estado atuação firme na proteção dos direitos fundamentais dos cidadãos.

Por essas razões, sem desprezar o trabalho realizado nas Comissões antecessoras, abrimos espaço, através de nosso gabinete, para receber contribuições de todos os setores direta ou indiretamente interessados na discussão, inclusive do Governo federal. Tivemos registro de mais de 1.330 laudas de colaborações técnicas, sobre as quais nos debruçamos, com as conclusões que passamos a expor.

A par das discussões no âmbito senatorial, tramita, também, perante a Câmara dos Deputados, projeto de lei de iniciativa do Poder Executivo (PL 5276, de 2016), propondo disciplinar a mesma matéria. Referida proposição há de ser considerada, na presente análise, em razão de sua legitimidade, na medida em que é fruto de consultas públicas, realizadas perante o Ministério da Justiça, em se colheram milhares de sugestões da sociedade civil. Passemos, assim, às alterações ora propostas.

Fundamentos da regulação dos dados pessoais

É de se notar que o marco regulatório de proteção e dados pessoais, ora em exame, tem como fundamento (art. 1º): “o princípio da dignidade da pessoa humana, a proteção da privacidade, a garantia da liberdade e a inviolabilidade da honra e da imagem das pessoas. ” No entanto, parece-nos equivocado regular essa questão somente sob a ótica protecionista dos direitos de personalidade, quando, efetivamente, temos aqui o desafio de regular, também, o uso econômico – legítimo, proporcional e razoável – dessas informações.

Aliás, é inquestionável que o viés protetivo da privacidade pessoal deva ser a força motriz da norma, mas não pode ser a única. A matriz de direitos que rege as relações públicas e privadas decorrentes do tratamento de dados pessoais também comporta o uso econômico dessas informações, daí sendo razoável elencar, entre os fundamentos do marco regulatório, normas fundamentais de proteção à ordem constitucional econômica, como a defesa do consumidor e o princípio da livre iniciativa – fundamento, aliás, do próprio Estado brasileiro.

A incorporação desse tema, na invocação principiológica, atende a uma percepção objetiva: ao longo de todo o texto, observa-se que o destinatário primário da regulação são as empresas privadas, por decorrência do exercício de suas atividades econômicas, e o setor público, quando voltado ao tratamento dos dados para a consecução das funções constitucionais do Estado. Ademais, a questão projeta-se para além das fronteiras nacionais, atraindo, em algum momento, o debate em torno da livre circulação de dados pessoais como fase sucedânea da integração econômica clássica (que, hoje, pressupõe a livre circulação de bens, serviços e fatores produtivos), tal como já se verifica no bloco econômico europeu, face à conectividade digital.

Por essa razão, propomos **Emenda** ao art. 1º, a fim de reverberar, também na presente lei, o objetivo de convivência normativa entre esses princípios fundamentais elencados na Constituição Federal.

Especialidade da norma legal

A fim de mitigar discussões doutrinárias e jurisprudenciais acerca da aplicabilidade da presente norma face a possíveis antinomias jurídicas, propomos **Emenda** ao art. 1º, visando estabelecer a prevalência deste marco regulatório face a outras normas legais de amplitude genérica: uma aplicação normativa cogente do princípio da especialidade.

A proposta aqui formulada atende aos anseios de aplicabilidade específica e objetiva do marco regulatório, ainda que incidentes outras legislações disciplinadoras das relações jurídicas, como o Código de Defesa do Consumidor. Dessa maneira, assegura-se um mínimo de paridade da norma geral brasileira de proteção de dados pessoais face à necessidade inafastável de adequação internacional nesse mesmo contexto.

Aplicabilidade da norma

Outro aspecto que deve ser revisto, no texto já deliberado pela CCT, refere-se à exceção de aplicabilidade da lei geral quanto ao uso dos dados para a finalidade de segurança pública.

Concordamos com a proposta apresentada pelo PL 5276, de 2016, no sentido de que devam essas regras serem disciplinadas por lei própria, diversa do presente marco regulatório. No entanto, o simples afastamento

dessas regras por cláusula de exceção abre espaço para, enquanto perdurar a omissão legislativa, não haver qualquer proteção mais específica, na medida em que as presentes normas deixarão se serem aplicadas até a superveniência de lei própria.

Em vista disso, propomos, na forma de **Emenda**, uma solução intermediária, em grande parte inspirados na nova proposta regulatória europeia.

Redundância redacional quanto aos dados anonimizados

O Substitutivo da CCT pode ser ainda adequado quanto à técnica legislativa em alguns pontos. No que tange às normas reguladoras dos chamados dados anônimos, dissociados ou simplesmente anonimizados, observamos um excesso de zelo, que acaba por ferir as regras gerais de redação legislativa, em razão das redundâncias conceituais. Em vista disso, propomos, na forma de **Emenda**, de redação.

Conceito de dados pessoais

Esse ponto revela grande consternação social. Isso porque a definição autêntica sobre termos regulados em norma jurídica pode atrair ou repelir toda a incidência normativa sobre o fato social. Daí a necessidade de se estabelecer uma conceituação legal adequada, justa e restritiva, a fim de não dar margem à insegurança jurídica e à própria exequibilidade legislativa.

Nesse sentido, a Emenda Substitutiva nº 31 - CCT/CMA propôs uma definição para dado pessoal bastante similar à proposta pelo PL 5276, de 2016.

Ora, os dados pessoais, para que se tornem merecedores de proteção legal, devem funcionar como identificadores, seja por sua característica ou natureza em, diretamente, distinguir um indivíduo dos demais, seja por sua capacidade de assim o fazer, uma vez tratados e interpretados. Ex: o nome de uma pessoa é capaz, na maioria das vezes, de permitir diretamente sua identificação. A placa de seu veículo, porém, não. No entanto, associando-se a placa ao nome, é possível identifica-la perante terceiros. O mesmo se dá com outros dados, como a cor do veículo ou sua geolocalização: uma informação que não tem condições, à primeira vista, de permitir a identificação do indivíduo. Porém, associando-se tais dados à placa, que já estava associada ao nome,

tem-se aí um conjunto de identificadores de pessoa natural.[7] O próprio Marco Civil da Internet, em seu decreto regulamentador, apresenta essa proposta, aliás, em similaridade redacional ao PL 5276, de 2016.

A proposta do Substitutivo da CCT, no entanto, não enumera as espécies de dados que entende como pessoais, tal como o PL do Poder Executivo faz. À primeira vista, poder-se-ia concluir tratar-se de mero capricho redacional, na medida em que os tipos legalmente estabelecidos na norma não são taxativos, mas meramente exemplificativos. Porém, face à liberdade hermenêutica, parece-nos prudente especificar, ainda que pelo método exemplificativo, alguns tipos, com o objetivo de conferir maior segurança jurídica. Sugerimos, assim, uma **Emenda**, para incluir os números identificadores, dados locacionais, identificadores eletrônicos.

Em uma análise sobre as normas internacionais de proteção de dados, observamos uma tendência legislativa de qualificar o titular dos dados entre o indivíduo "identificado" e "identificável". Porém, algumas variações mostraram-se interessantes, sob a lógica aqui proposta: a lei protetiva de dados pessoais da Austrália, por exemplo, define o dado pessoal como a informação pessoal sobre um indivíduo identificado ou razoavelmente identificável, o que representa uma singela, mas eficaz, mudança propositiva. Por essa proposta, não basta que o dado esteja apto a identificar a pessoa, mas é preciso que essa aptidão seja razoavelmente constatada. No exemplo acima, a cor do veículo não torna uma pessoa a ela relacionada identificável. Mas a cor do veículo, associada à placa, sim. São cenários distintos, que variam conforme o tratamento do dado coletado.

Transferência internacional de dados a organizações internacionais

O texto, fatalmente, deixou de prever uma realidade já concreta e devidamente regulada em normas de outros Países, inclusive na Regulação Geral de Dados Pessoais da União Europeia: a transferência internacional de dados para organismos internacionais.

Nesse regime proposto, inicialmente, sugerimos mudanças dos termos de equivalência de proteção para termos de adequação – um grau menos

[7] Fenômeno das combinações únicas.

restritivo, porém ainda suficiente a assegurar os direitos do titular dos dados. Essa proposta, inclusive, alinha-se ao modelo legislativo adotado pela RGPD europeia (ar.t 45).

Autoridade Nacional de Proteção de Dados

Um dos pontos mais importantes em torno dessa questão é a criação da autoridade central de fiscalização das regulações de dados pessoais. Lamentavelmente, o projeto de lei encaminhado pelo Poder Executivo à Câmara dos Deputados não trouxe a necessária e indispensável previsão normativa, o que inviabiliza por completo, face à reserva de iniciativa constitucional[8], que o Congresso Nacional possa fazê-lo, ainda que por meio de emendas àquela proposição e inclusive na presente proposição, apresentada pelo nobre Senador Antonio Carlos Valadares.

O contexto político e econômico que então permeava o cenário histórico brasileiro não permitia, e ainda não permite, hoje, que se proponha mais aumentos de gastos públicos. No entanto, estamos diante de um dilema moral e político-econômico: a ausência de previsão de uma autoridade central de dados pessoais fatalmente impedirá que o Brasil, ainda que aprovado seu marco regulatório, seja considerado um país com grau de adequação às normas internacionais congêneres. A própria Diretiva 95/46/CE estabelece a necessidade inafastável de os Países membros atribuírem, em suas legislações nacionais, a uma ou mais autoridades públicas, dotadas de independência, competência para supervisionar o cumprimento da norma protetiva europeia.

Por isso, registramos, neste parecer, a consideração que o Congresso Nacional tem sobre a importância dessa previsão, de maneira que o Poder Executivo encontre uma solução possível, sem impacto orçamentário, através do remanejamento de rubricas orçamentárias disponíveis, para sua própria criação desse órgão federal.

Entendemos, assim, que uma solução legislativa provisória, face ainda à continuidade do debate inclusive na Câmara dos Deputados, seria conferir a autorização legislativa para o Poder Executivo criar referido órgão,

---

[8] Art. 61, §1º, alínea “e”, da Constituição Federal.

mediante, inclusive, a atribuição do dever fiscalizatório e do exercício do poder de polícia. Propomos, assim, uma **Emenda** nesse sentido.

Responsabilidade civil por danos ao titular dos dados

A solução proposta pela CCT replica o regime de responsabilidade civil do Código de Defesa do Consumidor: objetiva e solidária. Porém, após detida análise dos pleitos encaminhados, bem como da proposta apresentada pela União Europeia[9], concordamos com os apelos no sentido de estabelecer uma limitação a essa responsabilidade, sob pena de inviabilizar a inovação e o desenvolvimento econômico do Brasil face ao progresso tecnológico. Para tanto, propomos **Emenda** nesse sentido, restabelecendo a responsabilidade civil subjetiva e, quando houve mais de um agente no desempenho da mesma ação de uso dos dados pessoais, fixar-lhes, e somente a eles, a responsabilidade solidária.

Vacatio legis

Outro pleito bastante razoável, que fora formulado quase que à unanimidade entre os que contribuíram com críticas e colaborações refere-se à cláusula de vigência, ora proposta em 120 dias. O PL do Poder Executivo, por sua vez, propõe 180 dias.

Entendo de pouca razoabilidade que se queira impor mudanças profundas como as que se propõe a todo um universo real de relações factuais e jurídicas, em pleno vigor de suas execuções, em intervalos de tempo não inferior a 1 ano. Estamos, aqui, a tratar de uma lei geral de dados pessoais, mas que, à toda evidência, possui nítidos traços de conformação das relações jurídica tal como um Código de leis se propõe fazer. Por tal razão, sensível a esses apelos, propomos prorrogação desse prazo, para o mesmo limite proposto de normas legais tão modificadoras da realidade social como a que ora analisamos. Segue, portanto, **Emenda** nesse sentido.

Outras emendas pontuais à proposição

No **inciso II, do art. 4º** o termo “exatidão”, em seu conceito vocabular, não pode ser demandada aos que realizam operações sobre dados

---

[9] Art. 82, *GDPR*.

pessoais ou banco de dados, desde que não são estes a fonte ou origem dos mesmos dados, mas apenas procedem à “coleta, armazenamento, ordenamento, conservação, modificação, comparação, avaliação, organização, seleção, extração, utilização, bloqueio, cancelamento e fornecimento a terceiros, por meio de transferência, comunicação, interconexão ou difusão”; como está definido no art. 3º, IV. Não lhes é possível garantir a “exatidão” das informações, mas, no máximo, apenas a “integridade” dos dados. A *exatidão* dá ideia de *veracidade*, e isso não é possível assegurar no tratamento de dados ou informações, pois estas possuem natureza declaratória em relação ao seu titular que as fornece, e que deve pautar-se segundo os requisitos de confiabilidade e correção. Destarte, o que se pode estabelecer como princípio é a responsabilidade pela “integridade” das informações coletadas e processadas ou utilizadas, justificando-se, destarte, a redação ora colimada ao preceito. Sugere-se a exclusão da palavra “exatidão” do inciso II, do art. 4º.

O uso de termos como “expresso”, “específico” ou “delimitado” – que figuram na atual redação do inciso **V do art. 4º** quanto na do **art. 13** – para adjetivar o consentimento do usuário não lhe traz benefícios, mas tão somente engessa a navegação do usuário, tornando-a lenta, burocrática e obstaculizada. A lei, por si só, já pretende que se obtenha o consentimento dos usuários, de forma livre e inequívoca. Assim, não se veem razões para adjetivar esse consentimento. Tal prática representaria, na verdade, um controle excessivo à liberdade empresarial, sem agregar qualquer benefício ao consumidor que pode, na realidade, simplesmente se sentir desencorajado a prosseguir em seu acesso a informação pela exigência excessiva de consentimentos específicos. Ora, se o consumidor consentiu com o tratamento dos dados, está ciente com a política comercial do site, não há razão para que cada passo em direção à informação desejada, seja precedida de autorizações. Essa interferência legislativa não protege o usuário. Cria, tão somente, ônus para as empresas que refletirão na navegação e fruição prazerosa pelo consumidor a produtos e serviços que busca. A maneira de conceder maior celeridade da navegação é garantir que um único consentimento seja suficiente para autorizar o tratamento dos dados pessoais. A internet é muito fluida, ativa, e a forma de consentimento, como este próprio é, deve ser livre. Sendo assim, não há que se qualificar o consentimento do usuário. Basta que seja inequívoco, que não haja dúvidas de que foi dado pelo usuário. Sugere-se a exclusão das palavras “específico” e “informado” nos artigos referidos.

Ao longo do projeto de lei há a preocupação constante de se obter o consentimento do usuário, de forma inequívoca, para o uso, e

consequentemente, o tratamento das informações. Essa é a tônica do projeto e de todas as discussões acerca da proteção de dados. Os *sites* devem, de antemão, possuir suas políticas de tratamento de dados. Os usuários têm à disposição as regras acerca do uso dos dados. Desse modo, o usuário tem ciência acerca do que será feito com os seus dados no momento do seu consentimento. O uso do termo "legítimas expectativas do usuário", tal como consta do preceito do **inciso XI do art. 4º**, é subjetivo, e não deve ser utilizado em texto de lei que não esteja necessariamente vinculado à proteção que o Estado e a Administração Pública devem oferecer a seus administrados, devendo, portanto, ser excluída a palavra "legítimas".

A alteração do **inciso IV, art. 6º**, justifica-se pelos mesmos argumentos em prol da nova redação alvitrada ao inciso V do art. 4º. Por isso, faz-se necessária a modificação do referido dispositivo, de modo a ser lido tal como proposto na também naquele artigo.

A exigência de emissão de relatórios pode resultar em obrigação bastante subjetiva, diante da natureza das informações a serem discriminadas, conforme prevê o dispositivo, quanto à "finalidade, forma de coleta e período de conservação", conforme consta da parte final do **art. 7º**, na redação do Substitutivo, que passa a ter nova redação com a presente emenda. A depender das informações às quais, com base nesta previsão, se faculta ao titular requerer o acesso; mais ainda, cabendo a este também pressupor a relevância das informações solicitadas, poder-se-á impactar dificultosamente as áreas técnicas em como deverão elaborar tais relatórios, na hipótese de que tenha sido confirmado o tratamento.

Já no **§1º, do art. 7º, e §1º do art. 8,** as alterações consistem em adequar os prazos imputados ao responsável pelo tratamento, visando torná-los mais razoáveis e exequíveis, a fim de que aquele possa atender requerimento do titular para acesso a seus dados pessoais, ou para correção destes, quando eivados de falsidade ou inexatidão. Nesse sentido, a proposta objeto do emendamento está em linha com o Regulamento da União Europeia sobre Proteção de Dados Pessoais.

De acordo com o enunciado do dispositivo previsto no **art. 9º**, o titular poderá requerer o imediato bloqueio, cancelamento ou dissociação de dados pessoais ao responsável pelo tratamento, quando ficar constatado que este se deu de forma "inadequada, desnecessária, desproporcional", contrariando a finalidade da coleta ou incorrendo em violação da lei. A despeito do intento meritório que inspirou a norma proposta, cabe, primeiramente, em prol

do aprimoramento técnico-legislativo, preconizar a retirada dos termos “desnecessária” e “desproporcional” por serem de cunho subjetivo e redundantes em relação ao termo “inadequada”. Segundo reparo pode arguir-se em relação ao prazo exíguo imputado ao responsável pelo tratamento, que deve ser adequado visando torná-lo mais razoável e exequível, a fim de que seja possível atender, de forma profícua e eficiente, ao requerimento do titular, conforme mencionado acima, considerando-se a eventualidade de numerosas demandas concomitantes. Nesse sentido, a proposta do emendamento também está em linha com o Regulamento da União Europeia sobre Proteção de Dados Pessoais.

No **inciso IV do art.12**, não se conforma com a boa técnica legislativa a inserção de disposições extensivas a conteúdos expressamente excluídos do alcance da lei projetada. Tal o caso do tratamento de dados para fins jornalísticos, que se acha excluído do objeto da lei por força do inciso II do § 3º do art. 2º: “(...) § 3º Esta lei não se aplica: (...) II - aos bancos de dados mantidos exclusivamente para o exercício regular da atividade jornalística; (...)”. Nessas condições, afigura-se apropriado a exclusão da palavra “jornalística”, para adequar o texto com outros pontos da proposição.

Não se justifica a exceção feita no **art. 16, inciso II**, ao enumerar hipóteses de encerramento do tratamento de dados, conforme a regra ali estampada: “Art. 16. (...). Parágrafo único. O encerramento implica a exclusão definitiva, dissociação ou anonimização dos dados pessoais do titular, ressalvadas as seguintes hipóteses: (...) II – pesquisa exclusivamente jornalística, histórica ou científica; ou (...)”. A sua vez, não se pode desconsiderar a pesquisa precipuamente de cunho cultural, que não se amolda nem se subsume à de natureza histórica ou científica, devendo, portanto, também figurar destacadamente no enunciado das normas acima referenciadas.

Alguns reparos devem ser apontados no que tange às condições estampadas no **art. 20**, para a realização de comunicação ou interconexão de dados pessoais, a começar pelo fato de que ali também deve ser contemplada a “difusão” de dados pessoais, consoante a conceituação vertente do inciso XII do art. 2º, para abrangência de hipótese como a que se depara nas informações divulgadas por diferentes mídias, termo esse que também deve ser incluído no enunciado do § 3º do art. 20. No **inciso I, do art. 20**, colima-se alteração meramente redacional, mas importante para caracterizar a extensão do consentimento, tendo em vista a amarra excessiva, o alcance de detalhamento que se pode exigir quando se sujeita a manifestação do titular a uma forma

“específica e própria”, o que pode suscitar dubiedades e questões interpretativas sobre os lindes obrigacionais do que se ficou compreendido no “consentimento específico”, motivo pelo qual se sugere a substituição da “forma inequívoca” simplesmente pela produção de anuência de “forma expressa”, ”, que atende ao mesmo objetivo sem render ensejo à discussão sobre o alcance da “especificidade” da vontade manifesta.que atende ao mesmo objetivo sem render ensejo à discussão sobre o alcance da “especificidade” da vontade manifesta.

No **§ 2º, do art. 20**, é importante filiar-se o texto à responsabilidade solidária para envolver “todos aqueles que tiverem acesso aos dados”, uma vez que o acesso aos dados não se confunde com as operações outras e, só por si, não pode gerar a responsabilização coletiva por “dano decorrente ou associado à comunicação ou à interconexão”. Esta só pode ser atribuída a quem de onde procede esse tratamento infracional de dados, e não a todos que a eles tiveram acesso, na realização de operações subsequentes legítimas de “coleta, armazenamento, ordenamento, conservação, modificação, comparação, avaliação, organização, seleção, extração, utilização, bloqueio, cancelamento e fornecimento a terceiros, por meio de transferência, comunicação, interconexão ou difusão”. Mormente em se cuidando de pessoas fictícias, como são as pessoas jurídicas, que não possuem vontade própria, mas esta é exteriorizada por pessoas físicas investidas da representação da entidade, eventuais sanções não deveriam ultrapassar, salvo comprovada coparticipação no ilícito, mesmo no campo da responsabilidade objetiva, os lindes da empresa infratora, evitando-se o redirecionamento de responsabilidades a terceiros, por maiores que sejam os laços gestores, de controle ou de capitais entre umas e outras organizações.

O **art. 31** contempla série de sanções administrativas aplicáveis nas diferentes infrações previstas na Lei projetada, sem prejuízo de outras cominações definidas em normas específicas, assim como as de natureza civil e penal. Especificamente, a regra proposta pelo Substitutivo para o inciso III prevê a imposição de “multa de até 5% (cinco por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos”. Há pelo menos dúplice objeção a ser suscitada quanto ao preceito, primeiramente a questão da responsabilidade de grupo econômico em caso de infração imputável a apenas uma das empresas componentes; em segundo lugar, a excessividade que a reprimenda pode assumir, em diversas situações. Como ficou precedentemente reportado alhures, não se coaduna com os fundamentos doutrinários e constitucionais da responsabilidade por atos ilícitos a extensão, por mera presunção legal, a terceiros, que não foram partícipes da irregularidade

ou violação de obrigações legais. Assim, no caso de grupos de empresas, caso uma das coligadas, controladas ou subsidiárias pratique uma irregularidade, sem coparticipação de qualquer outra, não se justifica que seja esta atingida pelas consequências do ato ímprobo ou ilícito da primeira, inclusive com cláusula penal de multa sobre receitas desvinculadas da empresa infratora. A objeção é tanto mais procedente como quando, apenas no caso de uma ou outra empresa do grupo, a atividade de tratamento de dados seja relevante no modelo de negócios que lhe cabe, mas não em relação às demais, que podem ter apenas utilização acessória ou subsequente de dados, ou nem tê-la. Outro ângulo da questão é que tal penalidade pode assumir proporções colossais, em alguns casos, cujos efeitos adversos a aproximariam da própria proibição da atividade, podendo tornar-se, portanto, desarrazoada e desproporcional e inviabilizar a atividade econômica. Diversamente, postulamos a fixação de valores, em patamares de até uma centena de salários mínimos, a ser aplicada apenas nas eventuais reincidências de infrações suscetíveis de "advertência com indicação de prazo para a adoção de medidas corretivas" (inciso I), e de "alteração, retificação ou cancelamento do banco de dados" (inciso II). A sua vez, a sanção de proibição ou suspensão total das atividades de tratamento de dados assume nítido efeito de encerramento ou extinção da pessoa jurídica, por comprometer de forma irreversível a sustentabilidade do negócio, podendo atingir inclusive outros segmentos de atividades que não têm participação ou atuação nas operações de tratamento de dados.

Não é possível ignorar as consequências sociais que certamente advirão de medida dessa natureza, em termos de extinção de postos de trabalho, perda de receitas fiscais e muitas outras sequelas adversas. É necessário, para que o texto permaneça nos lindes constitucionais e nas lições seculares das melhores fontes do direito, vincular a sanção à empresa faltosa, e delimitar o alcance da punição, para que não fique sujeita a extrapolações, subjetivas e objetivas, descabidas na imposição de restrições de atividades. Pelos fundamentos aqui sumariados, alvitramos as modificações redacionais do *caput* e incisos III, IV e V do art. 31, conforme a presente Emenda.

O **art. 34** deve ser alterado para não permitir que haja responsabilidade solidária no âmbito de futura lei de tratamento de dados pessoais. Isso porque o ordenamento jurídico brasileiro repudia, em sua hermenêutica, a responsabilização de pessoa, física ou jurídica, na ausência de nexo de causalidade entre a ocorrência da infração e a atuação do referido ente. Não há que se falar em responsabilidade solidária quanto aos fatos tratados pelo artigo em questão, posto que há, tanto na doutrina quanto na jurisprudência,

entendimento consolidado sobre o descabimento da responsabilização de entes que não praticaram a conduta infratora. Nesse sentido, de acordo com a atual orientação do Superior Tribunal de Justiça, o entendimento prevalente no âmbito das Turmas que integram a Primeira Seção desta Corte é de que a pessoas jurídicas não deve ser imputada a responsabilidade solidária, ainda que pertençam ao mesmo grupo econômico, na forma prevista no art. 124 do CTN. Na ocorrência de uma infração, uma das medidas iniciais a serem tomadas é a verificação da autoria. Verifica-se quem de fato incorreu na prática da conduta tipificada, justamente, para que a pena não seja estendida a terceiros isentos de culpa. Isso porque o apenamento de quem não provocou infrações pode, ao fim e ao cabo, inviabilizar a atividade de um terceiro que nada tem a ver com o ato ilícito. Além de ser flagrantemente injusto, pode prejudicar o desempenho desse terceiro, causando-lhe grandes prejuízos financeiros, ou até mesmo de credibilidade.

Emendas de outros Senadores apresentadas ao Substitutivo

A eminente Senadora Marta Suplicy apresentou a **Emenda nº 32** e as **Subemendas nºs 1** e **2**, à Emenda nº 31-CCT-CMA, que, em apertada síntese:

1. Excepciona, da incidência normativa da lei, os bancos de dados das serventias notariais e de registro; e

2. Delinear regras específicas de tratamento de dados pessoais quando voltadas a registros em cadastros de crédito negativadores;

3. Prever regras específicas para inclusão de dados restritivos ao crédito em decorrência de dívida.

A despeito do mérito das sugestões trazidas pela nobre Senadora Marta Suplicy, não podemos com elas concordar. Isso porque a proposta aqui formulada é de definição de uma lei geral de proteção de dados pessoais, sem descer ao detalhamento das relações jurídicas possíveis nos infindáveis setores de atuação pública ou privada, por meio dos quais essas informações trafegarão. Por tal razão, a fim de incorrer em uma norma sem observância da devida isonomia de tratamento normativo e, ainda, sem incorrer em vícios de

juridicidade, em razão das regras cogentes de elaboração de leis previstas na Lei Complementar nº 95, de 1998, opinamos por sua rejeição.

III – VOTO

Ante o exposto, votamos pela **aprovação** do Projeto de Lei do Senado nº 330, de 2013, nos termos do substitutivo aprovado na Comissão de Ciência, Tecnologia, Inovação, Comunicação e Informática, e pela Comissão de Meio Ambiente, pela **rejeição** da Emenda nº 32 e das Subemendas à Emenda nº 31-CCT-CMA, e pela declaração de prejudicialidade do Projeto de Lei do Senado nº 131, de 2014, e do Projeto de Lei do Senado nº 181, de 2014, com as seguintes subemendas:

SUBEMENDA Nº , À EMENDA Nº 31 – CCT/CMA – CAE

Dê-se ao art. 1º, do PLS 330, de 2013, na forma da Emenda nº 31 – CCT/CMA, a seguinte redação:

> "Art. 1º Esta Lei estabelece princípios, garantias, direitos e obrigações referentes à proteção, ao tratamento e ao uso de dados de pessoas naturais, tendo como fundamentos o princípio da dignidade da pessoa humana, a proteção da privacidade, a garantia da liberdade, a inviolabilidade da honra e da imagem das pessoas e sua harmonização com a proteção e a defesa do consumidor e os princípios da livre concorrência e da livre iniciativa."

SUBEMENDA Nº , À EMENDA Nº 31 – CCT/CMA – CAE

Inclua-se, no art. 1º, do PLS 330, de 2013, na forma da Emenda nº 31 – CCT/CMA, o seguinte parágrafo único:

“Art. 1º .....

Parágrafo único. Havendo conflito entre as normas previstas nesta Lei e outra legislação em vigor no território nacional, deverão as primeiras prevalecer sobre esta última, face à sua especialidade em matéria de regulação de princípios, garantias, direitos e obrigações referentes à proteção, ao tratamento e ao uso de dados pessoais, exceto se a norma conflitante for mais específica.”

SUBEMENDA Nº , À EMENDA Nº 31 – CCT/CMA – CAE (DE REDAÇÃO)

Substitua-se, no caput, do art. 2º, do PLS 330, de 2013, na forma da Emenda nº 31 – CCT/CMA, a expressão “Esta lei aplica-se” por “Aplica-se o disposto nesta lei”.

SUBEMENDA Nº , À EMENDA Nº 31 – CCT/CMA – CAE

Art. 1º Exclua-se, no inc. I, do § 3, do art. 2º, do PLS 330, de 2013, na forma da Emenda nº 31 – CCT/CMA, a expressão “**e segurança pública**”.

Art. 2º Inclua-se o seguinte § 4º, ao art. 2º, do PLS 330, de 2013, renumerando-se o atual:

“Art. 2º.....

.....

§ 4º O tratamento de dados realizado para fins de segurança pública ou de atividades de investigação e repressão de infrações penais será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observado o devido processo legal e os

princípios gerais de proteção e os direitos do titular previstos nesta Lei.

....."

SUBEMENDA Nº , À EMENDA Nº 31 – CCT/CMA – CAE (DE REDAÇÃO)

Exclua-se, no inc. IV, do § 3º, do art. 2º, do PLS 330, de 2013, na forma da Emenda nº 31 – CCT/CMA, a expressão "desde que não seja possível identificar o titular".

SUBEMENDA Nº , À EMENDA Nº 31 – CCT/CMA – CAE (DE REDAÇÃO)

O § 4º, do art. 2º, do PLS 330, de 2013, na forma da Emenda nº 31 – CCT/CMA, conforme sua nova renumeração, passa a vigorar com a seguinte redação:

"Art. 2º.....

.....

4º Os dados desanonimizados terão a mesma proteção dos dados pessoais, aplicando-se aos responsáveis por sua coleta, armazenamento e tratamento o disposto nesta Lei."

SUBEMENDA Nº , À EMENDA Nº 31 – CCT/CMA – CAE

O art. 3º, do PLS 330, de 2013, na forma da Emenda nº 31 – CCT/CMA, passa a vigorar com a seguinte redação:

"Art. 3º.....

I - dado pessoal: qualquer informação relacionada a pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos;

.....

XIV - dado desanonimizado: dado originalmente anônimo que, após tratamento, permite a identificação do titular."

SUBEMENDA Nº , À EMENDA Nº 31 – CCT/CMA – CAE

O art. 26, do PLS 330, de 2013, na forma da Emenda nº 31 – CCT/CMA, passa a vigorar com a seguinte redação:

"Art. 26. .....

I – para países ou organizações internacionais que proporcionem grau de proteção de dados adequado ao previsto nesta Lei;

.....

V – quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução criminal.

....."

SUBEMENDA Nº , À EMENDA Nº 31 – CCT/CMA – CAE

O art. 27, do PLS 330, de 2013, na forma da Emenda nº 31 – CCT/CMA, passa a vigorar com a seguinte redação:

"Art. 27. O grau de proteção de dados dos países de destino ou da organização internacional será analisado por meio de critérios

definidos em regulamento, assegurado à Procuradoria-Geral da República, à Advocacia-Geral da União, ao Ministério das Relações Exteriores e ao Ministério da Justiça a prerrogativa de requerer à autoridade competente a avaliação do nível de proteção a dados pessoais conferido por país ou organização internacional."

SUBEMENDA Nº , À EMENDA Nº 31 – CCT/CMA – CAE

O art. 37, do PLS 330, de 2013, na forma da Emenda nº 31 – CCT/CMA, passa a vigorar com a seguinte redação:

"Art. 37. A União fiscalizará o cumprimento desta Lei, através de órgão nacional competente, com as seguintes atribuições e competências , além de outras previstas em lei:

I – zelar pela proteção de dados pessoais, nos termos da lei, devendo tomar as medidas necessárias para atender a petições e reclamações formuladas pelas pessoas afetadas;

II – realizar auditoria nos tratamentos de dados pessoais e processos envolvidos com dados pessoais visando garantir a sua conformidade aos princípios e regras existentes na legislação brasileira, podendo aplicar as sanções administrativas nesta Lei, mediante processo administrativo que assegure o contraditório e a ampla defesa;

III – garantir a publicidade dos bancos de dados pessoais existentes e das operações de tratamentos por eles efetuados, especialmente através da publicação anual da relação destes bancos de dados pessoais e do direito de consulta pelos afetados ao órgão nacional competente;

IV - promover o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e as medidas de segurança;

V - promover estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade;

VI - estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais;

VII - promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transacional;

VIII - dispor sobre as formas pelas quais se dará a publicidade das operações de tratamento;

IX - solicitar, a qualquer momento, ao Poder Público, informações acerca dos seus órgãos que realizem operações de tratamento de dados pessoais, informe específico sobre o âmbito, natureza dos dados e outras informações relacionadas ao tratamento realizado, podendo emitir parecer técnico complementar para garantir o cumprimento desta Lei;

X - estabelecer normas complementares para as atividades de comunicação de dados pessoais;

XI – elaborar relatórios anuais acerca de suas atividades e sobre o estado da proteção de dados pessoais no país;

XII - elaborar diretrizes para uma Política Nacional de Proteção de Dados Pessoais e Privacidade;

XIII - realizar demais ações dentro de sua esfera de competência, inclusive as previstas nesta Lei e em legislação específica; e

XIII – editar normas complementares para a proteção de dados pessoais.

Parágrafo único. No exercício das atribuições previstas neste artigo, o órgão federal competente deverá zela pela preservação do segredo industrial e do sigilo das informações, quando assim atribuído em lei, sob pena de responsabilidade.”

SUBEMENDA Nº , À EMENDA Nº 31 – CCT/CMA – CAE

Inclua-se, seguinte artigo nº 38, ao PLS 330, de 2013, na forma da Emenda nº 31 – CCT/CMA:

“Art. 38. Fica o Poder Executivo autorizado a criar, observadas as normas de adequação orçamentária e fiscal, a Autoridade Nacional de Proteção de Dados, com jurisdição em todo o território nacional, responsável pelas atribuições e competências definidas no artigo anterior, com estrutura, organização e composição definidos em lei de iniciativa do Presidente da República.”

SUBEMENDA Nº , À EMENDA Nº 31 – CCT/CMA – CAE

O art. 17, do PLS 330, de 2013, na forma da Emenda nº 31 – CCT/CMA, passa a vigorar com a seguinte redação:

“Art. 17.....

§ 1º Aquele que efetuar o tratamento de dados pessoais responderá, de no limite de sua atuação, pela reparação dos danos causados aos titulares ou terceiros, se, no exercício de sua atividade, não tiver cumprido as determinações desta lei ou do órgão federal competente que lhe são impostas.

§ 2º As pessoas envolvidas na mesma atividade ou em atividades sucessivas de tratamento de dados que provocarem dano ao titular responderão solidariamente por sua reparação, assegurado o direito de regresso contra dos demais àquele que reparar integralmente o dano.”

SUBEMENDA Nº , À EMENDA Nº 31 – CCT/CMA – CAE

Inclua-se o seguinte art. 39, ao PLS 330, de 2013, na forma da Emenda nº 31 – CCT/CMA:

"Art. 39. Esta lei entra em vigor após decorrido 365 dias da data de sua publicação oficial."

SUBEMENDA Nº , À EMENDA Nº 31 – CCT/CMA – CAE

O art. 7º do PLS 330, de 2013, na forma da Emenda nº 31 – CCT/CMA, passa a vigorar com a seguinte redação:

"Art. 7º O titular poderá requerer do responsável o acesso à integralidade de seus dados pessoais, assim como a confirmação acerca do seu tratamento, bem como requerer, justificadamente, a elaboração de relatório que contenha todas as informações necessárias sobre o tratamento.

....."

SUBEMENDA Nº , À EMENDA Nº 31 – CCT/CMA – CAE

O § 1º do art. 7º e o § 1º do art. 8º do PLS 330, de 2013, na forma da Emenda nº 31 – CCT/CMA, passam a vigorar com a seguinte redação:

"Art. 7º .....
.....

§ 1º O requerimento do titular será atendido no prazo de trinta dias, de forma gratuita, de maneira que a resposta seja de fácil compreensão.

....."

"Art. 8º .....
.....

§ 1º O responsável deverá, no prazo de trinta dias, corrigir os dados pessoais e comunicar o fato a terceiros que tenham tido acesso aos dados.

.....”

SUBEMENDA Nº , À EMENDA Nº 31 – CCT/CMA – CAE

O art. 9º do PLS 330, de 2013, na forma da Emenda nº 31 – CCT/CMA, passa a vigorar com a seguinte redação:

“Art. 9º Constatado que o tratamento de dados se deu de forma inadequada, em contrariedade à finalidade que fundamentou sua coleta ou com violação a qualquer dispositivo desta Lei, o titular poderá requerer, sem qualquer ônus, o seu imediato bloqueio, cancelamento ou dissociação, que será realizado pelo responsável no prazo de trinta dias.

.....”

SUBEMENDA Nº , À EMENDA Nº 31 – CCT/CMA – CAE

O inciso I, assim como ao § 2º do art. 20 do PLS 330, de 2013, na forma da Emenda nº 31 – CCT/CMA, passam a vigorar com a seguinte redação:

“Art. 20**.** A comunicação, a difusão ou a interconexão de dados pessoais somente podem ser realizadas:

I – quando o titular consentir de forma inequívoca;

.....

§ 2º Em caso de dano decorrente ou associado à comunicação, à difusão ou à interconexão, respondem todos aqueles que fizeram mau uso dos dados ou permitiram que terceiros fizessem mau uso dos mesmos.

§ 3º Os critérios adicionais para a comunicação, a difusão e a interconexão de dados pessoais serão definidos em regulamento.”

SUBEMENDA Nº , À EMENDA Nº 31 – CCT/CMA – CAE

O *caput* do art. 34 do Substitutivo CCT/CMA ao PLS nº 330, de 2013, passa a vigorar com a seguinte redação:

“Art. 34. Serão responsáveis as empresas ou entidades que praticarem infrações a esta Lei.

.....”

SUBEMENDA Nº , À EMENDA Nº 31 – CCT/CMA – CAE

O inciso II do art. 4º do Substitutivo CCT/CMA ao PLS nº 330, de 2013, passa a vigorar com a seguinte redação:

“Art. 4º .....
.....

II – adequação, pertinência, integridade e atualização, periódica e de ofício, das informações;

.....”

SUBEMENDA Nº , À EMENDA Nº 31 – CCT/CMA – CAE

O inciso IV do art. 6º do Substitutivo CCT/CMA ao PLS nº 330, de 2013, passa a vigorar com a seguinte redação:

“Art. 6º .....
.....

IV – consentimento inequívoco sobre coleta, armazenamento e tratamento de dados pessoais;

.....”

SUBEMENDA Nº , À EMENDA Nº 31 – CCT/CMA – CAE

O inciso IV, do art. 12 e o inciso II, do parágrafo único, do art. 16 do Substitutivo CCT/CMA ao PLS nº 330, de 2013, passam a vigorar com a seguinte redação:

“Art. 12. **.**.....
.....

IV – quando realizado exclusivamente no âmbito da pesquisa cultural, histórica ou científica sem fins lucrativos e desde que sejam tomadas medidas adicionais de proteção, excetuadas as atividades ou hipóteses previstas no § 3º do art. 2º, em relação às quais esta lei não se aplica;

.....”

“Art. 16**.** .....
.....

Parágrafo único. .....
.....

II – pesquisa exclusivamente cultural, histórica ou científica, excetuadas as atividades ou hipóteses previstas no § 3º do art. 2º, em relação às quais esta lei não se aplica; ou

.....”

SUBEMENDA Nº , À EMENDA Nº 31 – CCT/CMA – CAE

O inciso V do art. 4º e o *caput* do art. 13, do Substitutivo CCT/CMA ao PLS nº 330, de 2013, passam a vigorar com a seguinte redação:

"Art. 4º .....
.....

V – consentimento livre e inequívoco do titular de dados como requisito à coleta de dados pessoais, quando se tratar de dados sensíveis ou de interconexão internacional de dados realizada por banco de dados privado;

....."

"Art. 13. O consentimento do titular deve ser prestado de forma livre e inequívoca e dizer respeito à finalidade legítima."

SUBEMENDA Nº , À EMENDA Nº 31 – CCT/CMA – CAE

O inciso XI do art. 4º do Substitutivo CCT/CMA ao PLS nº 330, de 2013, passa a vigorar com a seguinte redação:

"Art. 4º .....
.....

XI – o tratamento de dados pessoais deve ser compatível com as finalidades a que se destinam e nos termos da presente lei, respeitado o contexto do tratamento;

....."

SUBEMENDA Nº , À EMENDA Nº 31 – CCT/CMA – CAE

O art. 31, *caput* e seus incisos III, IV e V, do Substitutivo CCT/CMA ao PLS nº 330, de 2013, passam a vigorar com a seguinte redação:

“Art. 31. Às infrações desta Lei fica sujeito o responsável por tratamento inadequado de dados, conforme o caso, às seguintes sanções administrativas, sem prejuízo das de natureza civil, penal e das definidas em normas específicas:

.....

III – multa de até 100 (cem) salários mínimos por infração, no caso de reincidência de infração cometida que leve à aplicação das penalidades dos itens I e II;

IV – suspensão parcial e específica das atividades de tratamento de dados pessoais;

V – proibição parcial e específica das atividades de tratamento de dados pessoais;

.....”

Sala da Comissão,

, Presidente

, Relator