CONSIDERAÇÕES DA CNSEG/FENASEG SOBRE O APL DE PROTEÇÃO DE DADOS PESSOAIS

1) Definição de dado pessoal e de dado anônimo

A redação trazida pelo art. 5º, I do APL adotou um conceito de dado pessoal similar ao adotado pela Diretiva Europeia 95/46/CE, não tendo criado qualquer limitação à possibilidade de identificação do indivíduo, o que em alguma medida fez a referida Diretiva Europeia em seu considerando nº 26, quando prevê "que, para determinar se uma pessoa é identificável, importa considerar **o conjunto dos meios susceptíveis de serem razoavelmente utilizados**, seja pelo responsável pelo tratamento, seja por qualquer outra pessoa, para identificar a referida pessoa". Na nossa opinião essa possibilidade deve estar vinculada à razoabilidade e proporcionalidade da identificação. Conforme destacado por Guerra Filho "O 'princípio da proporcionalidade em sentido estrito' determina que se estabeleça uma correspondência entre o fim a ser alcançado por uma disposição normativa e o meio empregado, que seja juridicamente a melhor possível."[1]

Apenas a título exemplificativo, vale citar a posição adotada pelo legislador alemão em sua lei de proteção de dados, segundo a qual um indivíduo apenas será identificável se o tempo, despesa e trabalho empregados para essa identificação forem proporcionais.[2] Na mesma linha é a Recomendação R(97) 5 do Comitê de Ministros do Conselho da Europa, que afirma que um dado não pode ser considerado identificável se essa identificação requerer um montante de tempo e de trabalho irrazoáveis.[3]

Vê-se, portanto, que os critérios temporal, econômico e laboral para averiguar a proporcionalidade/razoabilidade mostram-se, no que se refere à possibilidade de identificação do titular do dado, os que melhor atendem ao requerimento da proporcionalidade que, apesar de não constar expressamente do texto constitucional, é dele deduzido com base no seu art. 5º, §2º[4] e amplamente aplicado por nossos tribunais.[5]

---

[1] GUERRA FILHO. O princípio constitucional da proporcionalidade. Disponível em http://bdjur.stj.gov.br/xmlui/bitstream/handle/2011/19640/O_Princ%c3%adpio_Constitucional_da_Proporcionalidade.pdf?sequence=1 (23.12.2010).

[2] *Apud* WALDEN. Anonymising Personal Data. In: *International Journal of Law and Information Technology*. Vol 20, n° 2. Oxford University Press, 2002. p. 226.

[3] COUNCIL OF EUROPE, Committee of Ministers, Recommendation No. R (97) 5 on the Protection of Medical Data (Feb. 13, 1997). Disponível em www.coe.int (07.09.2014).

[4] GUERRA FILHO. Op. cit. *"É assim que, mesmo no caso das normas que compõem o princípio da proporcionalidade (em sentido amplo), não a concebemos como dotadas da natureza de regras, até porque não se acham explicitadas em todo e qualquer ordenamento jurídico, tal como verificamos entre nós, onde o princípio como um todo haverá de ser deduzido do regime constitucional de direitos fundamentais por nós adotado, com base no art. 5º, § 2º da Constituição Federal."*

Assim, os dados que não se enquadrarem nessa lógica de razoabilidade e proporcionalidade da potencial identificação do titular do dado não estariam sujeitos às normas do APL, incluindo-se na definição de dados anônimos.

A definição de dados anônimos contida no inciso IV do art. 5º do APL, por sua vez, contempla a expressão 'conjunto de meios suscetíveis de serem razoavelmente utilizados para identificar o titular do dado', que, entretanto, não traz a clareza e segurança necessárias para a sua correta aplicação.

O termo 'razoavelmente' deveria ser explicitado, para considerar o tempo, custo e mão de obra empregadas para a identificação, como já salientado anteriormente. No setor de seguros, por exemplo, dependendo da interpretação dada a essa definição, os modelos estatísticos criados para fins de precificação poderiam estar sujeitos à incidência das normas do APL, visto que esses modelos são feitos com base em experiência pretérita, muitas vezes envolvendo dados que um dia foram pessoais.

Além disso, deveriam ser considerados, também, na definição de dado anônimo a finalidade do tratamento de tais dados bem como a probabilidade de que venham a ser re-identificados. A caracterização de um dado como anônimo apresenta importância capital, uma vez que informações que não podem ser relacionadas a uma pessoa identificada ou identificável podem suscitar a não aplicação das normas referentes à proteção de dados, como faz a Diretiva Europeia 95/46/CE no já citado considerando nº 26. Em muitas leis, por exemplo, há um procedimento de anonimização do dado pessoal em relação ao seu titular como requisito para o seu livre tratamento em determinadas circunstâncias.

Apresentamos, assim, proposta de nova redação para o inciso IV do art. 5º, bem como para novo inciso (III) no §2º do art. 2º do APL:

> Art. 5º - .....
>
> IV – dado anônimo: informação relativa a um titular que não possa ser identificado, nem pelo responsável pelo tratamento nem por qualquer outra pessoa, tendo em conta o conjunto de meios suscetíveis de serem razoavelmente utilizados pelo responsável pelo tratamento das informações ou por qualquer outra pessoa para identificar o referido titular, especialmente o tempo, custo e trabalho empregados na identificação, a finalidade do tratamento e a probabilidade de sua identificação;
>
> Art. 2º - .....
> §2º - .....
> III - ao tratamento de dados anônimos, incluídos os modelos estatísticos e atuariais.

---

[5] O STJ, em outro julgado, entendeu que *"Pelo Princípio da Proporcionalidade, as normas constitucionais se articulam num sistema, cuja harmonia impõe que, em certa medida, tolere-se o detrimento a alguns direitos por ela conferidos, no caso, o direito à intimidade"* (HC 33110/SP).

2) Princípio do livre acesso

O art. 6º, IV e o art. 17, II do APL criam a obrigação para o responsável pelo tratamento de dados de possibilitar ao titular do dado acesso às suas informações armazenadas por aquele. O direito de acesso já está assegurado aos consumidores pelo Código de Proteção e Defesa do Consumidor (CDC), em seu art. 43, caput, e a qualquer pessoa através da Lei nº 9.507/97, que regulamenta exatamente o direito de acesso a informações e disciplina o rito processual do Habeas data. Cabe salientar, contudo, que nem o CDC nem a Lei regulamentar do *Habeas data* fazem menção expressa à gratuidade do exercício de tal direito.

É importante salientar que nas relações entre consumidores e cadastros de proteção ao crédito de uma forma geral consolidou-se a prática de fornecer acesso às informações armazenadas por tais repositórios de dados sem a cobrança de qualquer custo. Nessa hipótese, entretanto, referidos repositórios de informação não recolhem dados diretamente de seus titulares, mas de outras fontes, como instituições financeiras, cartórios de protestos de títulos, cartórios de distribuição de ações, entre outros.

O APL sob análise, diferentemente, abrangerá todas as situações de tratamento de dados, inclusive aquelas decorrentes de contrato ou de relações de trabalho, o que importa dizer que os dados nesses casos são obtidos diretamente de seu titular, que, portanto, tem conhecimento das informações que são armazenadas pelo responsável pelo tratamento, não se justificando, dessa forma, a possibilidade de acesso gratuito ilimitado.

Ressalte-se, que a cobrança para acesso às informações já foi autorizada por diversas leis de proteção de dados, sendo exemplos as leis italiana[6] e inglesa.[7] Essa prática tem por objetivo evitar que alguns titulares de dados utilizem excessiva e desmotivadamente esse direito, gerando custos imotivados para o responsável pelo tratamento.

É importante salientar que o fato de se cobrar um valor pelo custo do fornecimento das informações solicitadas, seja em formato impresso ou eletrônico, por si só não prejudicará o exercício dos direitos pelo titular do dado, visto que poderá ser assegurado a

[6] A lei italiana reconhece a possibilidade de cobrança de um valor caso o direito de acesso seja exercido e não seja localizada nenhuma informação sobre o titular do dado armazenada pelo responsável do tratamento ao qual foi dirigido o requerimento de acesso a informações (art. 10, §7º do *Codice in materia di protezione dei dati personali*).

[7] UK INFORMATION COMMISSIONER. The Guide to Data Protection. Disponível em http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/the_guide_to_data_protection.pdf (08.09.2014). p. 133.

este o reembolso de tal custo caso seja identificada alguma incorreção ou inexatidão nas informações armazenadas. Essa foi a posição adotada pelo legislador francês em sua lei de proteção de dados.[8]

Além disso, ficaria assegurado também o direito de acesso àquelas pessoas consideradas pobres na forma da lei, cujo acesso aos seus dados pessoais seria gratuito, desde que solicitado mediante requerimento da defensoria pública, com base no disposto no art. 3º, II da Lei nº 1.060/50.

Outra solução seria a previsão de um acesso gratuito anual, para fins de verificação da qualidade dos dados armazenados (se estão exatos e atualizados) e de exercício de seus outros direitos de titular do dado (correção e cancelamento, por exemplo), o que, na nossa opinião, atenderia melhor aos requisitos de proporcionalidade já destacados anteriormente, equilibrando os interesses de titulares de dados e de responsáveis por tratamento de dados. Primeiro, porque o titular do dado teria a possibilidade de verificar anualmente a correção e exatidão de seus dados armazenados por determinado responsável por tratamento de dados, sem nenhum custo e, segundo, porque o responsável pelo tratamento apenas suportaria os custos de tal operação uma vez por ano ou nos casos em que fosse identificada alguma inexatidão ou incorreção nos dados armazenados.

Finalmente, vale destacar que essa medida segue a mesma orientação adotada pela Lei nº 12.007 de 29.07.2009, que obriga as pessoas jurídicas prestadoras de serviços públicos ou privados a emitir anualmente declaração de quitação de débitos.

Apresentamos, assim, proposta de nova redação para o §2º do art. 18 com supressão dos dois incisos, bem como para os §§ 2º e 3º do art. 18 do APL:

> Art. 6º - .....
>
> IV – princípio do livre acesso, pelo qual deve ser garantida consulta pelos titulares dos dados sobre as modalidades de tratamento e sobre a integralidade dos seus dados;
>
> Art. 18 - .....
>
> §2º - As informações e dados poderão ser fornecidos, a critérios do titular, por meio eletrônico, seguro e idôneo para tal fim ou sob a forma impressa, podendo ser cobrada em qualquer hipótese o valor necessário ao ressarcimento do custo dos serviços e dos materiais utilizados.
>
> §3º - Na hipótese de os dados pessoais objeto de tratamento não tiverem sido coletados diretamente do titular do dado, este poderá solicitar, anualmente, cópia integral dos seus dados pessoais em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento, sempre que o banco de dados estiver em suporte eletrônico,

[8] Artigo 39, §5º da lei de proteção de dados francesa.

podendo ser cobrada nessa hipótese apenas o valor necessário ao ressarcimento dos materiais utilizados para o fornecimento da cópia integral de seus dados.

3) Princípio da não discriminação

Outro dispositivo que merece ser melhor redigido é a previsão do princípio da não discriminação. Da forma como está redigido este princípio, sem qualquer ressalva, pode dar margem à interpretação de que não poderia existir distinção de prêmios de acordo com o perfil de dados de cada segurado, o que seria contrário à própria natureza do seguro.

Na União Europeia houve uma decisão nesse sentido, proferida pelo Tribunal de Justiça da União Europeia no caso "Test-Achats", de que o gênero não poderia ser o único fator de distinção de prêmios, e criou um imbróglio, motivando, inclusive, a adoção, pela Comissão da União Europeia das "Orientações sobre a aplicação ao setor dos seguros da Diretiva 2004/113/CE do Conselho, à luz do acórdão do Tribunal de Justiça da União Europeia no Processo C- 236/09 (Test-Achats)".

Sugere-se, assim, que haja uma ressalva expressa quanto à possibilidade de distinção de prêmios com base em informações pessoais dos segurados. Importante destacar que na definição do dicionário Houaiss "discriminação é a faculdade de distinguir", ou seja, não é uma ação necessariamente pejorativa. No caso dos seguros, a generalização e a discriminação – delimitação dos riscos a serem segurados, distinguindo pessoas e bens de acordo com os riscos aos quais estão expostos – são inerentes a essa atividade. Neste sentido, não há nenhum problema em se utilizar o tratamento de dados para fins discriminatórios. Ou seja, para distinguir pessoas.

O tratamento de dados pelo setor de seguros existe essencialmente para discriminar pessoas, agrupando-as ou separando-as em grupos, proporcionando uma maior efetividade no desenvolvimento de coberturas focadas em determinados grupos, o que é positivo para a economia.

Apresentamos, assim, proposta de nova redação para o inciso IX do art. 6º do APL:

Art. 6º - .....

IX - princípio da não discriminação, pelo qual o tratamento não pode ser realizado para fins discriminatórios, exceto naquelas atividades que dependem de avaliação de risco e quando esta avaliação compromete a contratação proposta, tais como seguros ou outros similares.

4) **<u>Tratamento de dados para cumprimento de dever imposto pela autoridade fiscalizadora/reguladora</u>**

Também merece revisão a hipótese de dispensa de consentimento para cumprimento de obrigação legal do responsável. Em setores regulados como o de seguros, muitas vezes as empresas têm o dever de transferir dados à autoridade reguladora do setor com base em normas de origem infralegal, adotadas por este mesmo órgão. Assim, a dispensa do consentimento deveria contemplar não apenas o cumprimento de obrigação legal, mas, também, de dever imposto pela autoridade fiscalizadora/reguladora do setor.

Apenas a título exemplificativo, algumas normas adotadas pelo órgão fiscalizador do setor de seguros, a Superintendência Nacional de Seguros Privados – SUSEP, estabelecem o dever de tratamento de dados pessoais pelas entidades supervisionadas, como a Circular SUSEP nº 344 sobre os controles internos específicos para a prevenção contra fraudes, que obriga seguradoras a estabelecerem uma política de prevenção, detecção e correção de fraudes, inclusive com o dever de oferecer notícias de práticas de fraudes aos órgãos de repressão, o que impõe, necessariamente, o tratamento de dados pessoais de seus clientes.

Nesse sentido apresentamos proposta de nova redação para o inciso I do art. 11, alínea 'a' do inciso II do art. 12, o inciso I do art. 15 e o §2º do art. 19 do APL:

Art. 11 - .....

I - cumprimento de uma obrigação legal ou regulatória pelo responsável;

Art. 12 - .....

II - .....

a) cumprimento de uma obrigação legal ou regulatória pelo responsável;

Art. 15 - .....

I - cumprimento de uma obrigação legal ou regulatória pelo responsável;

Art. 19 - .....

§2º - Ficam ressalvados os tratamentos de dados pessoais necessários ao cumprimento de obrigação legal ou regulatória pelo responsável.

5) **<u>Tratamento de dados necessário ao atendimento de interesses legítimos do responsável pelo tratamento</u>**

Ainda no tema da dispensa de consentimento, uma importante hipótese de dispensa de consentimento para o tratamento de dados pessoais contida na maioria das leis gerais de proteção de dados - para não dizer em todas - ficou de fora da relação contida no artigo 11 do APL. É a hipótese de tratamento de dados necessário ao atendimento dos interesses legítimos do responsável pelo tratamento ou do terceiro ou terceiros a quem os dados sejam comunicados. Essa base legal está prevista na Diretiva 95\46\CE, em seu artigo 7º (f).

Essa opção ao consentimento coloca de um lado os interesses e direitos do titular dos dados e de outro os legítimos interesses do responsável pelo tratamento (ou de terceiros) devendo ser realizada, caso a caso, uma ponderação de interesses para se verificar se no caso concreto o interesse de um ou outro irá prevalecer.

Essa hipótese de autorização ao tratamento de dados é de vital importância para se possibilitar a realização de tratamentos de dados legítimos, mas que seriam dificilmente enquadrados nos sete incisos do art. 11 do APL, em situações nas quais o consentimento não seria uma base legal adequada.

Cumpre-nos destacar que o Grupo de Trabalho do Artigo 29, grupo de trabalho composto por representantes das autoridades de proteção de dados pessoais dos países membros da União Europeia, representantes da Autoridade Europeia de Proteção de Dados e da Comissão da União Europeia, já se manifestou acerca do conceito de legítimo interesse para fins da Diretiva, bem como das situações em que é possível aplicar referido item "f", em sua "Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na aceção do artigo 7.º da Diretiva 95/46/CE".[9]

Neste sentido, o Grupo de Trabalho do Artigo 29 entende que "um interesse pode ser considerado legítimo desde que o responsável pelo tratamento possa prosseguir esse interesse em conformidade com a legislação em matéria de proteção de dados e a demais legislação aplicável. Por outras palavras, um interesse legítimo deve ser «admissível nos termos da lei»."[10] Deste modo para que o interesse seja considerado legítimo, para os fins da Diretiva, este deve: (i) ser lícito (ou seja, deve respeitar o direito da UE e o direito nacional aplicáveis), (ii) ser definido de forma suficientemente clara para permitir a realização do teste da ponderação em relação aos interesses e aos direitos fundamentais da

[9] Disponível em http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_pt.pdf#h2-2. Acesso em 16.06.15.

[10] Grupo de Trabalho do Artigo 29. Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na aceção do artigo 7.º da Diretiva 95/46/CE. P. 39.

pessoa em causa (ou seja, deve ser suficientemente específico) e (iii) representar um interesse real e atual (ou seja, não deve ser especulativo).[11]

Deste modo, a Diretiva cria o chamando "teste da ponderação", entre o interesse envolvido e os direitos dos titulares dos dados, para analisar a possibilidade de invocar o legítimo interesse previsto no item "f" como fundamento para o tratamento de dados pessoais. Ou seja, quando o interesse legítimo é identificado, parte-se para a realização do teste para apurar se o artigo 7, "f", justifica o tratamento dos dados.

A realização do teste deve levar em consideração os seguintes fatores: a) avaliação do interesse legítimo do responsável pelo tratamento, i.e, se os interesses envolvem direitos fundamentais ou coincidem com interesses públicos, b) impacto do tratamento sobre o titular do dado, c) o cumprimento pelo responsável pelo tratamento das exigências constantes da Diretiva; e d) a adoção pelo responsável pelo tratamento de medidas adicionais de proteção.[12]

Assim, para que o responsável pelo tratamento possa justificar o tratamento de dados por seu legítimo interesse, seja este comercial ou não, sem prévio consentimento do titular dos dados, conforme constante do Artigo 7º, "f" da Diretiva Europeia 95/46/CE, será necessária a realização do teste, de modo a verificar se este legítimo interesse se sobrepõe à proteção de dados pessoais concedida ao indivíduo pela Diretiva.

Nesse sentido propomos que seja incluído no art. 11 do APL novo inciso para contemplar essa hipótese, com a ideia de que os interesses tanto do titular do dado quanto do responsável pelo tratamento serão ponderados em cada situação, a fim de se verificar a possibilidade de utilização dessa base legal:

> Art. 11 - .....
>
> VIII - Tratamento necessário ao atendimento de interesses legítimos do responsável pelo tratamento, desde que não prevaleçam interesses e direitos do titular do dado.

6) Tratamento de dados sensíveis

Um ponto crucial para o mercado segurador é o tratamento de dados sensíveis, que no APL é regulado pelo art. 12. Não há nas hipóteses de tratamento de dados ali listadas uma que se refira à necessidade de tratamento para fins de conclusão ou execução de um contrato. Tais dados, em muitas hipóteses, como nos seguros de pessoas ou de saúde, são

[11] Ibid. P. 40.
[12] Ibid. P. 52.

fundamentais para a correta análise do risco e mesmo para o pagamento de eventual indenização. Na Inglaterra, por exemplo, o *Data Protection (Processing of Sensitive Personal Data) Order 2000* autoriza expressamente o tratamento de dados sensíveis para fins de seguros. No mesmo sentido, a autoridade italiana de proteção de dados, em sua autorização geral número 2/2009, autoriza o tratamento de dados de saúde para fins de seguro.

Diversos são os exemplos de situações nas quais a utilização dos dados sensíveis é indispensável para a relação entre o indivíduo e a entidade armazenadora do dado, como o caso de entidades religiosas, sindicais ou mesmo políticas em relação a seus associados ou afiliados, pois impedir que dados sensíveis relativos à crença religiosa, à opção política ou à associação sindical sejam coletados e utilizados nessas hipóteses não traria qualquer benefício para o titular dos dados, muito pelo contrário, provavelmente inviabilizaria a relação desse indivíduo com as referidas entidades.

No caso do contrato de seguro não é diferente. Existem situações nas quais o tratamento dados sensíveis é necessário, mas é evidente que não é todo e qualquer dado sensível que pode ser tratado para fins de seguro. A utilização de dados relativos à opção sexual, à orientação religiosa e à etnia, por exemplo (mesmo que se diga que possam influenciar no cálculo do risco), apresenta um potencial discriminatório elevadíssimo. Além disso, essa sua influência no risco seria demasiadamente subjetiva, não se justificando a utilização de tais dados, sob pena de se impor aos seus titulares um ônus excessivo, no sentido de fazerem prova negativa da existência desse aumento de risco, o que provocaria uma exposição inaceitável de sua privacidade.

A verificação da legitimidade do tratamento de dados sensíveis terá sempre como parâmetros os princípios gerais de proteção de dados trazidos no art. 6º do APL. Usaremos como exemplo a necessidade do tratamento de dados sensíveis nos contratos de seguros-saúde. Esse ramo de seguro conta com uma normativa específica, a Lei nº 9.656/98, que regula desde as coberturas mínimas que o seguro deve conter até as exclusões que estão autorizadas e o prazo máximo de carência que pode ser estabelecido no contrato.

Além disso, a seguradora, caso tenha dúvidas quanto à "higidez do consumidor ou da veracidade de suas informações", poderá exigir que ele se submeta a uma entrevista qualificada (§1º do art. 3º da Resolução Consu 02/98), na qual um médico o auxiliará no preenchimento da declaração de saúde.

Pode a seguradora, ainda, exigir que o potencial segurado se submeta a exames médicos ou periciais a fim de verificar seu real estado de saúde no momento da contratação, sendo vedada a alegação de preexistência de doença ou lesão após o segurado

ter se submetido a exame ou perícia em razão da entrevista qualificada, pois, nesse caso, o segurador teve todos os meios necessários para verificar o real estado de saúde do contratante. Essa é a interpretação que se extrai do disposto no §5º do art. 3º da Resolução Consu 02/98, que tem sido acompanhada por nossos tribunais superiores, que impõem ao segurador o dever de realizar exame prévio de saúde em seus potenciais clientes.[13]

Vê-se, portanto, que a seguradora, para uma adequada conclusão do contrato, deve exigir que o consumidor informe seus dados de saúde, notadamente no que toca a doenças e lesões preexistentes, determinando, quando necessário, que se submeta a exames médicos e periciais para verificar seu real estado de saúde no momento da contratação do seguro.

Da mesma forma, a seguradora deverá ter acesso aos dados médicos do segurado no decorrer do contrato (consultas, exames e cirurgias realizados após a contratação do seguro), a fim de que possa efetuar o reembolso dos gastos realizados, o que, aliás, é a razão de existir dessa atividade.[14] Pode ainda a seguradora exigir dados relativos à idade do consumidor, a fim de poder enquadrá-lo nas faixas etárias estabelecidas pela ANS.

Está, dessa forma, demonstrada a necessidade de tratamento de dados pessoais nessa relação contratual. A mesma necessidade existe em outros ramos de seguros, como os de vida ou acidentes pessoais, nos quais o tratamento de dados sensíveis é imperativo para a conclusão e execução dos contratos.

Da forma como está redigido o art. 12, qualquer tratamento de dados sensíveis que não estiver previsto em um dos seus incisos será ilegal, o que incluiu o tratamento para fins de execução de contrato de seguros, a não ser que se obtenha o consentimento especial do titular do dado, mediante instrumento próprio, na forma do que estabelece o art. 12, I do APL. Importante salientar que o próprio APL, no §1º de seu art. 7º reconhece que existem situações onde o consentimento pode ser condição para o fornecimento de produto ou serviço, quando os dados forem indispensáveis para a sua realização. Parece-nos, entretanto, que o consentimento em relação ao fornecimento de dados sensíveis em uma relação contratual não seria a base legal adequada a autorizar o tratamento de dados pessoais, o que justifica a inclusão de novo inciso no art. 12, na mesma linha do que prevê o inciso III do art. 11 do APL.

Outro dispositivo que merece revisão é a alínea ‘b’ do inciso I do art. 12 do APL que exige que o titular do dado seja alertado “quanto aos riscos envolvidos no tratamento

[13] STJ - AgRg no AREsp: 11056 RS 2011/0104868-9, Relator: Ministro RAUL ARAÚJO, Data de Julgamento: 16/08/2011, T4 - QUARTA TURMA, Data de Publicação: DJe 06/09/2011.
[14] DONEDA. Op. cit. p. 163.

desta espécie de dados". Parece-nos que a redação como está posta pode gerar confusão ao invés de beneficiar os titulares dos dados. Quais seriam esses riscos envolvidos – além da discriminação que já é vedada – que são diferentes dos riscos existentes em qualquer tratamento de dados, sensíveis ou não, a se justificar o 'alerta'. Acreditamos, assim, que referido dispositivo mereça ser revisto, para retirar a obrigação de alertar o titular do dado quanto aos riscos envolvidos no tratamento de dados desta espécie.

Por fim, ainda com relação ao tratamento de dados sensíveis, a previsão contida no §2º do art. 12, no sentido de que "o tratamento de dados pessoais sensíveis não poderá ser realizado em detrimento do titular, ressalvado o disposto em legislação específica", pode ter impactos negativos no setor de seguros, isto porque toda a lógica do seguro se funda na generalização e na discriminação, ou seja, de tratar grupos de pessoas semelhantes de forma semelhante e grupos distintos de forma distinta, a fim de enquadrá-las em categorias de risco de acordo com as características que apresentam, na medida em que os dados sensíveis de um titular podem ser utilizados para aumentar (ou reduzir) o valor do prêmio a ser pago, esse tratamento de dados poderia ser considerado "em prejuízo do titular", somente sendo autorizado por lei específica na forma da redação atual do APL.

Diante desse contexto, propomos redação de nova alínea a ser incluída no inciso II e para a alínea 'b' do inciso I, e do § 2º, todos do art. 12 do APL:

> Art. 12 - .....
>
> I - .....
> b) com informação prévia e específica sobre a natureza sensível dos dados a serem tratados; ou
>
> II - .....
> g) execução de procedimentos pré-contratuais ou obrigações relacionados a um contrato do qual é parte o titular.
>
> § 2º O tratamento de dados sensíveis não poderá ser realizado em detrimento do titular, ressalvado o disposto em legislação específica e as hipóteses na qual esse tipo de tratamento de dados decorrer da natureza do contrato do qual o titular do dado é parte.

7) <u>Término do tratamento de dados</u>

O parágrafo único do art. 14 do APL prevê que "Órgão competente estabelecerá períodos máximos para o tratamento de dados pessoais, ressalvado o disposto em legislação específica". Ocorre, porém, que existem situações, como nos contratos de longa duração, nas quais o tratamento de dados se dará por tempo indeterminado, o que, aliás, é reconhecido pelo próprio APL no §4º de seu art.10, que estabelece:

Art. 10 - .....

§4º - Nas atividades que importem em coleta continuada de dados pessoais, o titular deverá ser informado regularmente sobre a continuidade, nos termos definidos pelo órgão competente.

Assim, deve o parágrafo único do art. 14 ser coadunado com o §4º do art. 10 de forma a reconhecer a possibilidade de tratamento de dados por prazo indeterminado. Propomos, dessa forma, nova redação para o parágrafo único do art. 14 do APL:

Art. 14 - .....

Parágrafo único – O Órgão competente estabelecerá períodos máximos para o tratamento de dados pessoais, ressalvado o disposto no §4º do artigo 10 e disposição contida em legislação específica.

8) <u>Atendimento imediato de solicitação do titular do dado</u>

A obrigação de atender de imediato as solicitações apresentadas pelos titulares dos dados no que toca ao exercício dos direitos previstos nos incisos I a IV do art. 17 do APL, na forma prevista no §2º do mesmo art. 17 e no inciso I do art. 18 do APL pode criar uma série de problemas para os responsáveis pelo tratamento, já que tal obrigação não leva em consideração as peculiaridades dos tratamentos de dados a serem conduzidos pelos diversos setores.

Imaginemos a situação de uma universidade que receba diversos pedidos de acesso a informações de ex-estudantes e que tenha que atender a esses pedidos de solicitação ou mesmo que tenha que efetuar uma correção de dados solicitada por esses mesmos estudantes, ou então de um médico em relação a seus ex-pacientes. É evidente que a universidade e o médico, antes de atenderem à solicitação de acesso a informações, terão que rever todos seus arquivos, automatizados ou não, o que pode demandar um longo tempo, inviabilizando o atendimento imediato previsto no APL. A situação pode se complicar ainda mais se esses ex-estudantes ou ex-pacientes solicitarem alguma correção ou cancelamento de dados, o que imporá a análise de documentos e provas, no caso da universidade, e de exames clínicos, radiológicos e laboratoriais (só para citar alguns exemplos) no caso do médico, que muitas vezes não estarão na posse destes.

É importante salientar que diversos países-membros da União Europeia, além da própria Diretiva 95/46/CE, não estabeleceram prazos específicos para o atendimento aos direitos dos titulares de dados, deixando tal definição para leis específicas dos diversos setores que se utilizam de tratamento de dados pessoais para o desenvolvimento de suas

atividades ou para normas administrativas a serem adotadas pelas Autoridades de Proteção de Dados dos países.

Também o nosso Código de Proteção e Defesa do Consumidor, que tem como foco os cadastros de proteção ao crédito, apesar de ter estabelecido alguns prazos no § 3º de seu art. 43 em relação à comunicação a destinatários de dados de eventuais correções efetuadas nos dados por solicitação do consumidor titular do dado, não estabelece qualquer prazo nem para o atendimento a um pedido de acesso de dados nem para o momento em que o consumidor deve ser informado a respeito da abertura de cadastro, ficha, registro e dados pessoais e de consumo (art. 43, caput e §2º).

Apenas a título exemplificativo, a Lei de Acesso à Informação Pública prevê no §1º de seu art. 11 um prazo de 20 dias para o atendimento ao pedido de acesso a informação, prazo esse que pode ser prorrogado por mais 10 dias na forma do §2º do mesmo artigo.

Uma opção que parece mais adequada, e compatível com a própria lógica do APL, inclusive com o que estabelece o §3º do art. 17 do APL, seria a **faculdade** de o responsável atender à solicitação imediatamente e **não o dever** de fazê-lo. Propomos assim, nova redação para o §2º do art. 17 e para o inciso I do art. 18:

> Art. 17 - .....
>
> §2º - Os direitos previstos neste artigo serão exercidos mediante requerimento do titular a um dos agentes de tratamento, que adotará, sempre que possível, imediata providência para seu atendimento.
>
> Art. 18 - .....
>
> I - em formato simplificado e, sempre que possível, imediatamente, observado, na impossibilidade, o disposto no §3º do art. 17, ou

9) Possibilidade de revogação do consentimento

Outro ponto que traz insegurança para os setores produtivos é a possibilidade, irrestrita e sem qualquer ônus, de revogação do consentimento pelo titular do dado prevista no §6º do art. 7º do APL. É verdade que os tratamentos de dados que estão dispensados do consentimento, como aqueles previstos no inciso III do art. 11 do APL não seriam afetados por este dispositivo, entretanto, os tratamentos de dados sensíveis, que não possuem essa hipótese de dispensa do consentimento, seriam impactados, já que o §6º do art. 7º não traz qualquer consequência para a revogação do consentimento ou mesmo limitação ao exercício desse direito, o que pode prejudicar a correta e adequada prestação de diversos

serviços, como aqueles securitários, como os seguros de vida e de saúde, que dependem do tratamento de dados sensíveis para a correta entrega dos serviços contratados.

A solução que nos parece mais acertada, além da inclusão da hipótese de dispensa do consentimento prevista no §6º do art. 7º, seria limitar a possibilidade de revogar o consentimento nas hipóteses em que o tratamento for necessário à correta prestação do serviço contratado, ou seja, se o titular quiser revogar o consentimento para tratamento de dados sensíveis nessas hipóteses o contrato será rescindido, cabendo os ônus dessa rescisão ao titular do dado.

Propomos a seguinte redação para o §6º do art. 7º do APL:

> Art. 7º - .....
>
> §6º O consentimento pode ser revogado a qualquer momento, desde que sua revogação não implique na impossibilidade de execução de procedimentos pré-contratuais ou de cumprimento de obrigações relacionadas a um contrato do qual é parte o titular, hipóteses na quais a revogação do consentimento importará na rescisão do contrato com a imposição dos ônus da rescisão em desfavor do titular do dado.

10) Dever de comunicação sobre correção, cancelamento, dissociação ou bloqueio dos dados

Poderá trazer insegurança aos setores produtivos o disposto no §5º do art. 17, que prevê que "O responsável deverá informar aos terceiros a quem os dados tenham sido comunicados sobre a realização de correção, cancelamento, dissociação ou bloqueio dos dados, para que repitam idêntico procedimento". Em muitas situações, especialmente em tratamentos de dados realizados na internet, será inviável, se não impossível, comunicar a todos que tiveram acesso aos dados e que, portanto, terão realizado tratamento desses dados na forma do que estabelece o inciso II do art. 5º do APL. Parece-nos que aqui o melhor caminho seria determinar que essa obrigação de comunicação deveria ser limitada pela razoabilidade e proporcionalidade da medida.

Propomos a seguinte redação para o §5º do art. 17:

> Art. 17 - .....
>
> § 5º - O responsável deverá, sempre que possível, informar aos terceiros a quem os dados tenham sido comunicado sobre a realização de correção, cancelamento, dissociação ou bloqueio dos dados, para que repitam idêntico procedimento.

11) Revisão de decisões automáticas e segredo comercial

Outro ponto que chama a atenção no APL é o disposto em seu art. 19. Na sociedade de massa, a maioria dos processos decisórios decorrentes de relações contratuais é baseado em procedimentos automatizados. Essa situação se torna ainda mais evidente quando se trata de acesso a crédito ou a cobertura securitária, sendo possível hoje em dia, por exemplo, a contratação de um empréstimo por meio de uma transação online.

Além disso, o § 1º do referido dispositivo do APL prevê a possibilidade do titular do dado, que exercer o direito de revisão de decisões automáticas, conhecer os critérios e procedimentos utilizados para a decisão automática, sem qualquer ressalva quanto ao segredo comercial ou industrial, dispondo que o responsável estará obrigado a "fornecer, sempre que solicitadas, informações adequadas a respeito dos critérios e procedimentos utilizados para a decisão automatizada". Da forma como está redigido este dispositivo poderá violar não apenas o segredo comercial ou industrial, como também facilitar a prática de infrações penais, como, por exemplo, a fraude contra o seguro, já que conhecendo os critérios e procedimentos utilizados pelos sistemas das seguradoras fica muito mais fácil encontrar caminhos para burlar os sistemas de aceitação.

Acreditamos, assim, que o §1º do art. 19 do APL deve ressalvar, expressamente, o respeito ao segredo industrial e comercial como forma de impedir o fornecimento dos critérios e procedimentos utilizados para a decisão automática. Esse posicionamento está alinhado com as orientações contidas na já citada Diretiva europeia 95/46/CE,[15] que foi o modelo que inspirou o anteprojeto de lei sob análise.

Propomos assim, nova redação para o §1º do art. 19:

> Art. 19 - .....
>
> §1º - O responsável deverá fornecer, sempre que solicitadas e respeitado o segredo comercial e industrial, informações adequadas a respeito dos critérios e procedimentos utilizados para a decisão automatizada.

12) Responsabilidade solidária entre cedente e cessionário dos dados

Igualmente merece revisão o disposto no art. 22 do APL. O texto da forma como está prejudica sensivelmente a atividade econômica, porque muitas vezes o acesso a dados não significa automaticamente a sua utilização.

[15] Vide art. 15, §2º da Diretiva 95/46/CE.

Em grande parte das situações, o acesso a dados pode representar apenas uma consulta com o objetivo de obter elementos para sustentar o desenvolvimento de um produto ou serviço para ser futuramente oferecido ao mercado de consumo. Portanto, muitos daqueles que têm acesso não o utilizam e não podem ser solidariamente responsáveis.

No caso da atividade securitária é imprescindível que o dado tenha sido utilizado efetivamente, porque as seguradoras realizam milhares de acessos a dados e não os utilizam.

Se um segurado preenche proposta de contratação de seguros junto a várias seguradoras, com objetivo de contratar coberturas próprias do seguro de automóvel, e formaliza a contratação com uma delas em detrimento de todas as outras para as quais pediu uma cotação, todas as que consultaram dados de crédito sem utilizá-los porque a contratação não ocorreu com elas, não poderão ser responsabilizadas se, por ventura, esse segurado vier a ter um dano decorrente da referida consulta.

Em outras palavras, ter acesso é diferente de utilizar. Para caracterizar responsabilidade é preciso que os dados tenham sido efetivamente utilizados e seja determinado quem o fez. Caso contrário, a expansão da responsabilidade motivará os agentes a não utilizar dados e, consequemente, a não oferecer maior diversidade de produtos e serviços, o que é negativo para o mercado e para os consumidores em especial.

Por fim, há diferença fundamental entre a responsabilidade do agente que trata efetivamente os dados e aquele que por interconexão tem acesso a esses mesmos dados.

A responsabilidade é de quem efetua o tratamento e, somente poderá ser do agente que tem acesso por interconexão se, comprovadamente, esse agente utilizar os dados de forma ilícita e prejudicial.

Estabelecer responsabilidade objetiva e solidária em razão de acesso ou interconexão é excessivo, incompatível com a economia de mercado e, a rigor, cria uma cauda longa que vai dificultar a identificação do real causador do dano e permitir, em contrapartida, que ele continue agindo de forma indevida porque outros que tiveram acesso (diretamente ou por interconexão) indenizarão as vítimas de danos.

Ademais, tal posicionamento está na direção contrária da posição adotada pelo Superior Tribunal de Justiça no que toca à responsabilidade por inclusão indevida em

cadastros de proteção ao crédito, sendo responsável única e exclusivamente o fornecedor que incluiu a informação no cadastro e não o gestor da base de dados.[16]

Propomos, assim, seja suprimido o art. 22 e seu parágrafo único.

13) <u>Transferência para o Brasil de dados tratados no exterior</u>

Outra questão que deve ser melhor avaliada é a exigência contida no art. 32 do APL no sentido de que dados transferidos para o Brasil de um país estrangeiro somente poderão ser tratados em território nacional se em referido país tiverem sido observadas as suas normas – parece que do Brasil – relativas à obtenção do consentimento. É razoável exigir que o tratamento desses dados não poderá ser efetuado no Brasil se os dados não foram adequadamente tratados no exterior? Como será efetuado esse controle? Será que toda e qualquer transferência de dados pessoais do exterior para o Brasil deverá ser previamente aprovada pelo órgão competente? Essa exigência não encontra previsão similar na diretiva europeia já citada nem nas leis de proteção de dados dos países membros da União Europeia.

Ademais, o processo para verificação se, no caso concreto, os dados foram tratados em conformidade com as normas relativas ao consentimento é de alta complexidade, seja porque em diversas situações o consentimento não é exigido, seja pela barreira linguística - já que no mundo existem 192 idiomas oficiais – seja pela barreira técnica, uma vez que para se verificar se tais normas foram atendidas necessita-se conhecer o ordenamento jurídico do país no qual se deu o tratamento de dados em questão, o que não é tarefa fácil. Ademais, muitas vezes no país no qual se deu o tratamento de dados pode não existir qualquer exigência de consentimento ou mesmo de respeito às normas de proteção de dados para se admitir a transferência de dados, caso em que serviria, na verdade, a assegurar mais direitos aos titulares dos dados que estão sendo transferidos, já que os tratamentos de dados posteriores a essa transferência de dados serão regidos pelo regime estabelecido no APL.

Propomos, assim, seja suprimido o art. 32 do APL.

14) <u>Transferência internacional de dados</u>

O art. 28 do APL da forma como está redigido, traz uma série de dificuldades para a transferência internacional de dados.

[16] Vide REsp 1.087.487, Rel. Min. Luis Felipe Salomão. 4ª Turma. Julg. em 15/12/2011.

Diversas leis de proteção de dados adotaram posicionamento no sentido de autorizar a transferência internacional de dados para países não reconhecidos como provedores de um nível adequado de proteção de dados, sem a necessidade de aprovação de uma Autoridade Local, para situações nas quais tal transferência de dados é necessária para a execução de obrigações decorrentes de um contrato, como é o caso, por exemplo, da letra 'b' do item 1 do art. 43 da lei italiana[17] e o §5º do art. 69 da Lei Francesa,[18] só para citar alguns exemplos.[19]

Ressalte-se, outrossim, que o APL deixou de estabelecer um prazo dentro do qual o órgão competente deve se manifestar sobre um pedido de autorização para transferência internacional de dados, ou mesmo sobre a aprovação de cláusulas contratuais específicas, cláusulas padrão ou normas corporativas globais. Diante do enorme número de transferências internacionais de dados diárias e das conhecidas limitações de recursos dos órgãos públicos, manter-se a redação do art. 30 da forma como está gerará uma grande dificuldade e um incremento enorme de custos em diversas operações de transferências de dados, que teriam consequência direta no custo que o titular do dado pagaria por determinado serviço ou produto.

Além disso, quais seriam os critérios para avaliar se um país possui um nível de proteção de dados equiparável ao Brasil (é possível comparar, dadas as diferenças de cultura em cada país?). Há maneira de se fiscalizar de adequadamente o cumprimento dessa disposição? E como ficaria a transmissão de dados para funcionamento da internet, considerando a arquitetura da rede e sua característica fundamental de descentralização? Em outras palavras, há forma efetiva de o "órgão competente" controlar por quais países os dados pessoais dos usuários que trafegam na rede mundial de computadores ou fora dela serão transmitidos?

E ainda que se admitisse que tal controle seria possível, até que ponto esse tipo de controle efetivamente seria benéfico ao usuário e de seu pleno interesse? O "órgão competente" mencionado no APL teria capacidade técnica e legitimidade jurídica para averiguar quais são os países envolvidos em uma transmissão de dados, sobretudo via internet? Essa são questões primordiais que devem ser levadas em consideração no debate que permeia a redação do artigo 28 do APL.

Portanto, por mais que o artigo 28 do APL, em seu inciso III, preveja que o órgão competente poderá autorizar a transferência internacional de dados em sede de

[17] *Codice in materia di protezione dei dati personali (Decreto legislativo 30 giugno 2003, n. 196)*
[18] *Loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.*
[19] No mesmo sentido vide são as alíneas 'f' e 'g' do art. 34 da Lei Espanhola (*Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Caráter Personal).*

regulamento, parece de vital importância que a legislação brasileira não se limite a reproduzir as disposições europeias. Deve haver maior nível de atualidade, de modo que a redação desse artigo, se ele for mantido, seja compatível com o atual nível de desenvolvimento tecnológico das comunicações e da transmissão de dados no país e no mundo.

Por fim, na hipótese de manutenção do regime de adequação contido no art. 28 do APL, com o fim de se garantir a necessária segurança jurídica para os setores que realizam transferências internacionais de dados no curso de suas atividades, apresenta-se de fundamental importância a divulgação, por parte do órgão competente, de listas periódicas contendo os países que apresentam níveis adequados de proteção de dados, o que evitaria que os responsáveis pelo tratamento de dados tivessem que consultar o órgão competente em cada nova operação de transferência internacional de dados, o que, além de criar entraves desnecessários a tais operações, inundariam o órgão competente com consultas nesse sentido.

Sugerimos que, na hipótese de se optar pela manutenção desse procedimento de "adequação", nos moldes da Diretiva Europeia 95/46/CE, o que não se deseja, seja incluído mais um inciso e dois parágrafos no art. 28 – transformando o parágrafo único em parágrafo primeiro - e novo parágrafo no art. 30 do APL, para o que apresentamos a proposta de redação abaixo:

> Art. 28 - .....
>
> VI – quando a transferência for necessária à execução de procedimentos pré-contratuais ou obrigações relacionados a um contrato do qual é parte o titular.
>
> §1º -.....
>
> §2º - O órgão competente divulgará periodicamente lista contendo os países que proporcionem nível de proteção de dados pessoais equiparável ao desta Lei.
>
> §3º - Somente após a divulgação da primeira lista, com a análise mencionada acima, é que será exigido o cumprimento do disposto neste artigo.
>
> Art. 30 - .....
>
> §4º – até a aprovação do regulamento de que trata o caput deste artigo ficarão autorizadas, independente de autorização prévia do órgão competente, as transferências internacionais de dados pessoais para países que não proporcionem nível de proteção de dados pessoais equiparável ao desta Lei.

15) <u>Encarregado pelo tratamento de dados pessoais</u>

O art. 41 do APL, da forma como está redigido, pode ensejar a interpretação de que deverá existir um funcionário exclusivo para esta atividade. A diretiva europeia 95/46CE não trouxe essa previsão e diversas leis dos estados-membros europeus também não.

É bem verdade que, ultimamente, alguns países que já têm um solidificado sistema de proteção de dados, como França e Alemanha, incorporaram a figura do *data protection officer*, que exerce exatamente o papel do 'encarregado pelo tratamento de dados pessoais'. O exemplo francês, que teve o *correspondant à la protection des données personnelles* incorporado em sua lei de proteção de dados com a modificação de 2004, é uma faculdade do responsável pelo tratamento, que lhe traz uma série de benefícios no sentido de evitar diversas formalidades previstas na lei de proteção de dados. Além disso, a lei francesa autoriza a indicação de um único *correspondant à la protection de données personnelles* na hipótese de o responsável pelo tratamento ser parte de um grupo econômico, de uma entidade representativa de classe ou mesmo de uma empresa controladora ou controlada. Essa, em nossa opinião, é uma posição que balanceia melhor os interesses dos dois lados envolvidos, responsáveis pelo tratamento e órgão competente.

Portanto, a opção que parece mais correta é a que admite a possibilidade de indicação de um funcionário com funções de gerência ou direção que já exerça outras funções dentro da empresa e que passe também a acumular as funções de encarregado pelo tratamento de dados pessoais. Essa, aliás, foi a solução adotada pela Circular nº 344 da SUSEP, no parágrafo único de seu artigo 2º. Além disso, incluir a possibilidade de se indicar apenas um encarregado pelo tratamento de dados pessoais para todo um grupo econômico ou atividade vinculada à entidade de classe, na forma adotada pela lei francesa, seria um facilitador para a relação entre o órgão competente e os diversos responsáveis por tratamento de dados, pois nessa hipótese este teria que se relacionar apenas com um encarregado ao invés de diversos.

Além disso, o dispositivo em comento cria essa obrigação para todo e qualquer responsável por tratamento de dados pessoais, independente do seu tamanho ou do tipo de tratamento de dados que conduz. É verdade que o órgão competente estabelecerá normas sobre as hipóteses de dispensa da necessidade de definição, conforme critérios de natureza ou porte da entidade, e volume de operações de tratamento de dados, mas até que essas normas sejam adotadas os responsáveis pelo tratamento, por menor que sejam, terão que indicar um encarregado pelo tratamento de dados. Parece-nos que a melhor solução seria já constar do texto do APL – ao invés de deixar ao arbítrio do órgão competente – as hipóteses de dispensa, tais como o fato de ser micro ou pequena empresa, bem como o tipo tratamento de dados que está sendo conduzido, ou seja, que exija um controle regular e sistemático, por exemplo pelo potencial discriminatório do tratamento em questão,

conforme prevê o artigo 35.º da proposta de regulamento UE sobre proteção de dados. Propomos, assim, a seguinte redação para o art. 41 e para seu §3º e a redação de dois incisos no caput do art. 41 e três novos parágrafos para o mesmo artigo, com a renumeração dos demais parágrafos:

> Art. 41 – O responsável pelo tratamento deverá designar um encarregado pelo tratamento de dados pessoais sempre que:
>
> a) O tratamento for efetuado por uma autoridade ou órgão público;
> b) O tratamento for efetuado por uma empresa com 250 (duzentos e cinquenta) ou mais empregados; ou,
> c) As atividades principais do responsável pelo tratamento consistiam em operações de tratamento que, devido à sua natureza, âmbito e/ou finalidade, exijam um controle regular.
>
> §1º Caberá ao órgão competente determinar os critérios e requisitos aplicáveis às atividades principais do responsável pelo tratamento referidas na alínea c do caput deste artigo.
>
> §2º - .....
>
> §3º - .....
>
> §4º - Órgão competente estabelecerá normas complementares sobre a definição e as atribuições do encarregado.
>
> §5º - O encarregado pelo tratamento poderá ser apontado entre os funcionários com função de gestão ou direção já existentes na entidade privada e poderá acumular as funções de encarregado pelo tratamento de dados com outras funções por ele desenvolvidas.
>
> §6º - As entidades integrantes de um mesmo grupo econômico ou de uma mesma entidade de classe ficam autorizadas a indicar uma única pessoa que exercerá as funções de encarregado pelo tratamento de dados pessoais de todo o grupo ou setor econômico.

16) Vedação à transferência de dados pessoais por órgãos públicos para entidades privadas

O §3º do art. 2º do APL vedo aos "órgãos públicos e entidades públicas efetuar a transferência de dados pessoais constantes de bases de dados que administram ou a que tenham acesso no exercício de suas competências legais para entidades privadas, exceto em casos de execução terceirizada ou mediante concessão e permissão de atividade pública que o exija e exclusivamente para fim específico e determinado."

Essa vedação, se mantida, criará dificuldades para a cooperação entre poder público e privado em diversas áreas, inclusive no combate a atividades criminosas, como no caso do combate à fraude contra o seguro.

Importante frisar que em diversos países europeus é reconhecida a possibilidade de comunicação e interconexão de dados entre os setores privado e público.[20] Além disso, alguns instrumentos internacionais também reconhecem tal possibilidade, como a Recomendação Rec(2002) 9 do Conselho da Europa, que autoriza o tratamento de dados relativos a condenações penais para o fim de combate à fraude contra o seguro.[21]

Além disso, alguns setores empresariais se valem de informações fornecidas pelo setor público para o correto exercício de suas atividades. Exemplo disso ocorre com o setor de seguros, que necessita acessar informações de veículos, por exemplo, para efetuar de forma correta o pagamento das indenizações securitárias em caso de sinistros. Se esse acesso for inviabilizado, as seguradoras poderão deixar de indenizar uma financeira que possui uma garantia real sobre determinado veículo, o que certamente gerará insegurança para o mercado de financiamento de veículos.

Parece-nos que aqui a melhor solução seria admitir essa transferência de dados quanto existir um interesse público relevante. Essa é opção adotada por diversos estados membros da União Europeia, sujeitos às normas da já citada Diretiva Europeia 95/46/CE, que inspirou o texto do APL em comento. Neste sentido, mencione-se a experiência do DVLA (*Driver and Vehicle Licensing Agency*), órgão britânico responsável pelo licenciamento de veículos e condutores que, muito embora vinculado à obediência dos princípios de proteção de dados presentes no DAP (Data Protection Act, de 1998), tem a prática de revelar seletivamente informações referentes a condutores e veículos diante de requisições fundamentadas tanto de autoridades públicas que visam à investigação de delitos, como a terceiros que tenham um "motivo razoável" para tal pedido.[25] No mesmo sentido é a posição adotada pela Autoridade de Proteção de Dados de Malta, Estado-Membro da União Europeia, que, em suas linhas guias sobre a proteção de dados com vistas a promover boas práticas no setor securitário, reconhece como legítimo o tratamento de dados pessoais para fins de prevenção, detecção e combate à fraude contra o seguro, reconhecendo, ainda, que este tratamento pode envolver a troca de informações entre diferentes responsáveis por tratamento de dados no setor securitário.[26]

A própria lei de acesso à informação, no inciso V do §3º de seu art. 31 dispensa o consentimento do titular do dado nas hipóteses em que estiver presente um interesse público e geral preponderante.

Propomos, assim, a seguinte redação para o §3º do art. 2º do APL:

---

[20] Nesse sentido é o art. 120 do *Codice in materia di protezione dei dati personali* e as seções 68 a 72 do *Serious Crime Act 2007* do Reino Unido.
[21] Vide art. 4.7 do apêndice.

Art. 2º - .....

§3º – É vedado aos órgãos públicos e entidades públicas efetuar a transferência de dados pessoais constantes de bases de dados que administram ou a que tenham acesso no exercício de suas competências legais para entidades privadas, exceto em casos de execução terceirizada ou mediante concessão e permissão de atividade pública que o exija e exclusivamente para fim específico e determinado e naquelas hipóteses nas quais esteja presente um interesse público e geral preponderante, conforme preceitua o inciso V do §3º do art. 31 da Lei nº 12.527, de 18 de novembro de 2011.

17) Órgão competente pela fiscalização do atendimento à futura lei de proteção de dados

O APL não definiu qual será o órgão competente.

Um dos princípios norteadores da administração pública é o princípio da eficiência, incluído no art. 2º da Lei nº 9.784/99, que regula o processo administrativo em âmbito federal.

Na definição de Alexandre de Moraes "princípio da eficiência é o que impõe à administração pública direta e indireta e a seus agentes a persecução do bem comum, por meio do exercício de suas competências de forma imparcial, neutra, transparente, participativa, eficaz, sem burocracia e sempre em busca da qualidade, rimando pela adoção dos critérios legais e morais necessários para melhor utilização possível dos recursos públicos, de maneira a evitarem-se desperdícios e garantir-se maior rentabilidade social."[22]

A manutenção da redação atual, sem a definição de quem será o órgão (ou órgãos) competente, pode levar não só a uma repetição de procedimentos administrativos, mas também a um aumento de custos desnecessário para a administração pública e, como consequência, para a sociedade, já que diversas estruturas nas diversas esferas de governo poderiam ser criadas, isso sem se falar na necessidade de observação do princípio da legalidade na criação de novas estruturas na administração pública.

Como se não bastasse, a existência de diversas autoridades competentes para cuidar da matéria pode produzir decisões divergentes sobre a interpretação e aplicação dos dispositivos da lei de proteção de dados, o que geraria grande insegurança jurídica. O princípio da segurança jurídica, além de estar expressamente reconhecido na já citada Lei nº 9.874/99, vem sendo amplamente utilizado pelo Supremo Tribunal Federal.[23]

[22] Alexandre de Moraes. Reforma Administrativa*:* Emenda Constitucional nº 19/98. 3. ed., São Paulo : Atlas, 1999, p. 30.
[23] Vide RE 587648 RS. Rel. Min. Celso de Mello. 2ª Turma. Julg. em 30/11/2010.

Dessa forma, constata-se a inadequação da opção adotada pelo APL com relação aos princípios basilares da administração pública, impondo-se sua alteração. A solução que nos parece adequada é estabelecer que na hipótese de mercados regulados ou supervisionados, como o bancário e o securitário, o órgão competente seja o órgão regulador/supervisor do setor, que teria condições de editar as normas necessárias com relação a prazos e outras características do setor, bem como de aplicar as penalidades que se somariam às já sob sua competência.

Propomos, assim, a inclusão de um novo artigo nas disposições finais e transitórias – com a renumeração dos demais -, com a seguinte redação:

> Na hipótese de setores regulados ou supervisionados o órgão competente, para todos os fins desta Lei, será o órgão regulador ou supervisor do setor.

18) <u>Sanções administrativas</u>

Outro ponto que traz preocupação no APL diz respeito às sanções a serem aplicadas aos responsáveis pelo tratamento de dados pessoais.

Diversas leis de proteção de dados, como a Francesa,[24] preveem que a Autoridade Competente, antes de aplicar uma sanção, deve notificar o responsável pelo tratamento de dados a fim de que ele possa efetuar os ajustes necessários para se adequar à lei de proteção de dados. Só após o não atendimento à determinação feita na notificação é que a Autoridade Competente pode aplicar uma das sanções estabelecidas na lei.

Importante salientar que o fato de dar ao responsável pelo tratamento de dados a oportunidade de corrigir as falhas por ventura existentes não afasta, de forma alguma, o dever de indenizar eventuais danos causados em razão do não cumprimento das normas de proteção de dados.

Também merece atenção a questão de que não foram estabelecidos no APL os valores da multa pecuniária que pode ser aplicada, o que, além de afrontar o princípio da legalidade – eis que o valor das multas deve estar previsto em lei -, gera insegurança jurídica, pois, ao que parece, tais valores ficarão ao arbítrio do órgão competente, vinculado ao Poder Executivo e sujeito a influências políticas.

Propomos, assim, a seguinte redação para o inciso I do art. 50 do APL.

[24] Artigo 45 da *Loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.*

Art. 50 - .....

I – advertência e, em caso de reincidência, multa simples ou diária;

19) <u>Dados de acesso público irrestrito</u>

Tanto o art. 11 quanto o inciso II do art. 12 tratam dos "dados de acesso público irrestrito" cujo tratamento não necessita de consentimento prévio do titular.

Entretanto, o APL não traz uma definição do que seriam esses "dados de acesso público irrestrito", sendo de grande relevância definir que tipo de dado seriam.

Dessa forma, propomos a inclusão de novo inciso no art. 5º com a seguinte redação:

Art. 5º - .....

XIX – dado de acesso público irrestrito: dado pessoal que esteja disponível à consulta pública gratuita, por obrigação legal ou que seja livremente divulgado pelo próprio titular ao público, por qualquer meio.

20) <u>Período de transição</u>

Não há no APL regra transitória prevendo um período de adequação para que os tratamentos de dados já em funcionamento no momento da entrada em vigor da possível lei possam se adaptar às regras por ele trazidas, ficando tal previsão a cargo do órgão competente, na forma do que estabelece o art. 51 do APL.

Tanto a diretiva europeia, que serviu de inspiração para o anteprojeto de lei, quanto diversas leis dos estados-membros europeus estabeleceram prazos para adequação dos tratamentos de dados já em operação quando de suas entradas em vigor. Nesse sentido é o artigo 32, §1º da diretiva europeia e os artigos. 54 da lei portuguesa e 14, §1º da lei inglesa.

Além disso, diversas leis nacionais têm previsto períodos de adequação para que as partes por elas atingidas se adaptem às suas regras, sendo exemplos o §1º do art. 35-E da Lei nº 9.656/96, a Lei Complementar nº 657/2007 do Município de Blumenau e até o Código Civil de 2002 (art. 2.031), este último tendo estabelecido um prazo de 5 (cinco) anos dentro do qual as "associações, sociedades e fundações, constituídas na forma das leis anteriores, bem como os empresários, deverão se adaptar" às suas disposições.

Vê-se, portanto, que a previsão de um período de adequação na forma proposta neste item, com a alteração da redação do art. 51 do APL, segue a mesma orientação adotada por diversas leis nas diversas esferas federativas.

Também não se mostra razoável o prazo de *vacatio legis* estabelecido pelo APL em seu art. 52, de apenas, 120 (cento e vinte) dias, considerando-se que suas regras modificarão consideravelmente a atuação, procedimentos e sistemas de diversos setores, sendo recomendável a adoção de prazo maior, de no mínimo 180 (cento e oitenta) dias.

Propomos, assim, as seguintes redações:

> Art. 51 – Os tratamentos de dados pessoais que já estiverem em atividade quando da entrada em vigor desta Lei, terão o prazo de 2 (dois) anos para se adaptarem às regras previstas nesta Lei.
>
> Art. 52 – Esta Lei entrará em vigor no prazo de 180 (cento e oitenta) dias contados da data de sua publicação.

21) <u>Outros temas</u>

a - <u>Princípio da adequação</u>

Um dispositivo que merece aperfeiçoamento é o inciso II do art. 6º que define o princípio da adequação. O conceito de “almejadas e com as legítimas expectativas” é muito subjetivo, pois o titular pode almejar, por exemplo, a concessão de um financiamento e o tratamento de seus dados pode causar o efeito inverso, o que não significa que a finalidade pela qual o dado foi coletado não fosse adequada. Propomos a seguinte redação para referido dispositivo do APL:

> Art. 6º - .....
>
> II – princípio da adequação, pelo qual o tratamento deve ser compatível com as finalidades informadas ao titular no momento do consentimento, de acordo com o contexto do tratamento;

b - <u>Princípio da finalidade</u>

O inciso I do art. 6º do APL prevê que o tratamento dos dados deve ser realizado com finalidades legítimas, específicas, explícitas e conhecidas pelo titular. Sugerimos alteração quanto ao termo “conhecidas”. Isso porque, a depender da interpretação que se tenha (ou que se queira ter), o termo “conhecidas” pode impactar diretamente na análise da legalidade do tratamento dos dados. Se a finalidade já será legítima, específica e explícita,

ou seja, devidamente informada ao titular, poder-se-ia suprimir o termo “conhecida”, porque isso implica, em última análise, no nível de instrução, educação e conhecimento geral do titular, o que transcende as obrigações legais do responsável pelo tratamento. Em outras palavras, a legalidade do tratamento dos dados não deveria depender de fatores que extrapolam a capacidade do responsável pelo tratamento, como, por exemplo, o nível de conhecimento geral e cultural do titular.

Parece-nos que a melhor opção seria substituir o termo “conhecidas” pelo termo “informadas”, que reflete melhor o intuito do APL, de assegurar que o titular do dado receba todas as informações necessárias ao correto entendimento do tratamento de dados que será conduzido. A redação do dispositivo em comento passaria a ser a seguinte:

> Art. 6º - .....
>
> I - princípio da finalidade, pelo qual o tratamento deve ser realizado com finalidades legítimas, específicas, explícitas e informadas ao titular;

c - <u>Princípio da qualidade doa dados</u>

O inciso V do art. 6º do APL determina que os dados estejam sempre atualizados. No entanto, muitas das vezes a atualização de determinados dados depende da própria conduta de seu titular ou de intermediários, responsáveis pela efetiva coleta dos dados. Nesse ponto, entendemos, salvo melhor juízo, que a lei deveria deixar claro que não se poderá exigir a atualidade dos dados ao agente que é incapaz de ter conhecimento sobre a desatualização.

Propomos, assim, a seguinte redação para o dispositivo em comento:

> Art. 6º - .....
>
> V - princípio da qualidade dos dados, pelo qual devem ser garantidas a exatidão, a clareza e a atualização dos dados, de acordo com a periodicidade necessária para o cumprimento da finalidade de seu tratamento, ressalvadas as hipóteses nas quais a atualização depender de informação a ser prestada pelo titular do dado.

d - <u>Consentimento</u>

Também se mostra pertinente esclarecer que o outro meio que certifique o consentimento previsto no §3º do artigo 7º pode ser o eletrônico.

Com a expansão da utilização da internet e do comércio eletrônico, a grande maioria dos dados pessoais são coletados através desse meio, sendo mais do que razoável que o consentimento também possa ser fornecimento através do mesmo meio pelo qual a contratação é realizada.

Além disso, diante dessa possibilidade de fornecimento do consentimento através de outro meio que o certifique, conforme salientado acima, mostra-se igualmente necessário alterar o disposto no §4º do artigo em comento.

Propomos, assim, a seguinte redação para os §§3º e 4º:

> Art. 7º - .....
>
> §3º O consentimento deverá ser fornecido por escrito ou por outro meio que o certifique, inclusive o meio eletrônico.
> §4º No caso de consentimento por escrito, esse deverá ser fornecido de forma destacada das demais cláusulas contratuais.

e - Consentimento de incapaz

O art. 8º do APL prevê que "o titular de dados pessoais com idade entre doze e dezoito anos idade poderá fornecer consentimento para tratamento que respeite sua condição peculiar de pessoa em desenvolvimento, ressalvada a possibilidade de revogação do consentimento pelos pais ou responsáveis legais, no seu melhor interesse." Esse dispositivo não observa o disposto nos arts. 3º e 4º do Código Civil, devendo ser com eles compatibilizado. Propomos a seguinte redação para o art. 8º do APL:

> Art. 8º - o titular de dados pessoais com idade inferior a dezoito anos poderá fornecer consentimento para tratamento que respeite sua condição peculiar de pessoa em desenvolvimento, assistido ou representado por seus pais, tutores ou curadores na forma da Lei civil e no seu melhor interesse.

f - Dispensa de consentimento e contratos por tempo indeterminado

O § 1º do art. 11 do APL exige que os dados pessoais devem ser tratados pelo menor período de tempo possível, o que pode gerar alguma confusão no que toca aos contratos por tempo indeterminado, como os seguros saúde. Apesar de a definição de menor tempo possível não parecer limitar o tratamento de dados nestas hipóteses, parece-nos seja recomendável, para afastar qualquer dúvida, incluir uma ressalva expressa a esses tipos de contratos. Propomos, assim, a seguinte redação para o dispositivo em comento:

Art. 11 - .....
§ 1º Nas hipóteses de dispensa de consentimento, os dados devem ser tratados exclusivamente para as finalidades previstas e pelo menor período de tempo possível, salvo nas hipóteses de contratos por tempo indeterminado, conforme os princípios gerais dispostos nesta Lei, garantidos os direitos do titular.

g - Incidente de Segurança

Mostra-se relevante, também, definir o significado de "incidente de segurança", contido no art. 44 do APL, para que haja clareza do que efetivamente deve ser comunicado, afastando-se interpretações subjetivas.

h - Responsabilização por violação do disposto no §2º do art. 11 do APL

O referido dispositivo prevê que o operador ou responsável pelo tratamento poderá responsabilizado, sem esclarecer que tipo de responsabilização seria essa. Parece-nos que a melhor opção seria mencionar que o operador ou responsável que descumprir o disposto no §2º do art. 11 do APL estará sujeito às sanções previstas em seu art. 50. Propomos, assim, a seguinte redação:

Art. 11 - .....

§3º - No caso de descumprimento do disposto no §2º, o operador ou o responsável pelo tratamento de dados estará sujeito às sanções previstas no art. 50 desta Lei.

i - Informações sobre o contato do responsável pelo tratamento

Outro ponto que merece reparo diz respeito ao §3º do art. 10 do APL que exige que o responsável pelo tratamento comunique aos titulares dos dados suas informações de contato atualizadas toda vez que ocorrer qualquer mudança. A redação como está posta pode levar à interpretação de que essa informação deverá ser feita de forma individualizada, por exemplo por meio de carta com aviso de recebimento, o que traria um ônus grande e, por outro lado, não traria um benefício significativo para o titular dos dados. Uma medida que parece razoável e proporcional e que atenderia os interesses do titular do dado, seria manter essa informação atualizada em seu sítio eletrônico para que o titular do dado, sempre que precisar, puder consultar essa informação. Propomos, dessa forma, a seguinte redação para o dispositivo sob análise:

Art. 10 - .....
§3º Em caso de alteração de informação referida no inciso IV do caput, o responsável deverá comunicar as alterações em seu sítio eletrônico.

São esses os comentários e sugestões da CNseg/FENASEG.

Rio de Janeiro, __ de junho de 2015.

_____
CNseg/FENASEG